Протокол IPSec

(RFC 2401)

Назначение IPSec

- ✔ Разграничение доступа (фильтрация IP-трафика)
- ✔ Обеспечение целостности передаваемых данных
- ✔ Обеспечение аутентичности передаваемых данных
- ✔ Защита от повторной передачи IP-пакета
- ✔ Шифрование передаваемых данных

Семейство IPSec

Протокол Authentication Header (AH)

Аутентификация
Контроль целостности
Защита от повторной передачи IP-пакета

Протокол Encapsulated Security Payload (ESP)

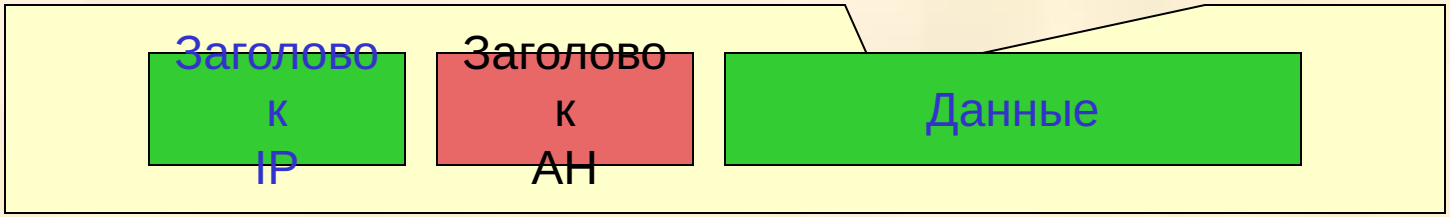
Аутентификация
Контроль целостности
Защита от повторной передачи IP-пакета
Шифрование

Протокол Internet Key Exchange (IKE)

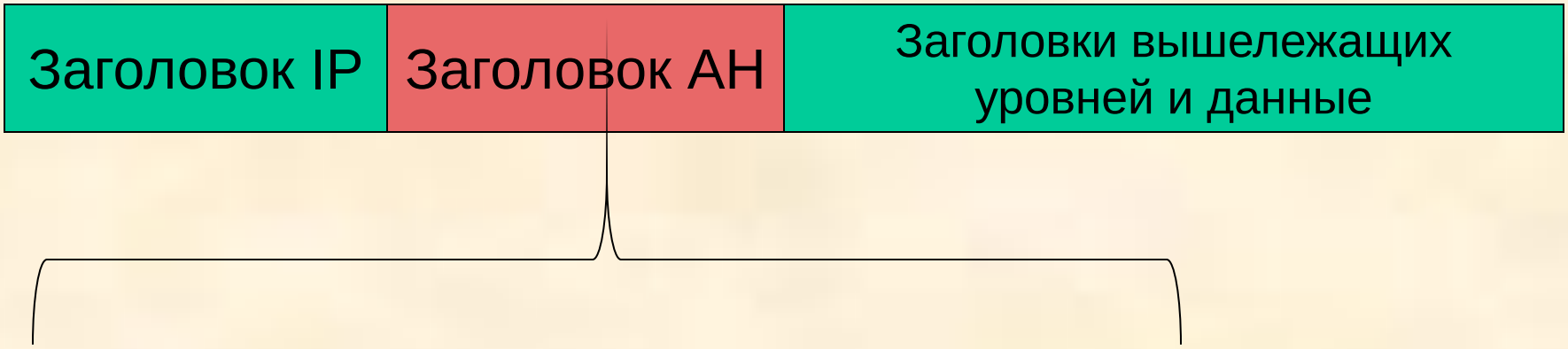
Согласование алгоритмов шифрования
Обмен ключами

Протокол AH


Узел А
IP-пакет
IP-пакет
IP-пакет
Узел В


Заголовок IP
Заголовок AH
Данные

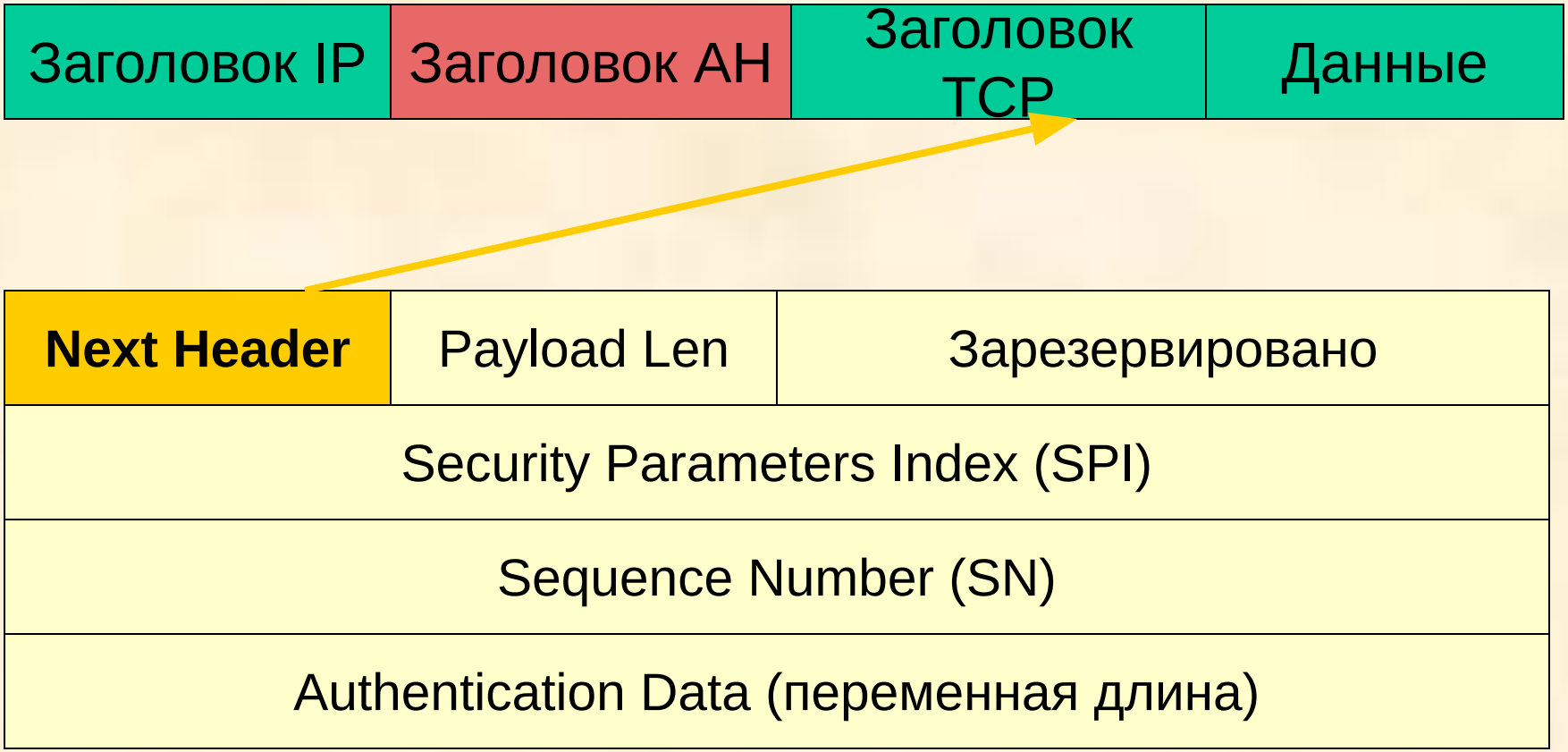
Протокол AH



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

0 8 16 31

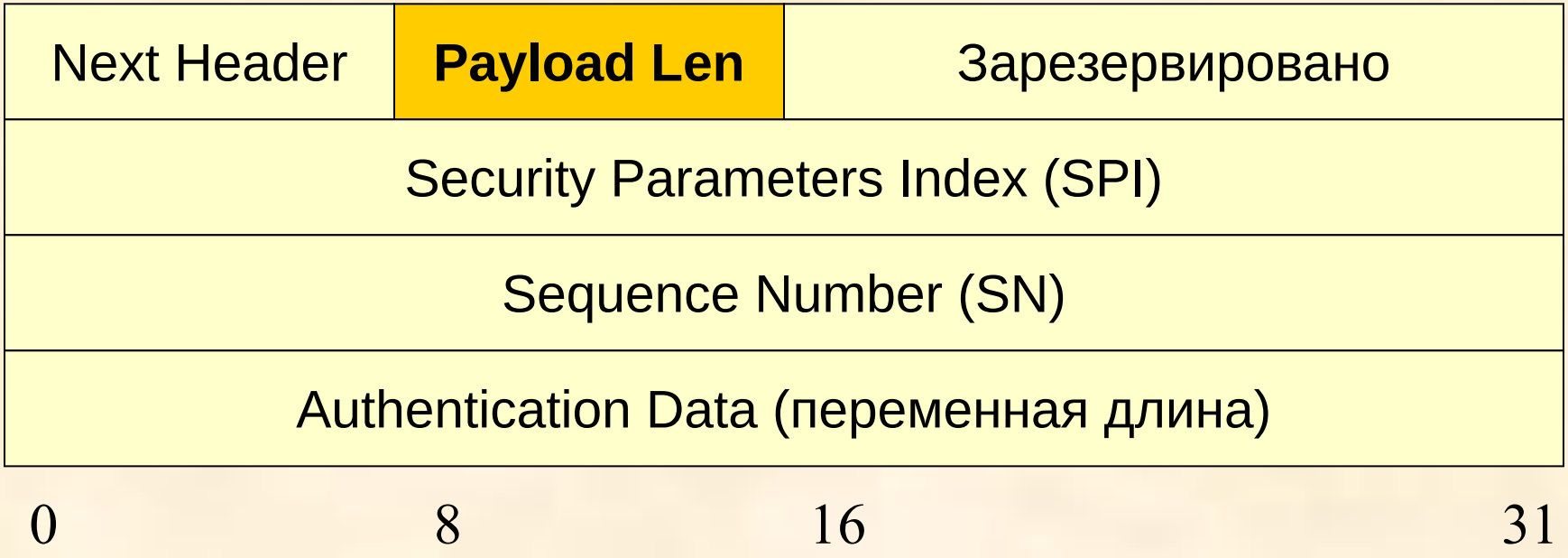
Протокол AH



Поле Next Header

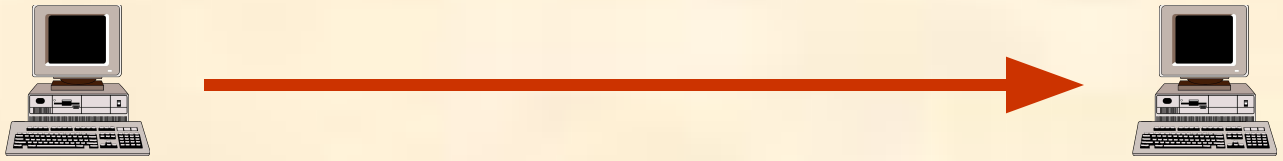
Протокол AH

Длина



Поле Payload Len

Протокол AH



Метка безопасной ассоциации

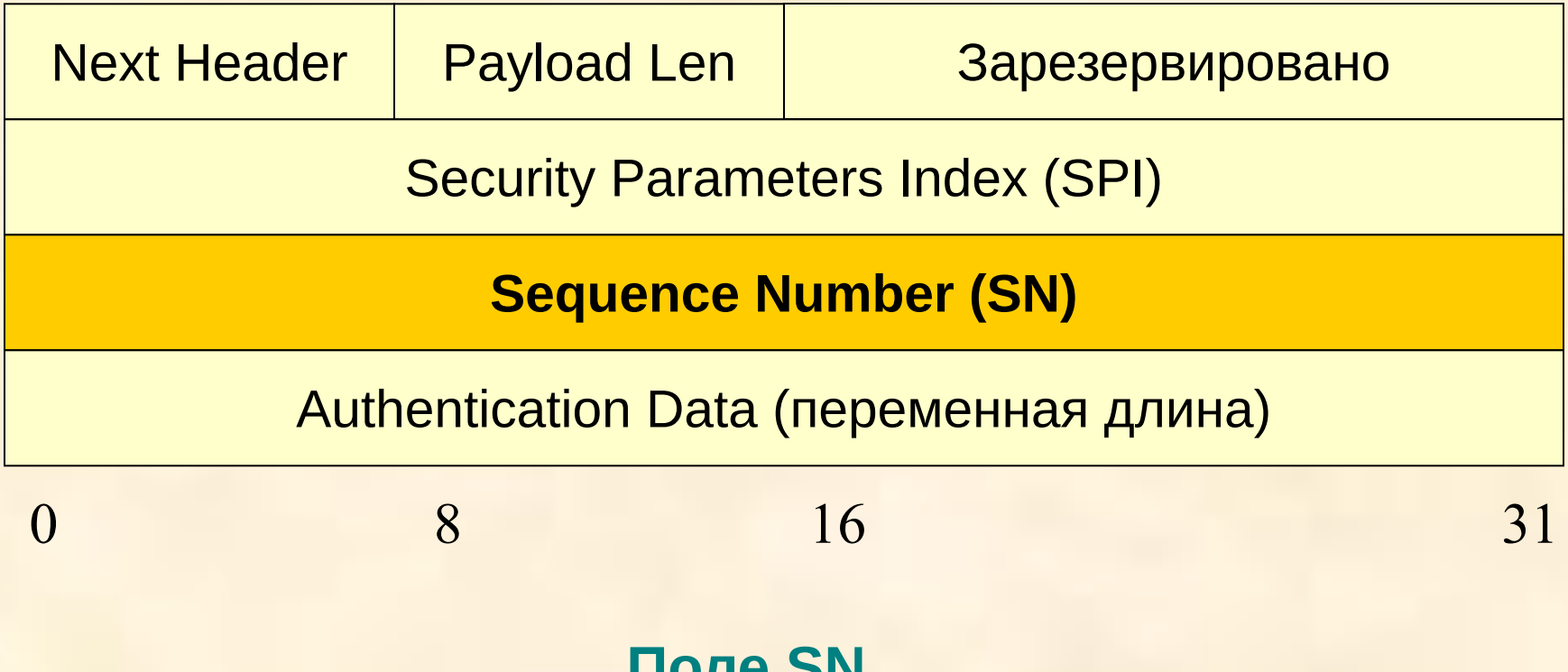
Next Header	Payload Len	Зарезервировано
Security Parameters Index (SPI)		
Sequence Number (SN)		
Authentication Data (переменная длина)		

0 8 16 31

Поле SPI

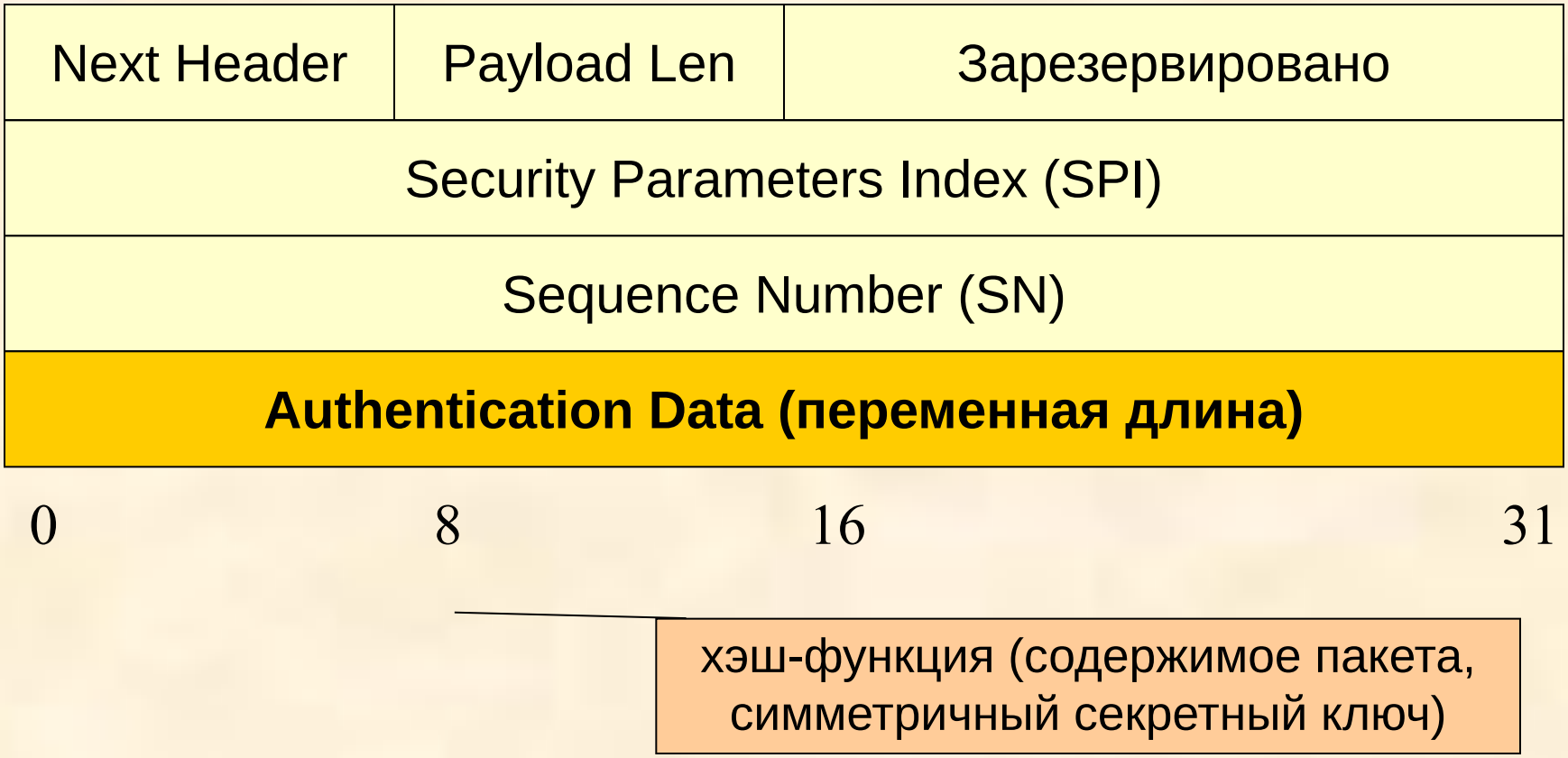
Протокол AH

Наращивается для каждого следующего пакета



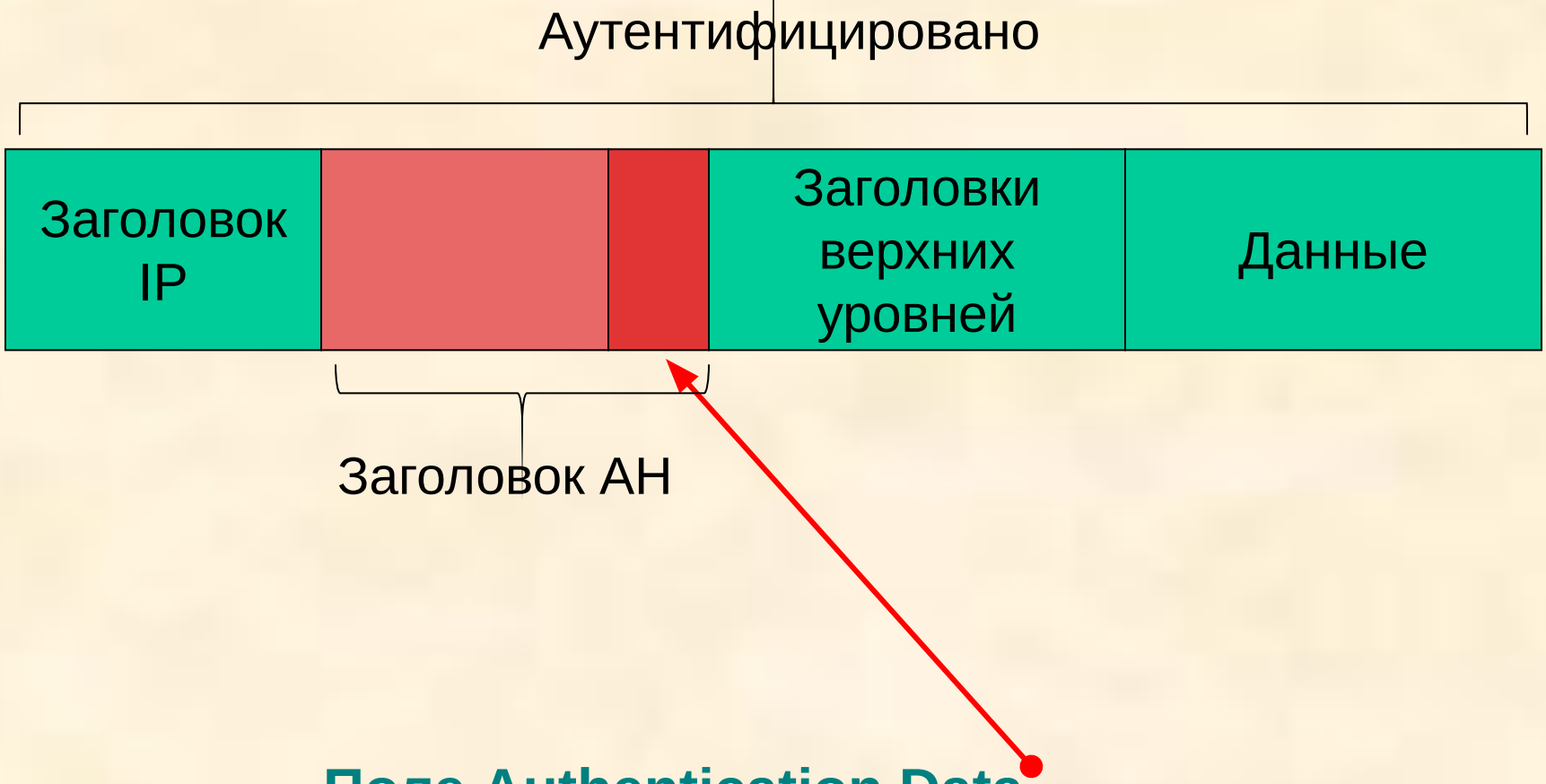
Поле SN

Протокол AH

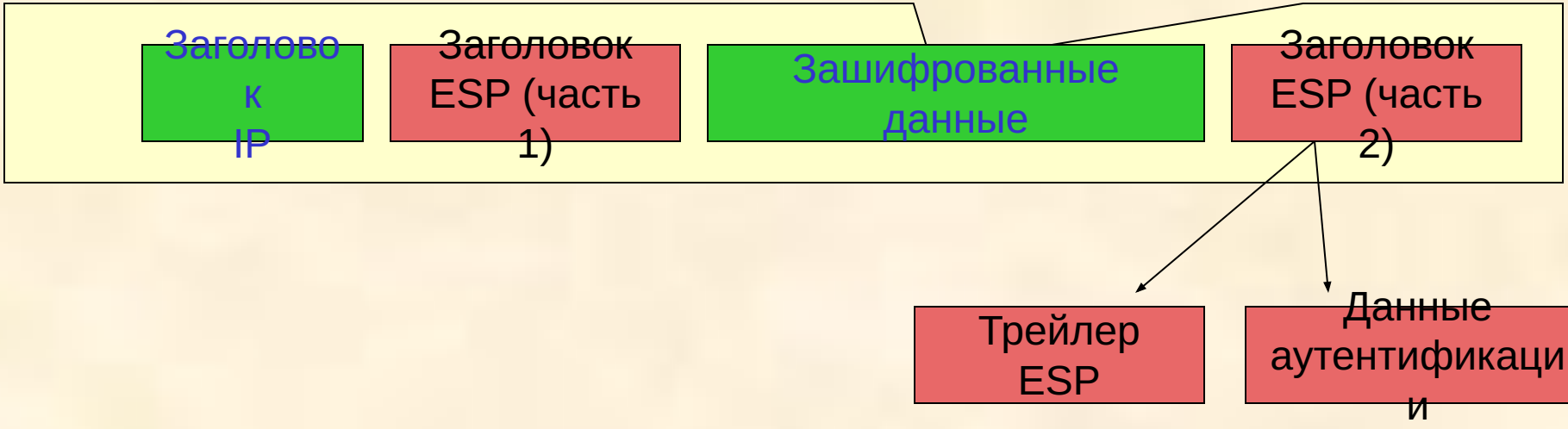


Поле Authentication Data

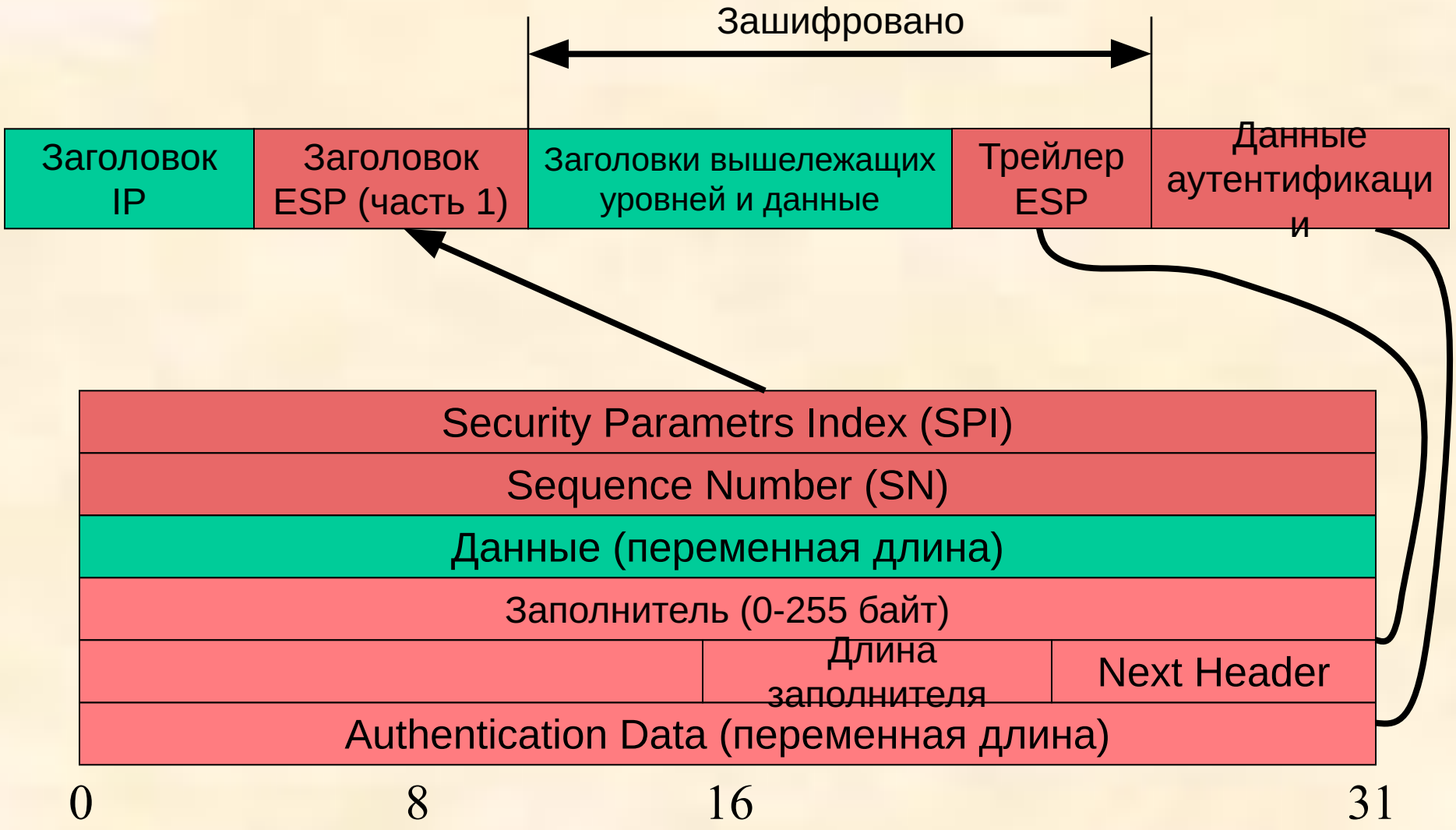
Протокол AH


Аутентифицировано
Заголовок IP
Заголовки верхних уровней
Данные
Заголовок AH
Поле Authentication Data

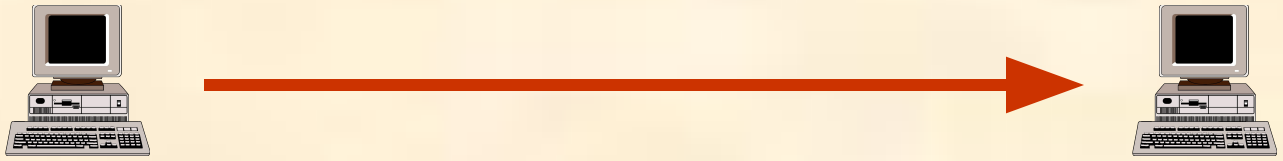
Протокол ESP



Протокол ESP



Протокол ESP



Метка безопасной ассоциации

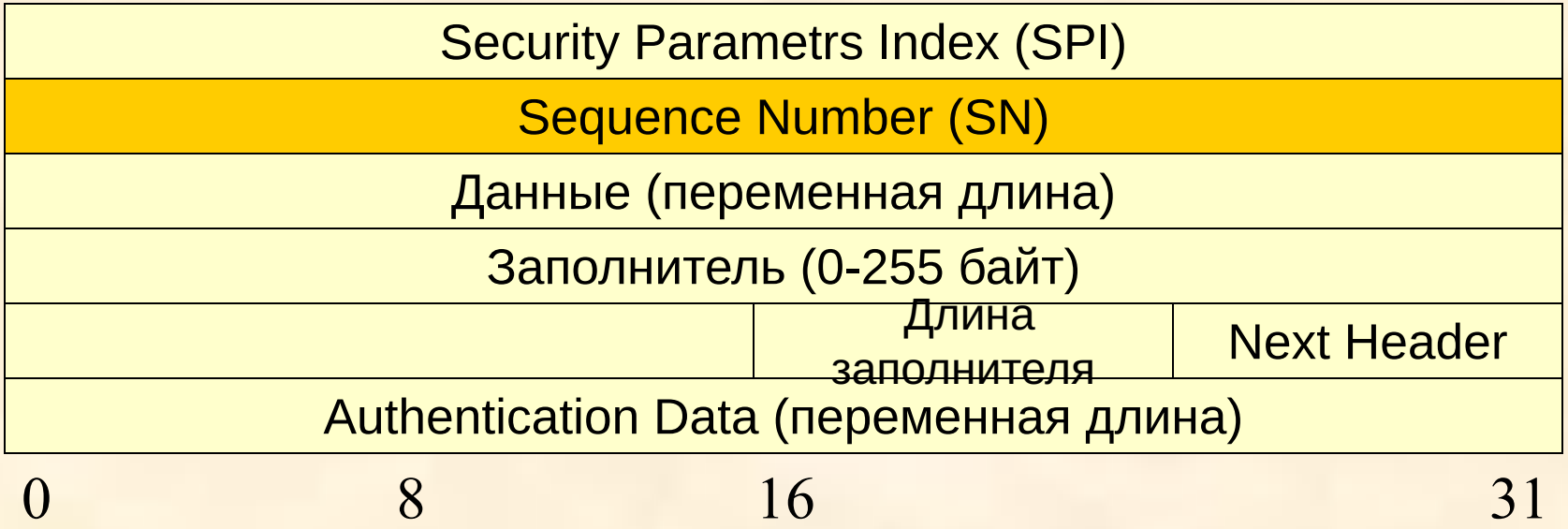
Security Parametrs Index (SPI)		
Sequence Number (SN)		
Данные (переменная длина)		
Заполнитель (0-255 байт)		
	Длина заполнителя	Next Header
Authentication Data (переменная длина)		

0 8 16 31

Поле SPI

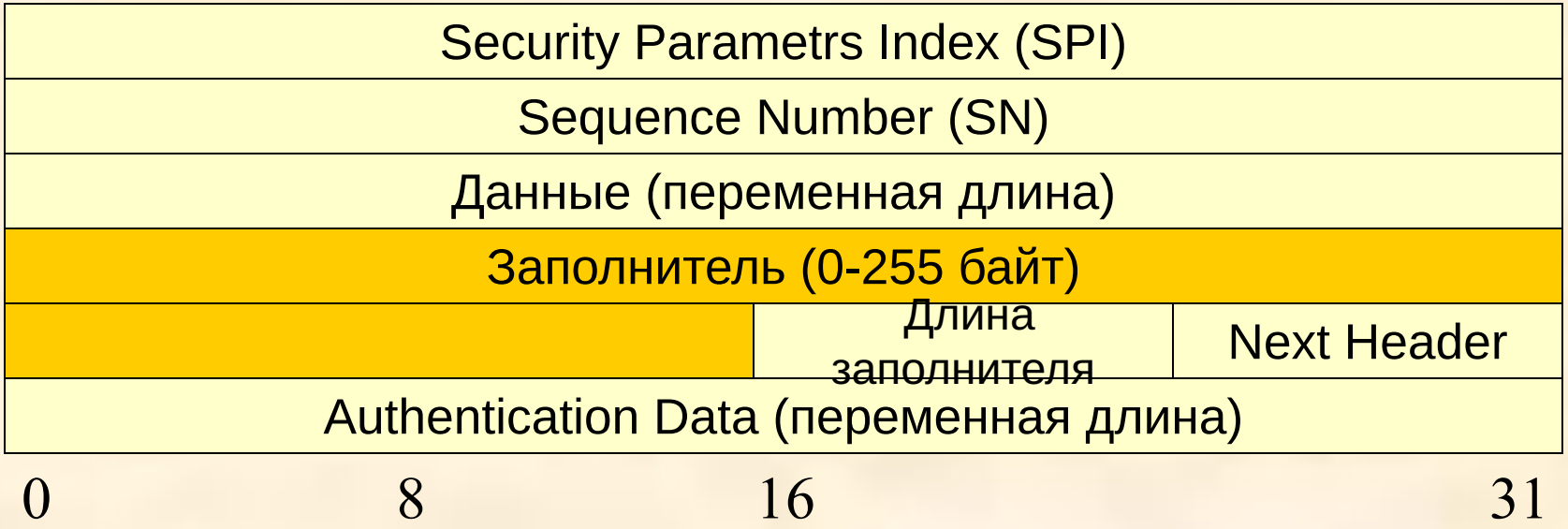
Протокол ESP

- Наращивается для каждого следующего пакета



Поле SN

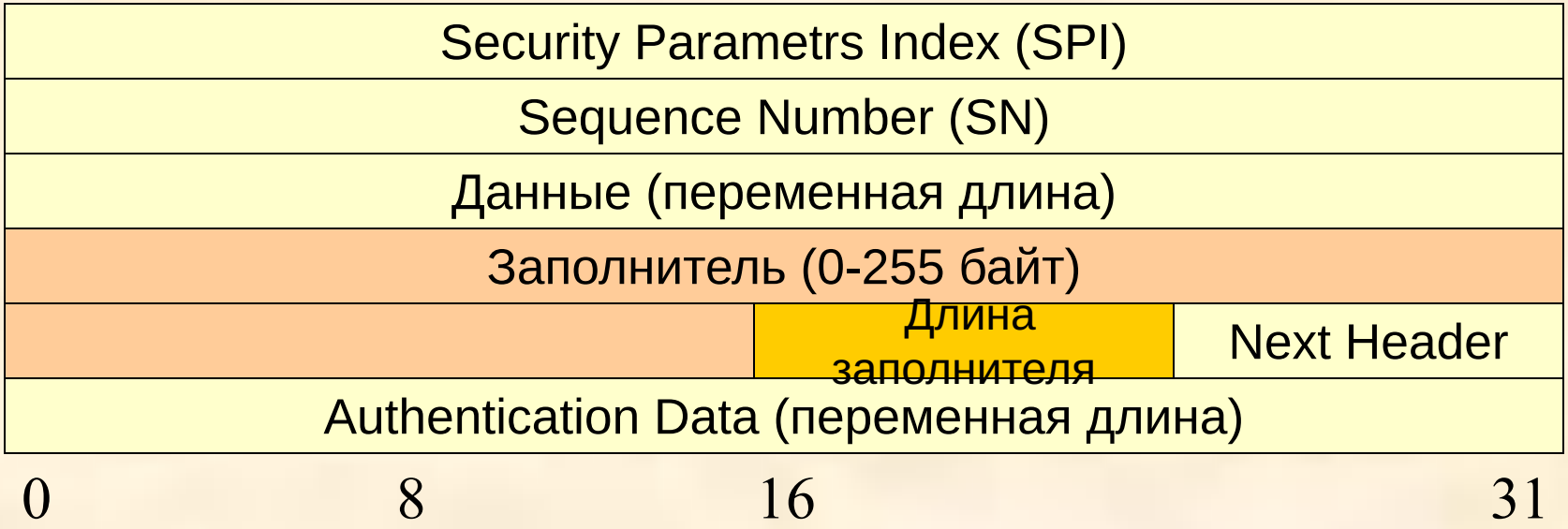
Протокол ESP



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

Поле заполнителя

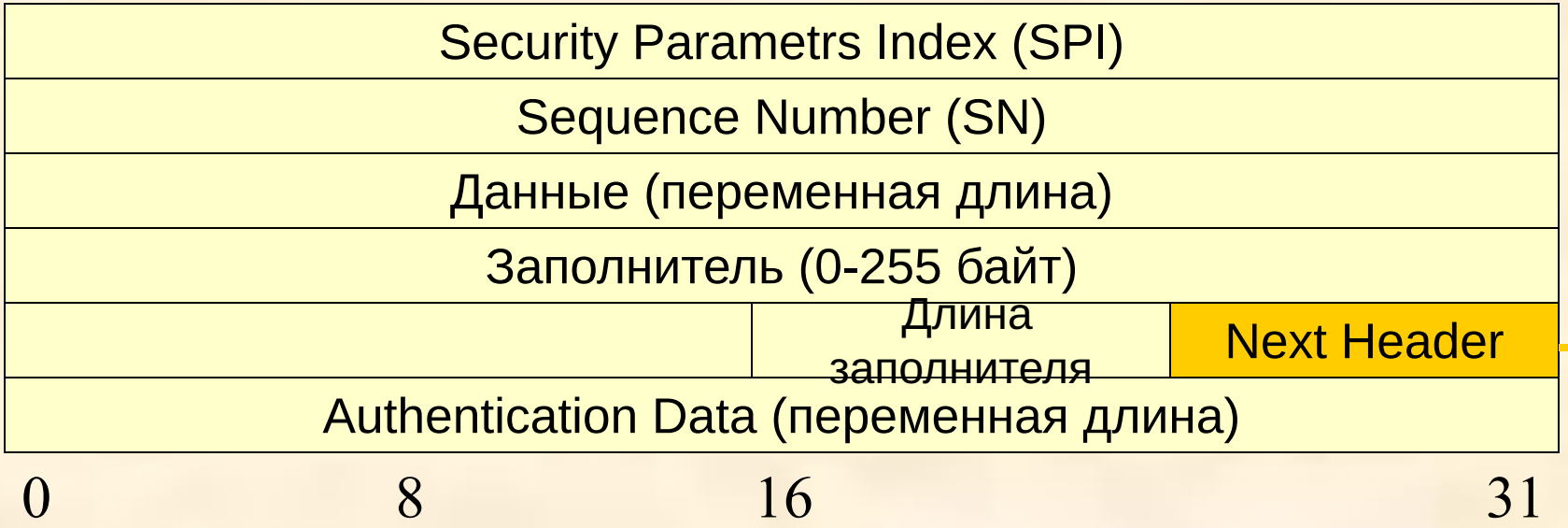
Протокол ESP

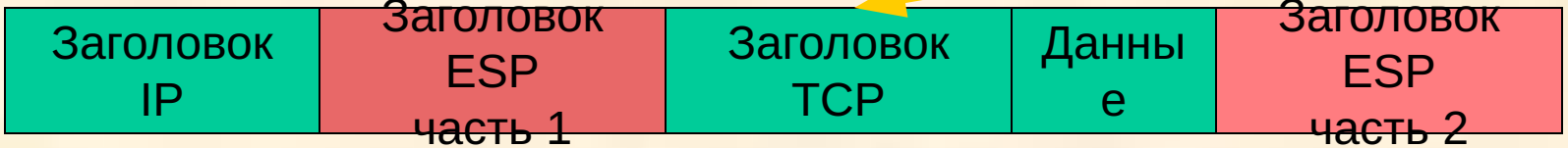


- Длина заполнителя в байтах

Поле длины заполнителя

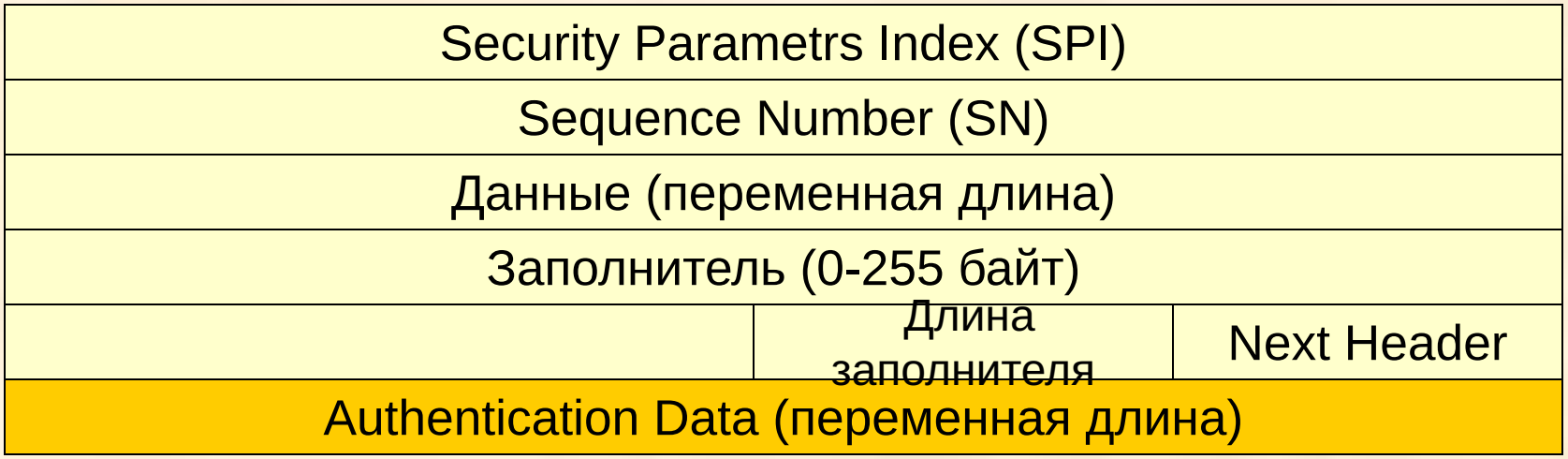
Протокол ESP





Поле Next Header

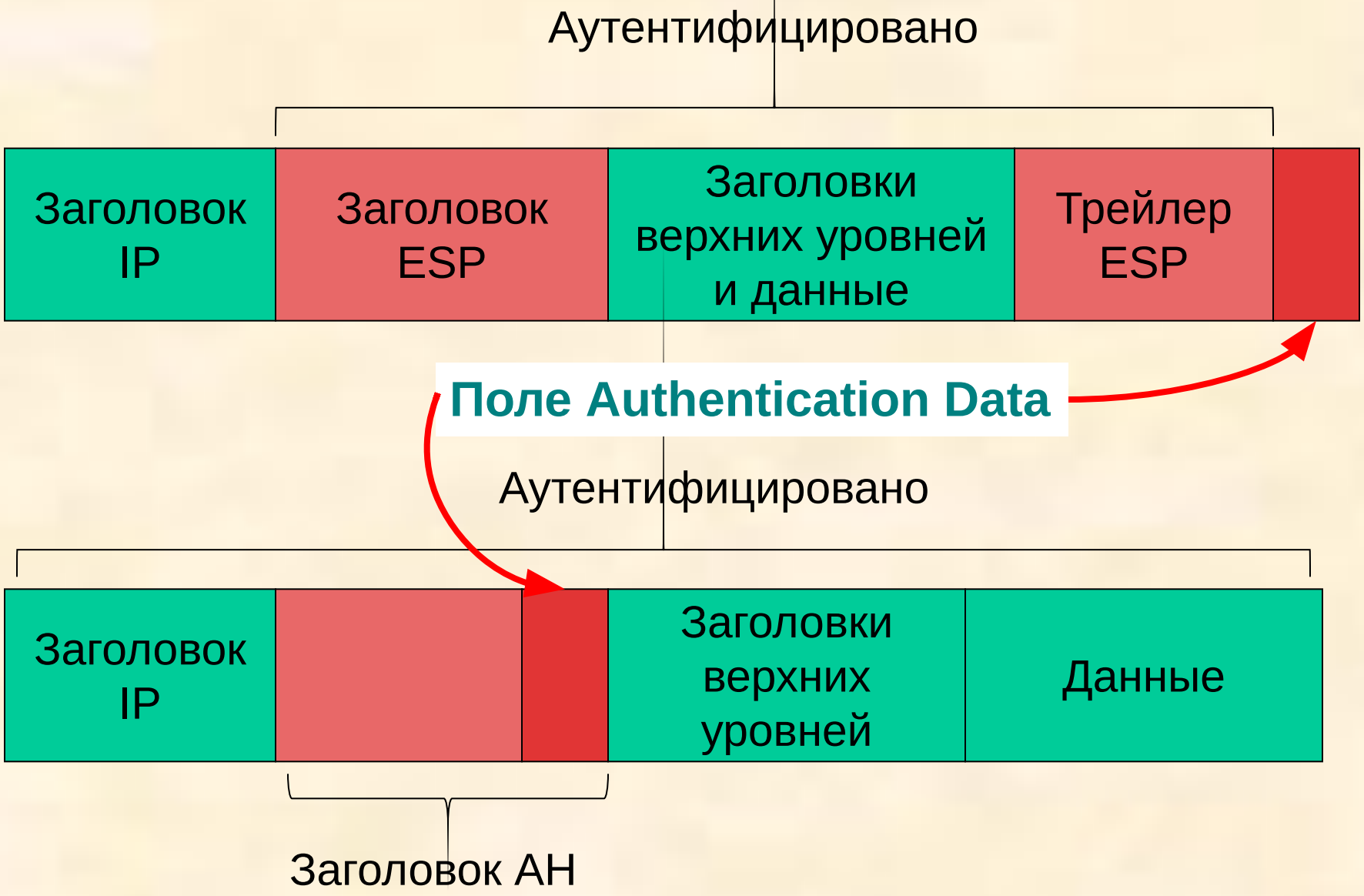
Протокол ESP



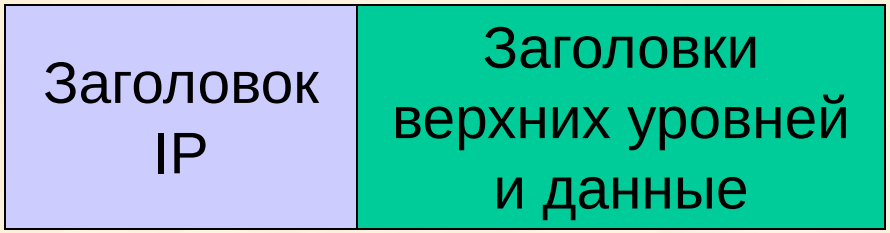
Поле Authentication Data

Протокол ESP

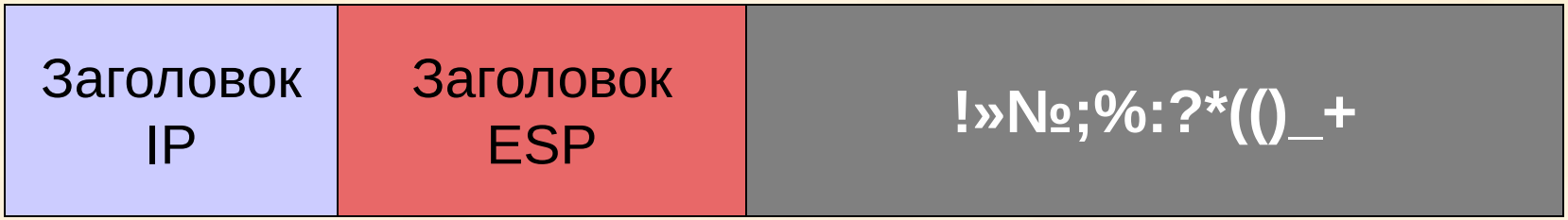
Протоколы AH и ESP - сравнение



Формирование пакета ESP



Формирование пакета ESP

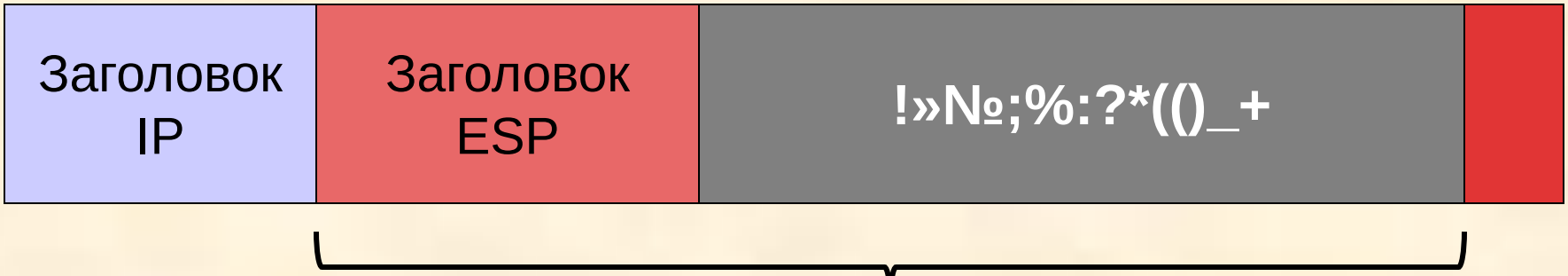


1. Формирование заголовка ESP (часть 1)

2. Формирование трейлера ESP

3. Шифрование

Формирование пакета ESP

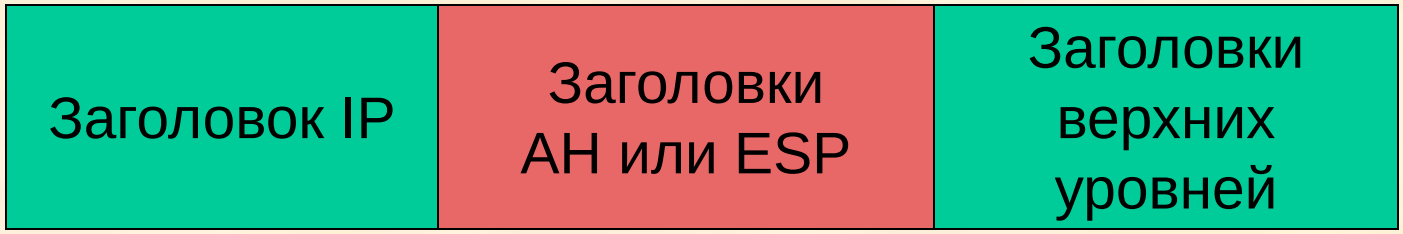


4. Вычисление данных аутентификации

5. Добавление данных аутентификации в конец пакета

Режимы работы IPSec

Транспортный режим



Туннельный режим

Схемы применения IPSec

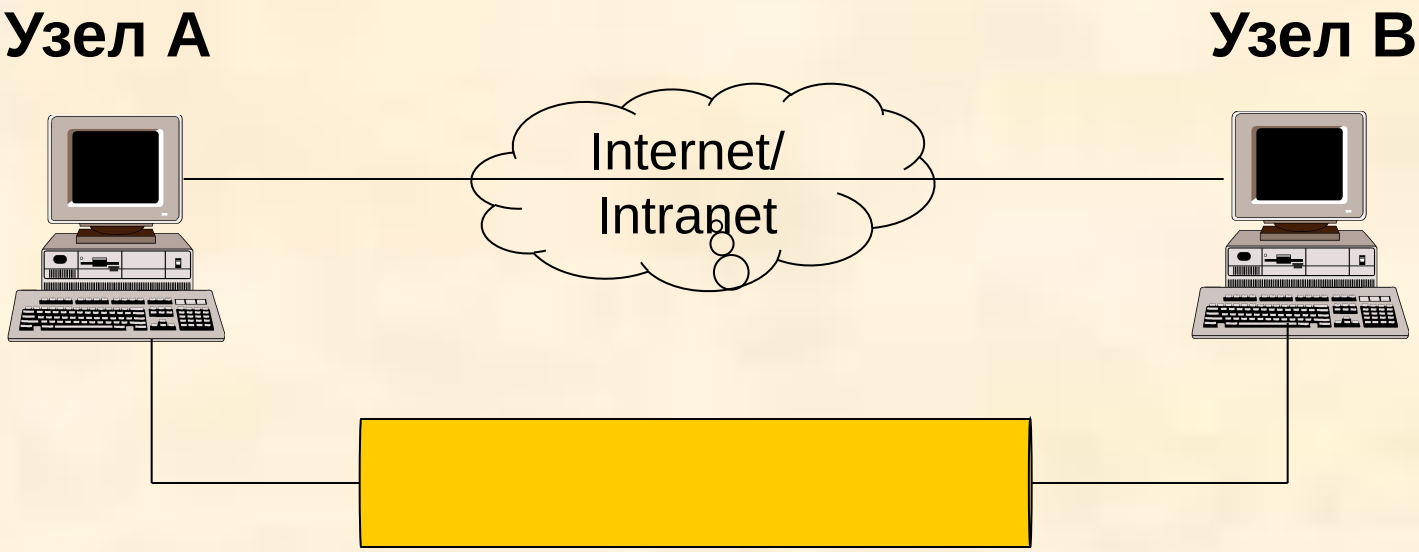


Схема узел-узел (точка-точка)

Схемы применения IPSec

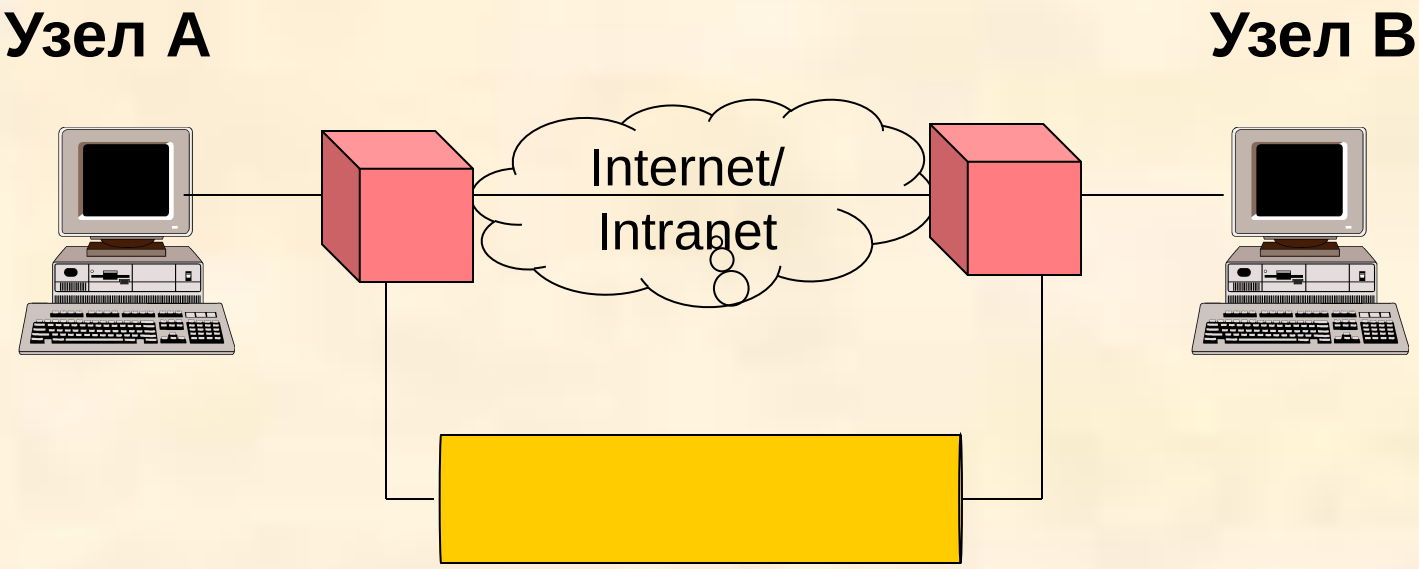
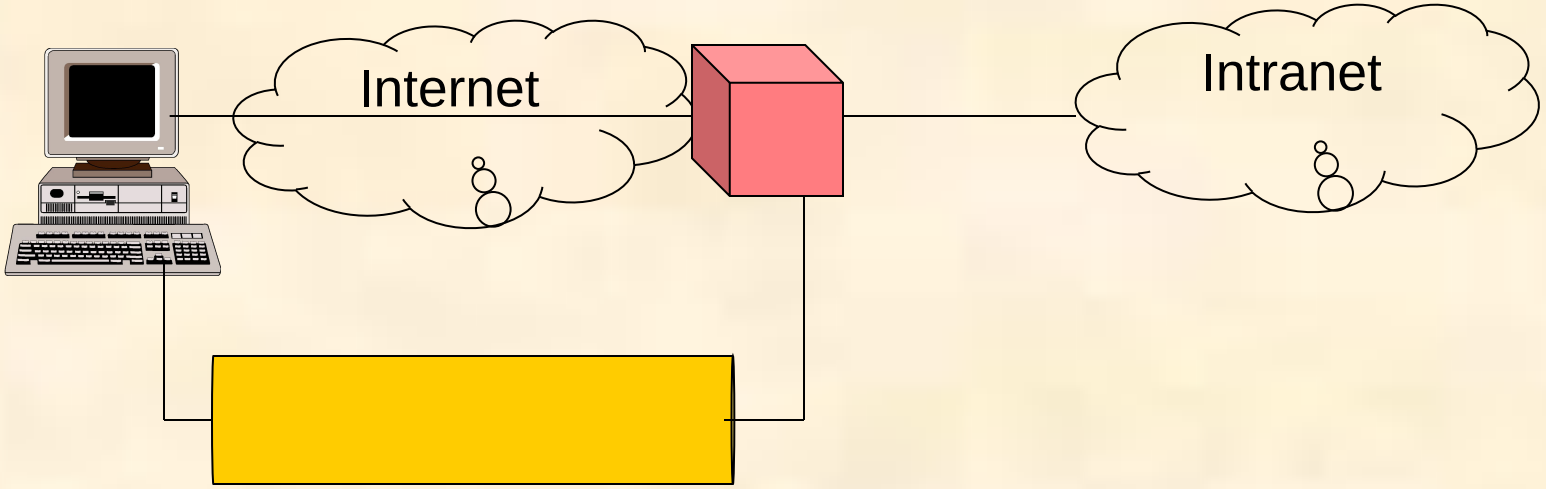


Схема шлюз-шлюз

Схемы применения IPSec

Узел А

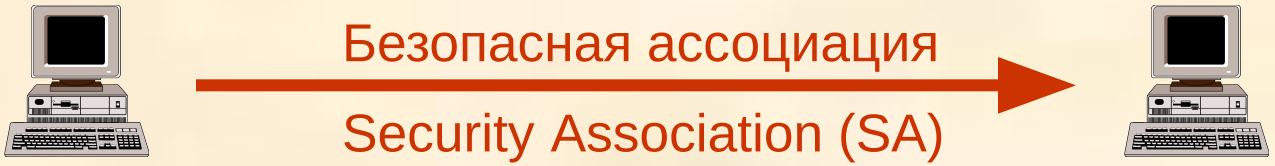


Смешанная схема

Протокол IKE

- **Согласование алгоритмов шифрования и характеристик ключей, которые будут использоваться в защищенном сеансе;**
- **Непосредственный обмен ключами (в том числе возможность их частой смены);**
- **Контроль выполнения всех достигнутых соглашений.**

Протокол IKE



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

Безопасная ассоциация

Безопасная ассоциация IPSec

32-разрядный индекс (SPI)

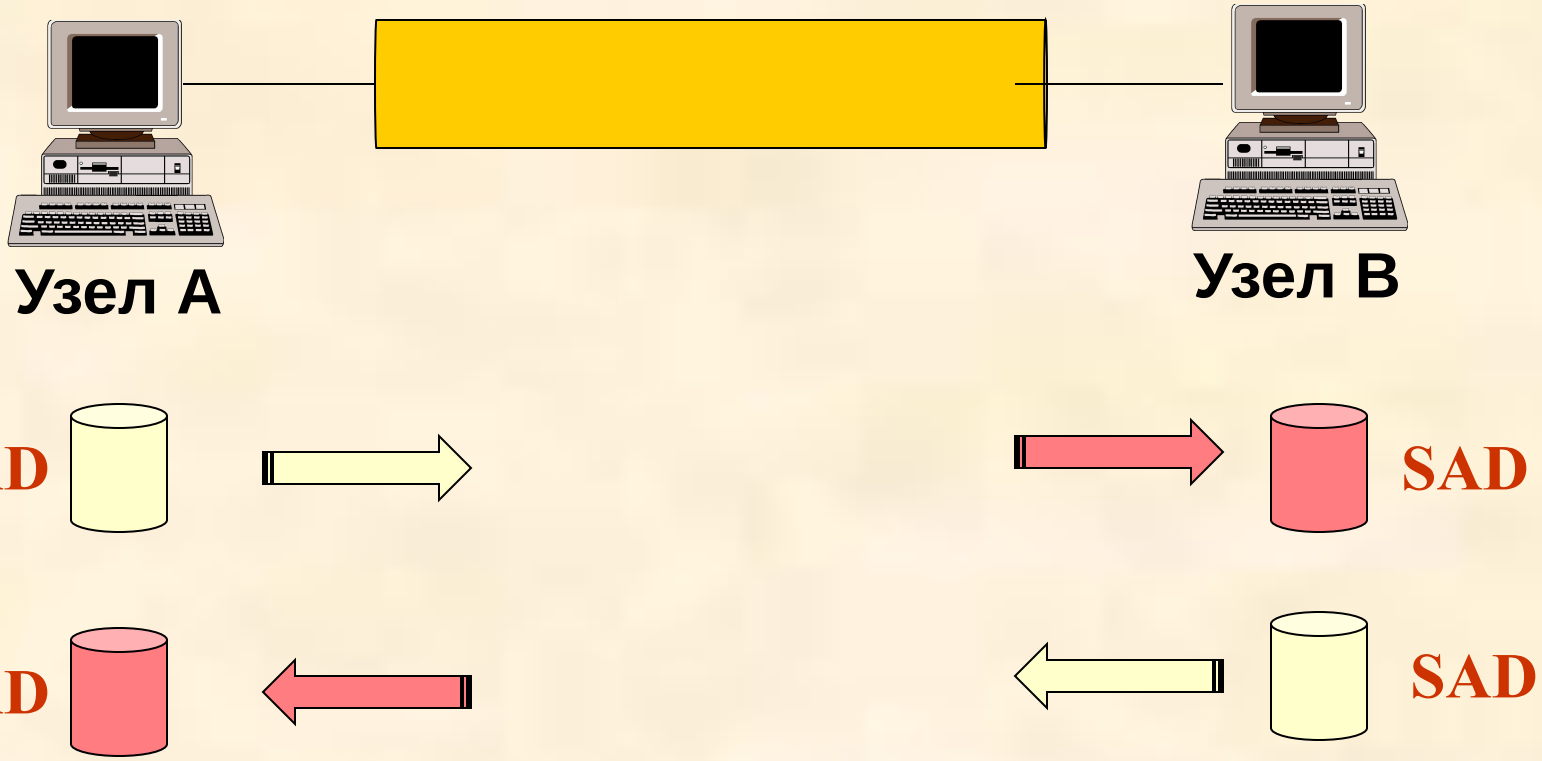
Узел A **Узел B**

IP- адрес узла назначения

SA SA

Идентификатор протокола защиты
(AH или ESP)

Безопасная ассоциация IPSec



Базы данных SA

Протокол IKE

Фаза 1

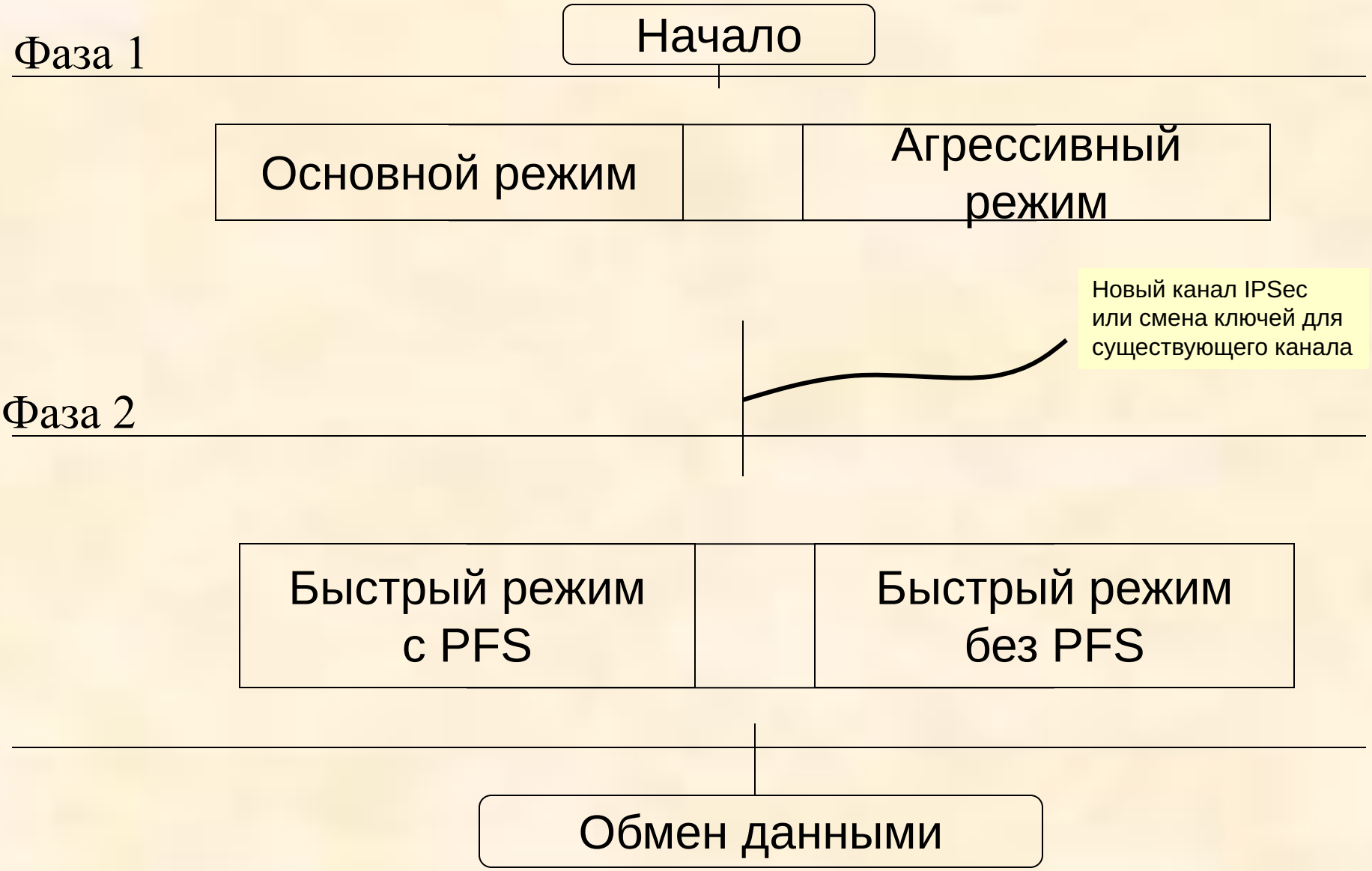
- Установление защищенного соединения для процедуры обмена (IKE SA)

Фаза 2

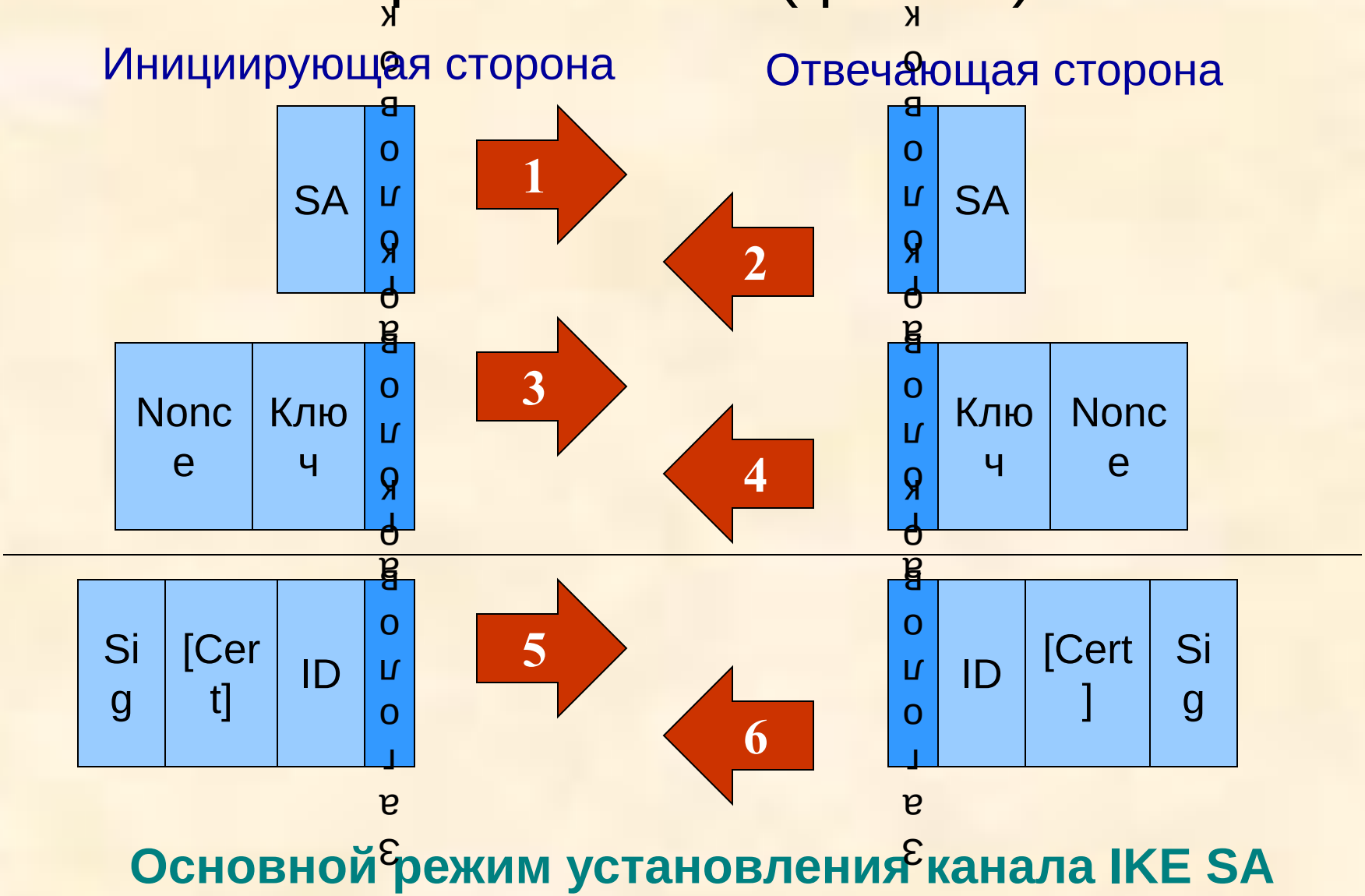
- Согласование параметров SA для защиты канала данных

Этапы функционирования протокола IKE

Протокол IKE

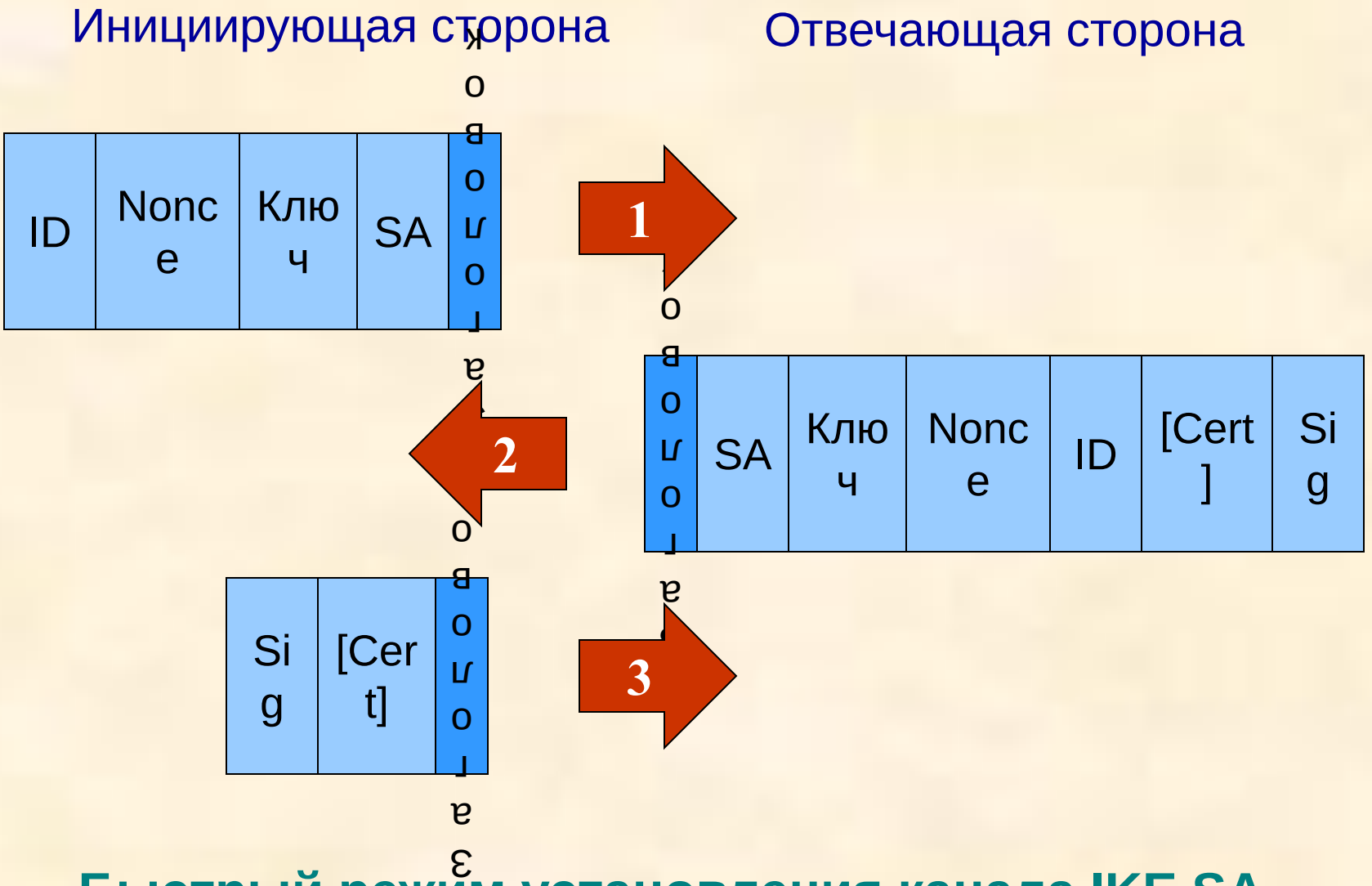


Протокол IKE (фаза 1)



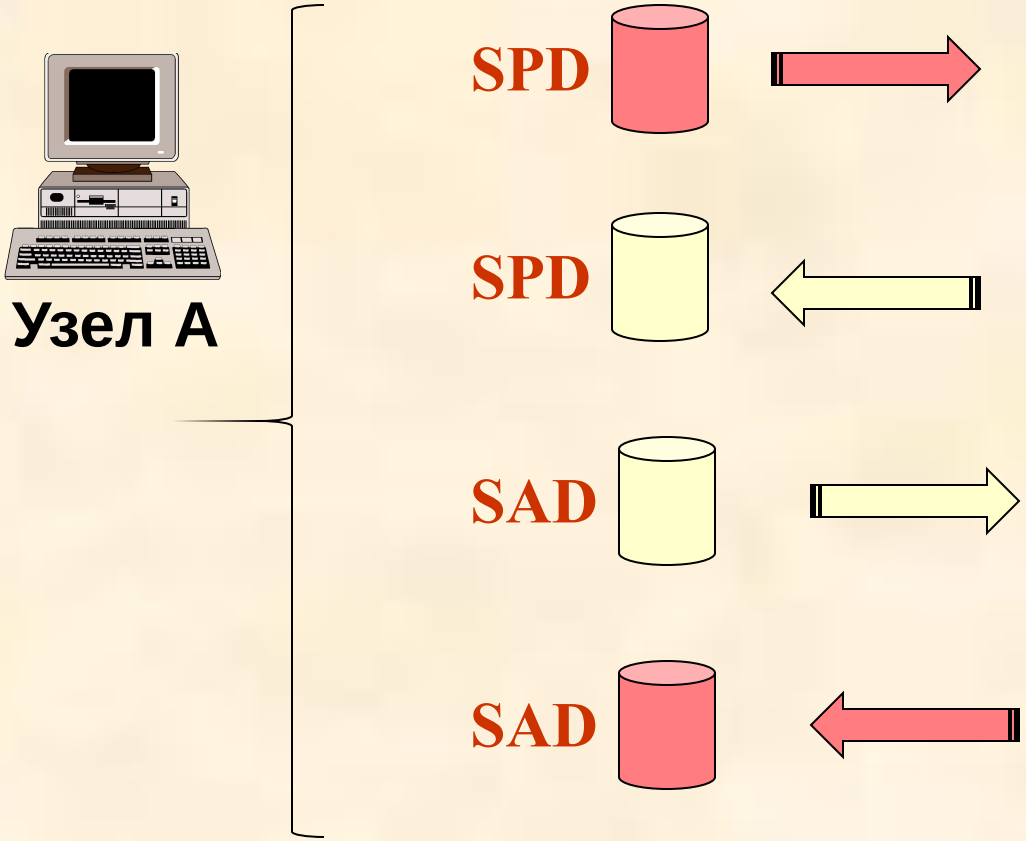
Основной режим установления канала IKE SA

Протокол IKE (фаза 2)



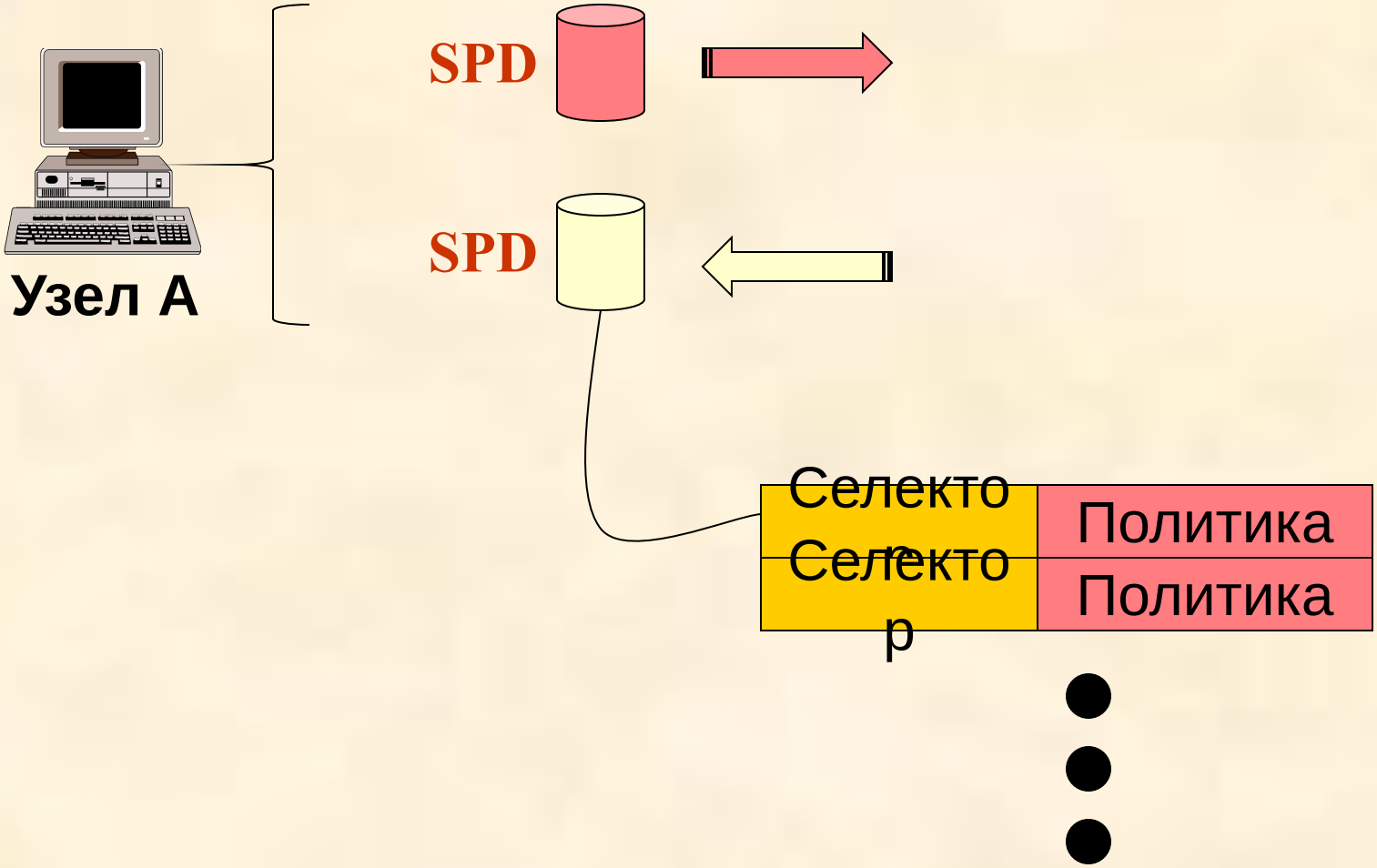
Быстрый режим установления канала IKE SA

Базы данных IPSec

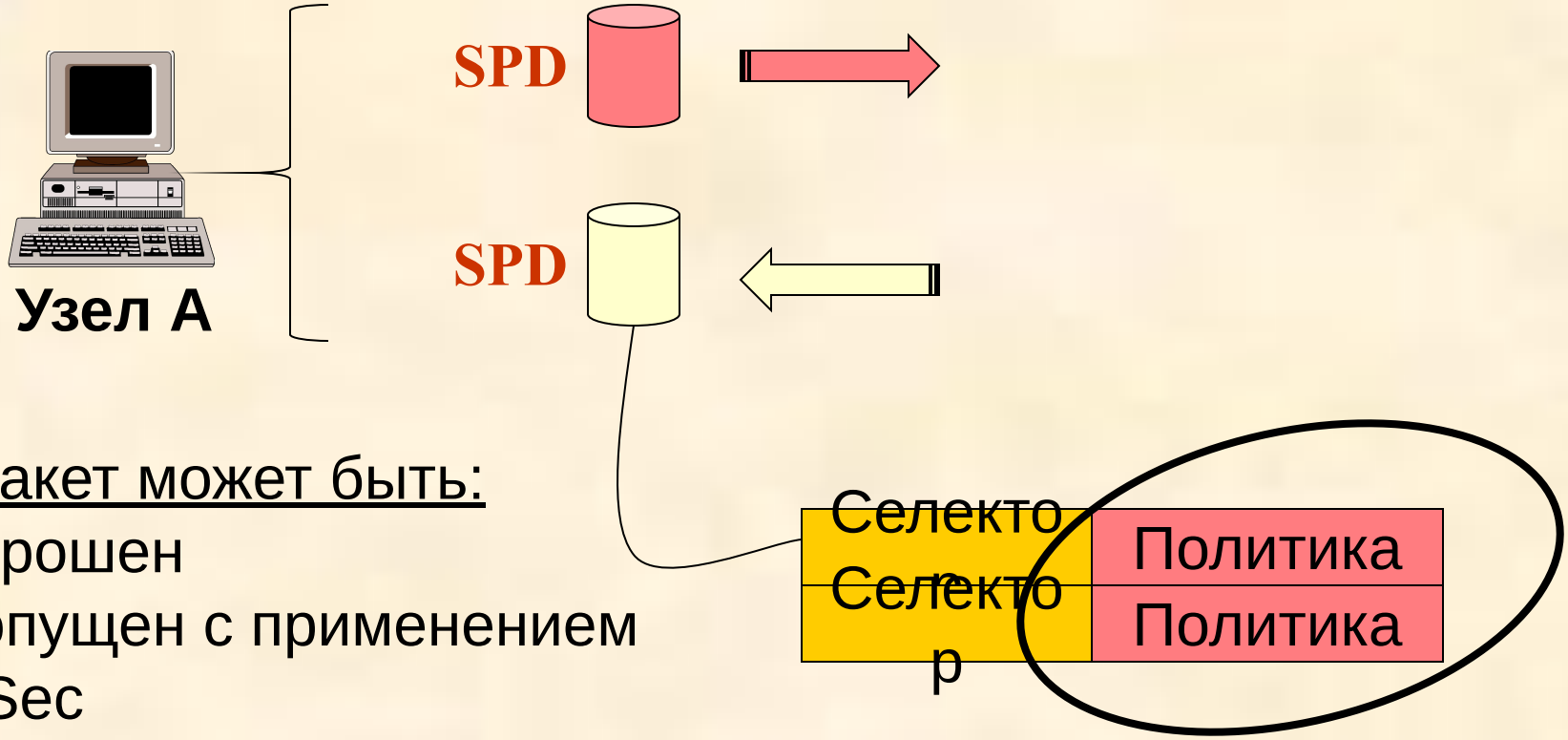


Базы данных SAD и SPD

База данных SPD



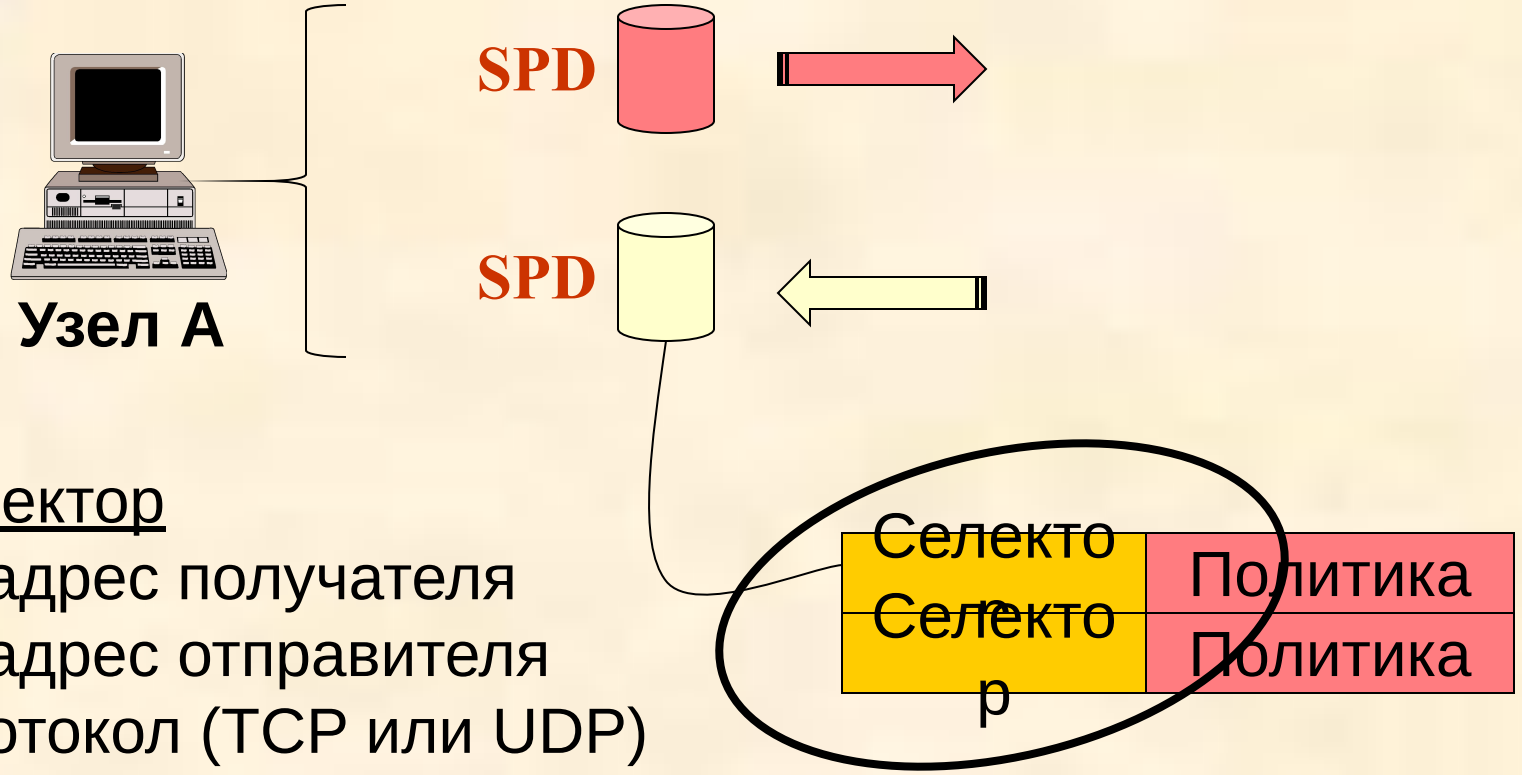
База данных SPD



IP-пакет может быть:

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

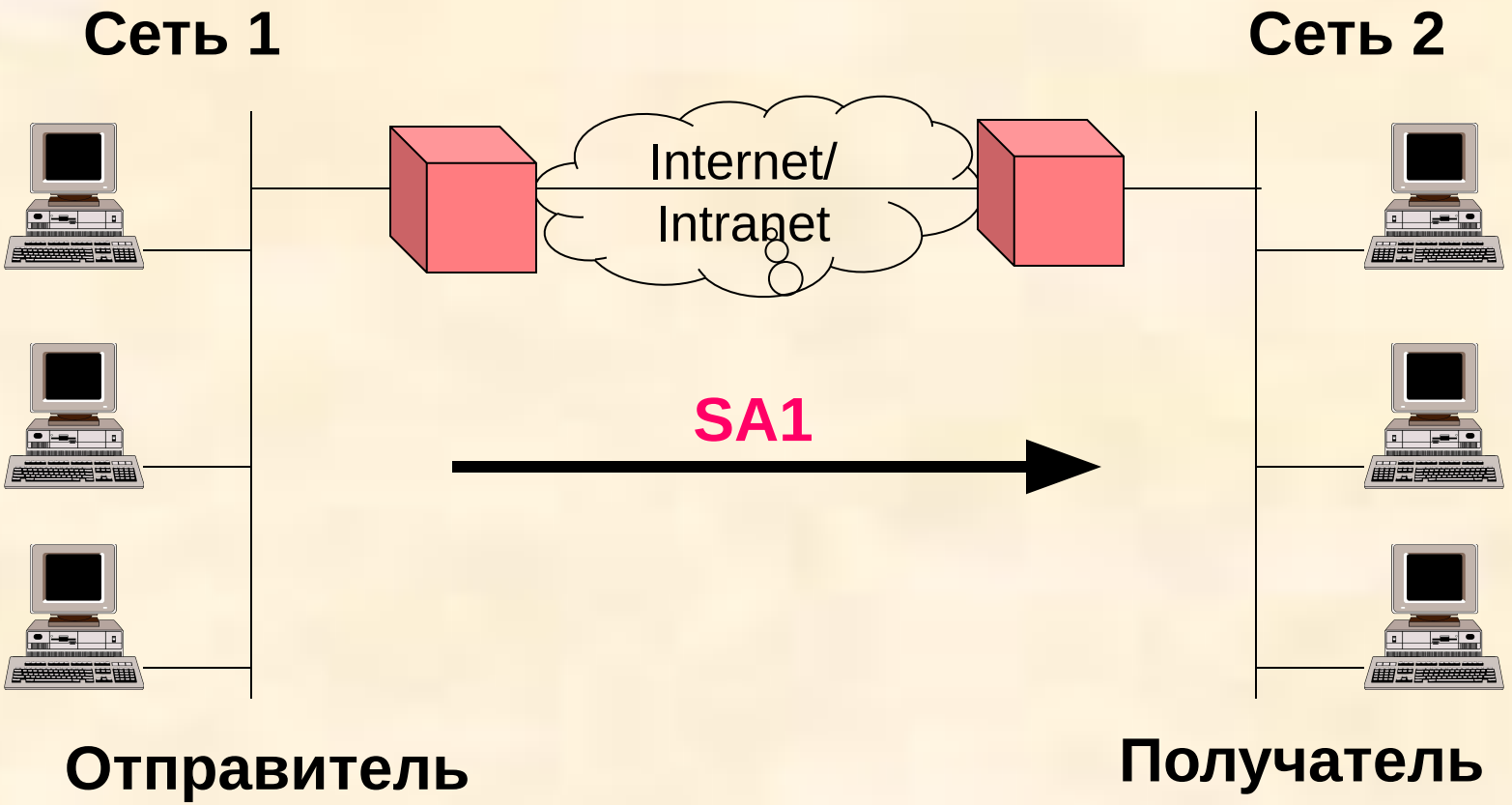
База данных SPD



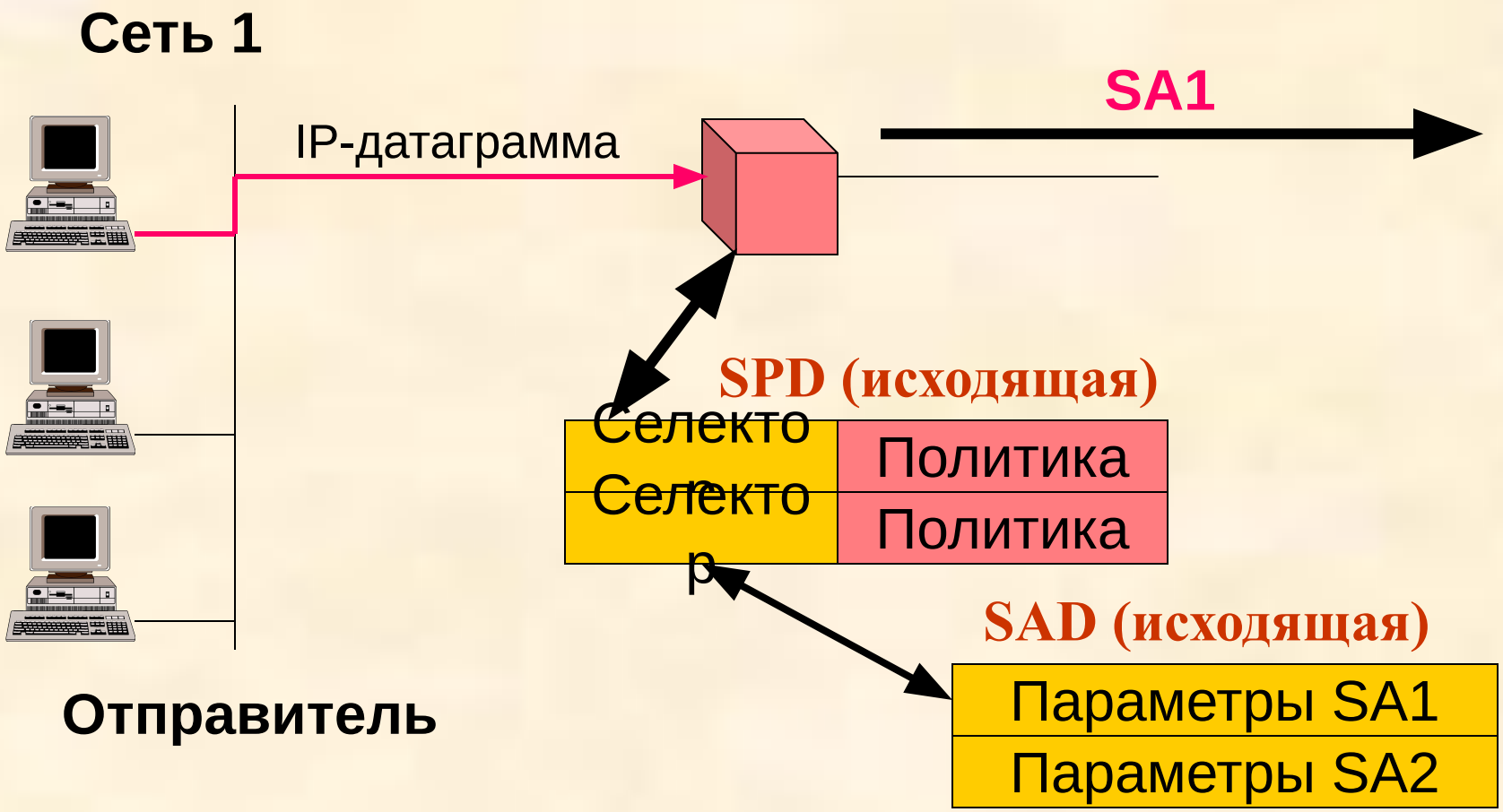
Селектор

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

Пример работы IPSec

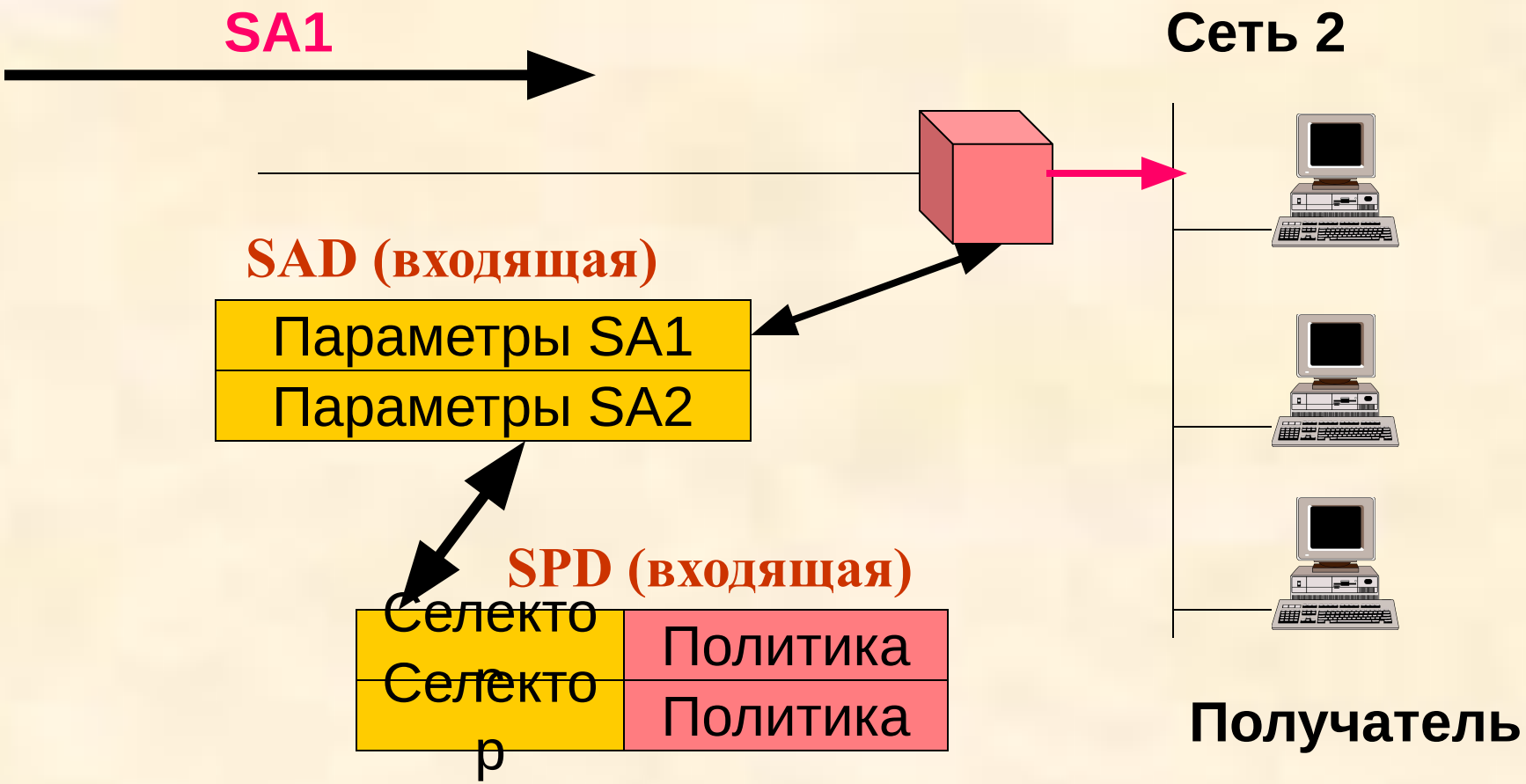


Пример работы IPSec



Отправка пакета

Пример работы IPSec



Получение пакета

Практическая работа 9
Настройка IPSec

Настройка IPSec средствами ОС Windows 2000