

# Протокол IPSec

**(RFC 2401)**

# Семейство протоколов IPSec

## **Протокол Authentication Header (AH)**

Аутентификация  
Контроль целостности

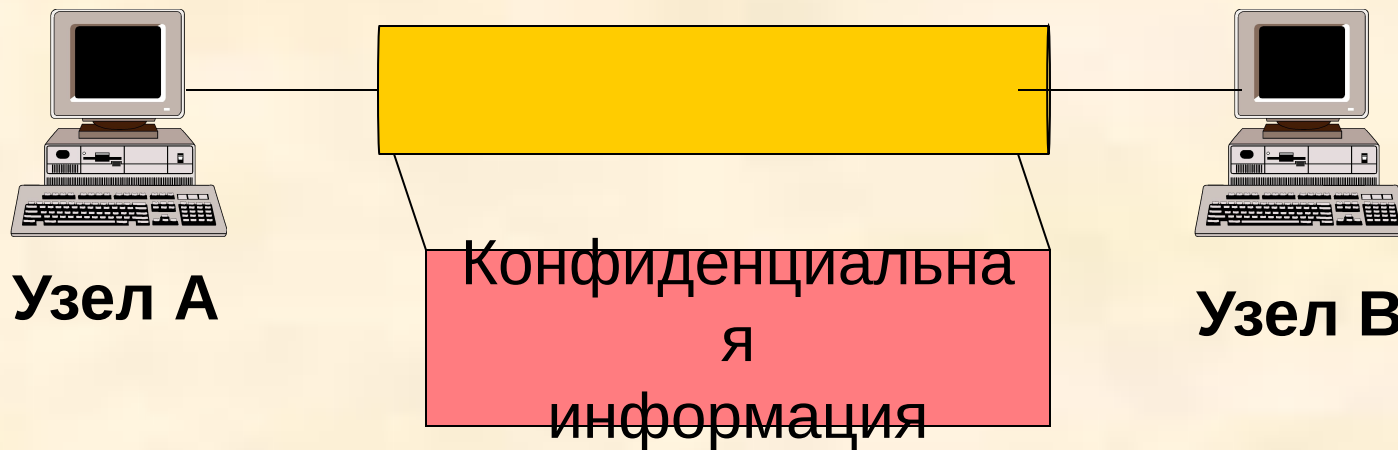
## **Протокол Encapsulated Security Payload (ESP)**

Аутентификация  
Контроль целостности  
Шифрование

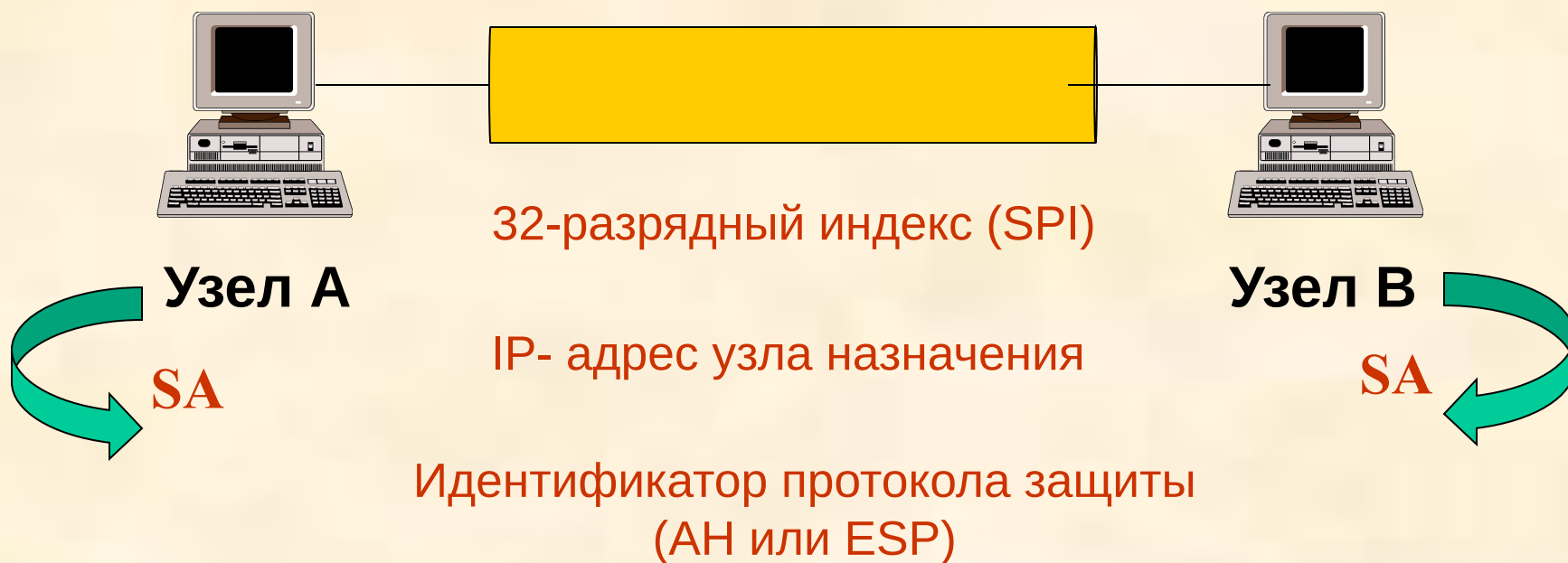
## **Протокол Internet Key Exchange (IKE)**

Согласование алгоритмов шифрования  
Обмен ключами

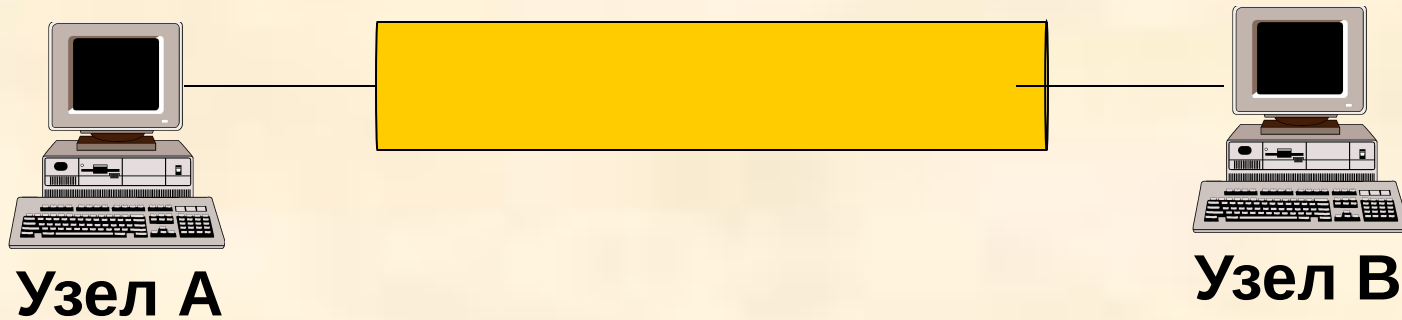
# Защищённый канал IPSec



# Безопасная ассоциация IPSec



# Безопасная ассоциация IPSec

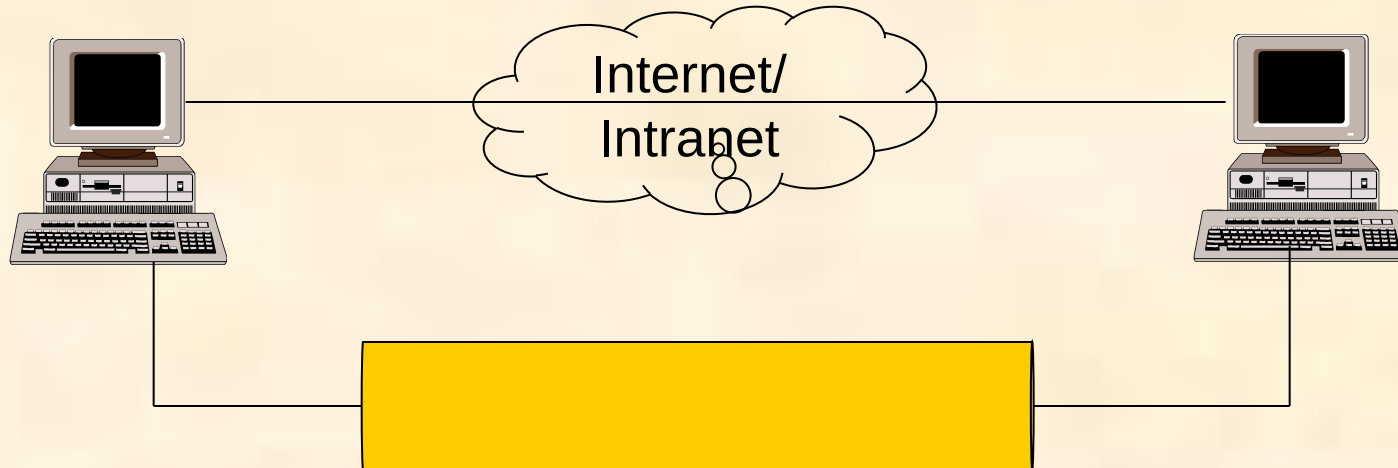


Базы данных SA

# Схемы применения IPSec

**Узел А**

**Узел В**

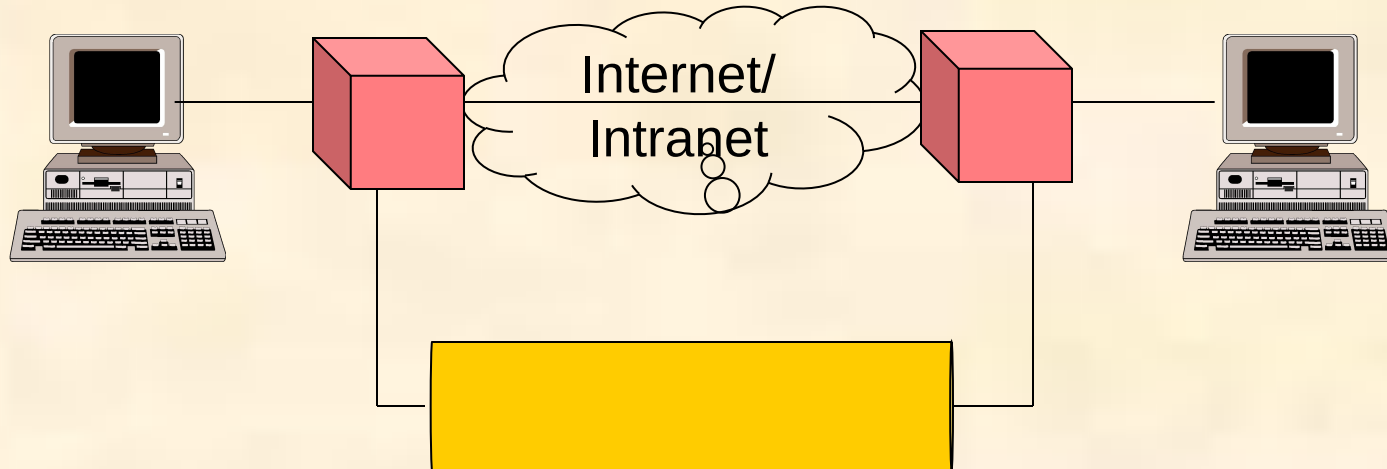


**Схема узел-узел (точка-точка)**

# Схемы применения IPSec

**Узел А**

**Узел В**

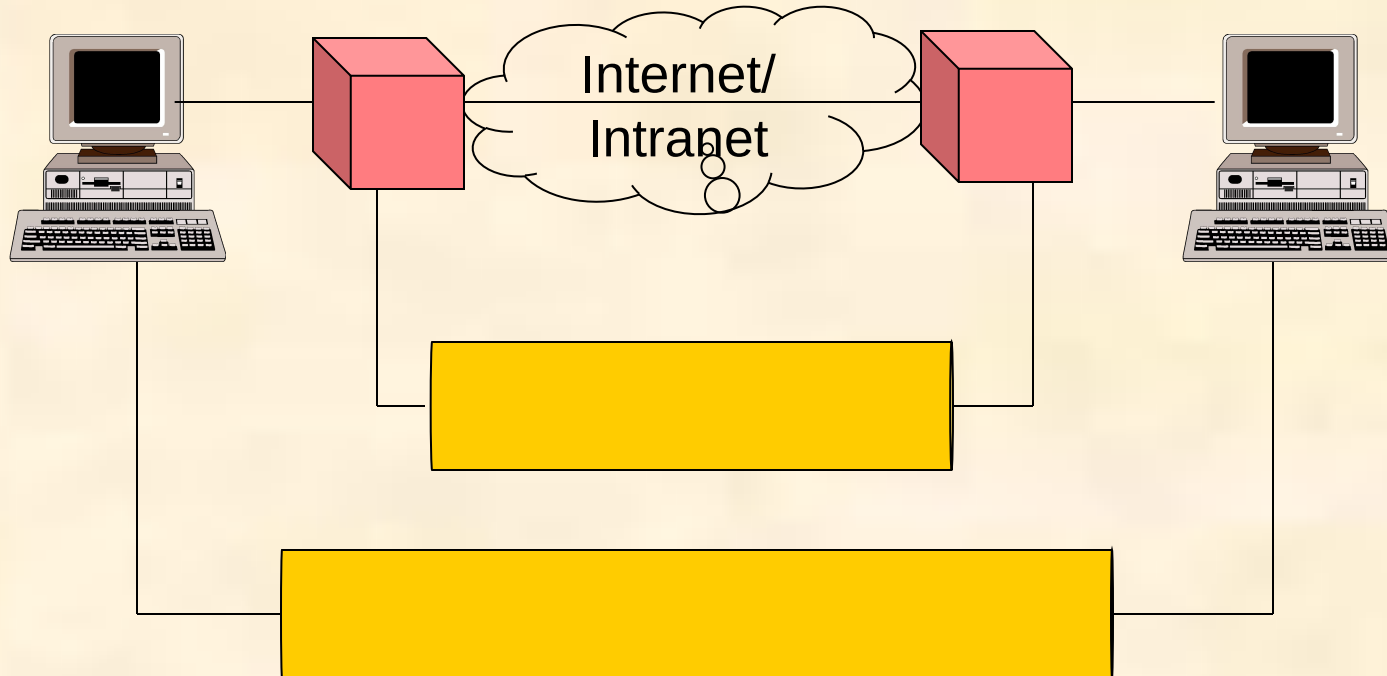


**Схема шлюз-шлюз**

# Схемы применения IPSec

Узел А

Узел В



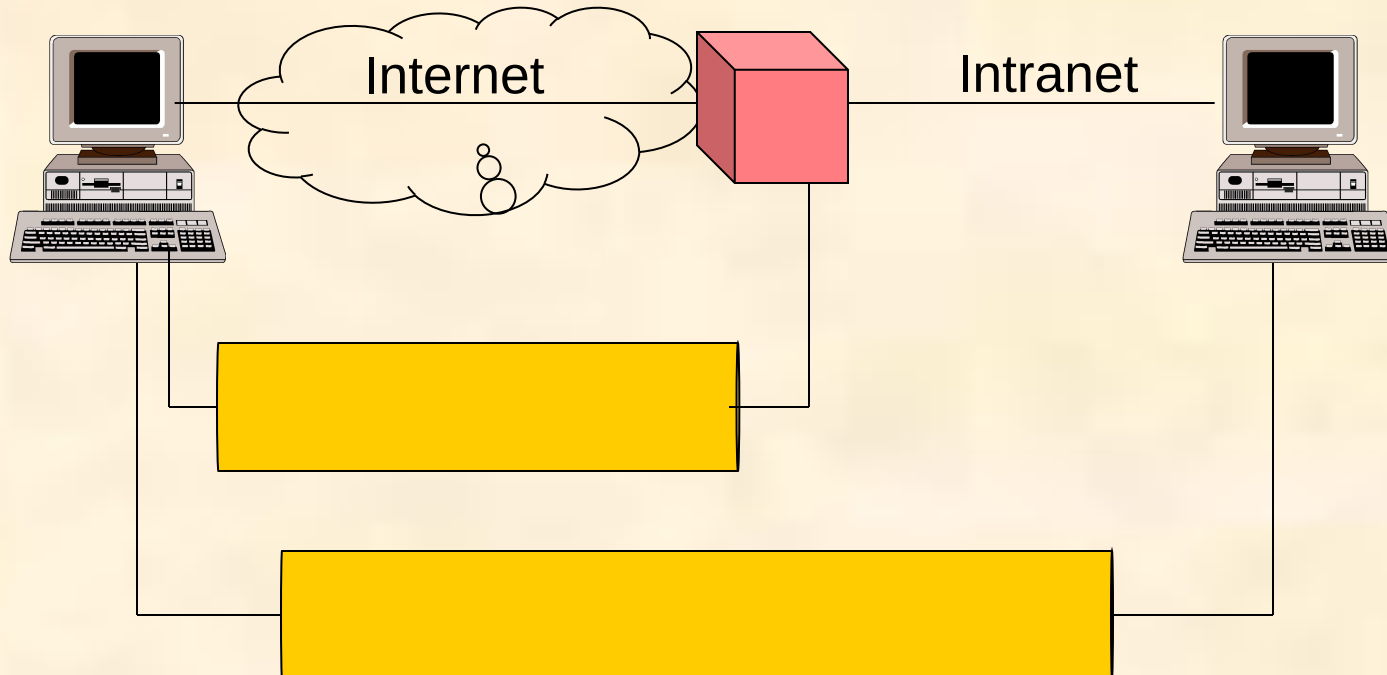
Смешанная схема (вариант 1)



# Схемы применения IPSec

Узел А

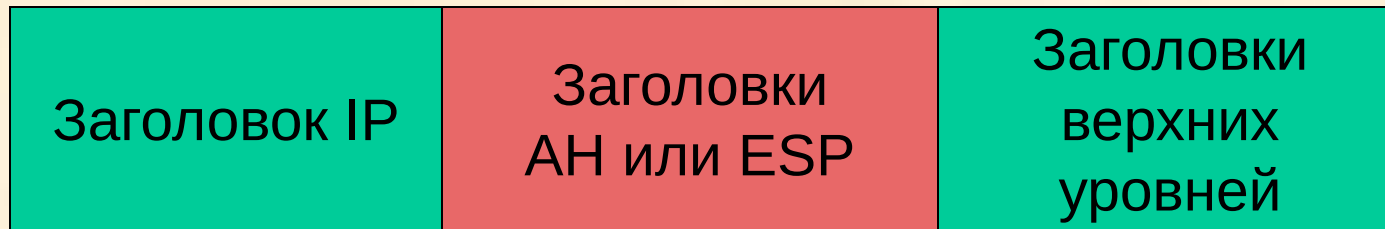
Узел В



Смешанная схема (вариант 2)

# Режимы работы IPSec

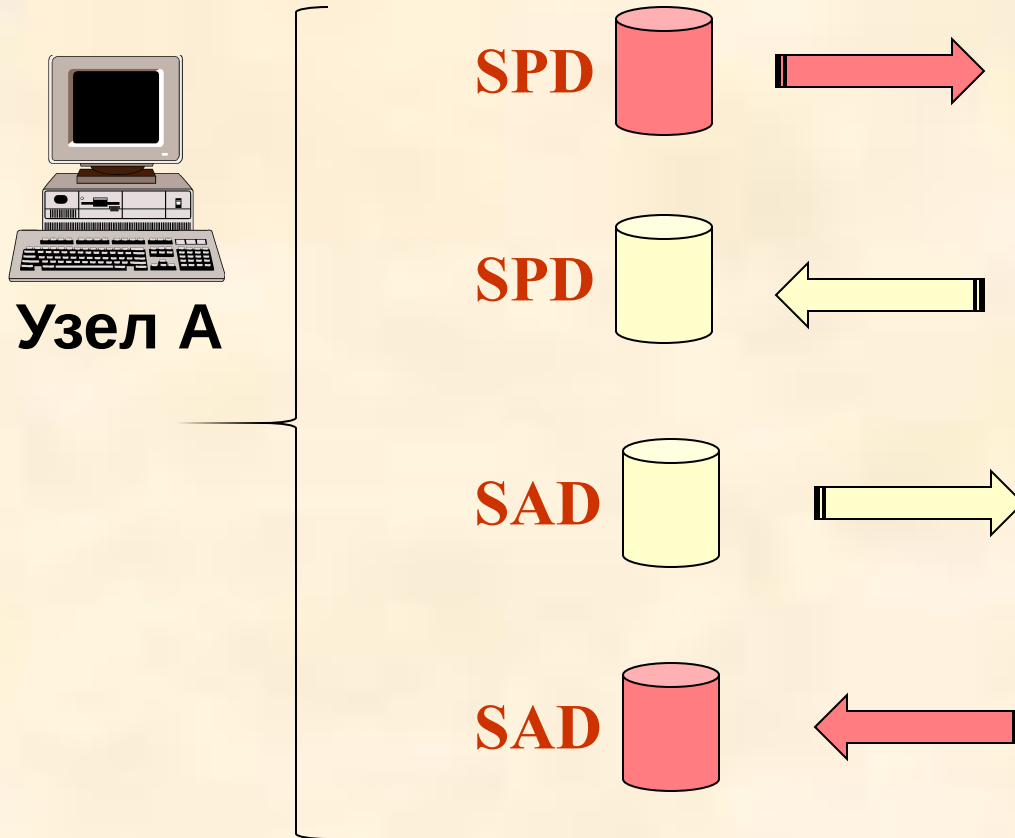
## Транспортный режим



## Туннельный режим

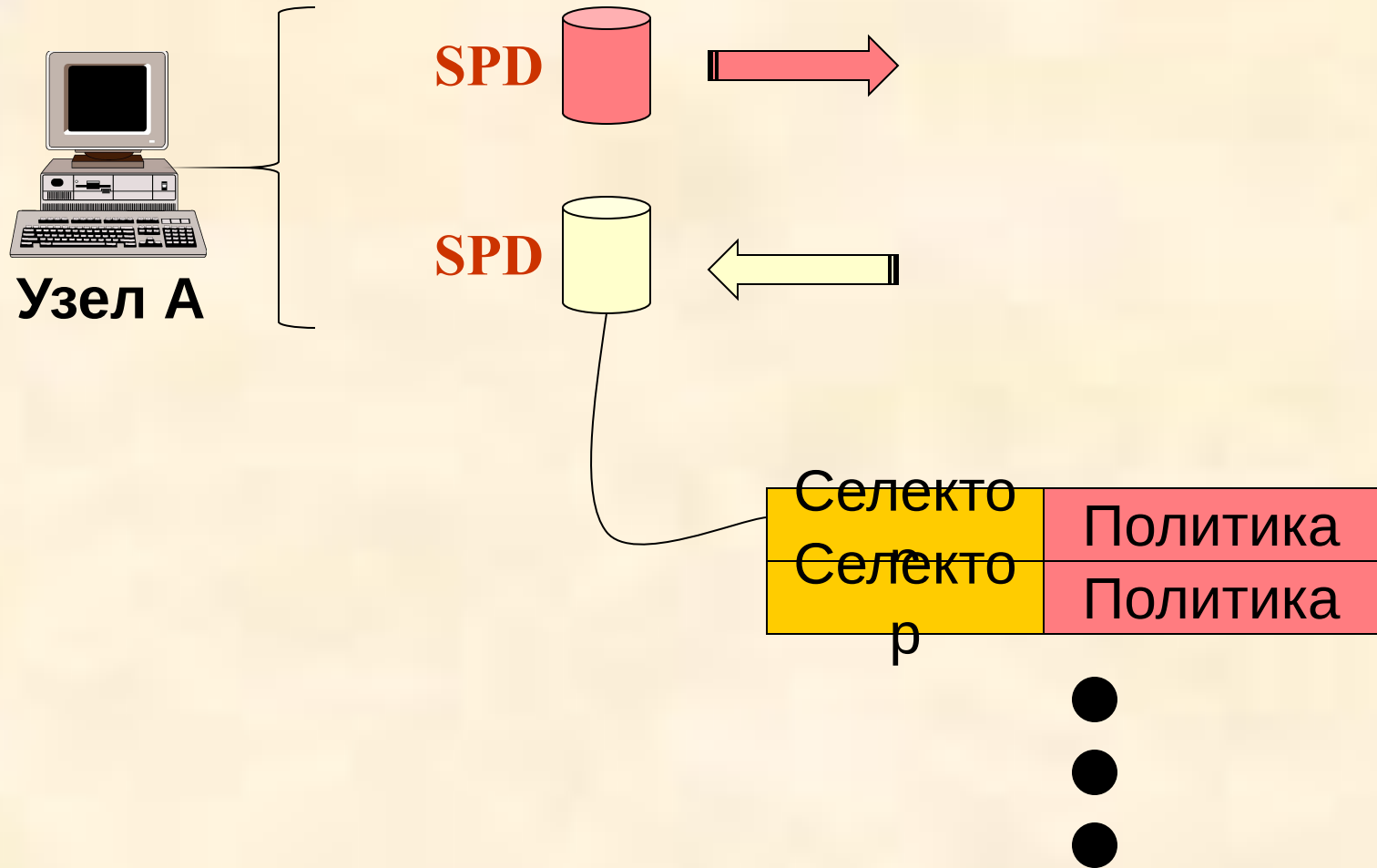


# Базы данных IPSec

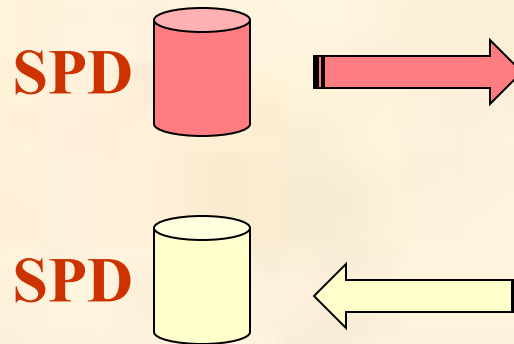
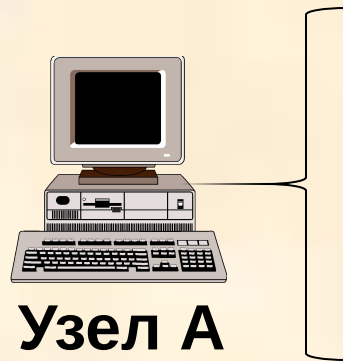


Базы данных SAD и SPD

# База данных SPD

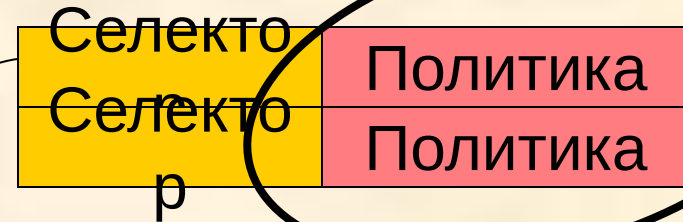


# База данных SPD

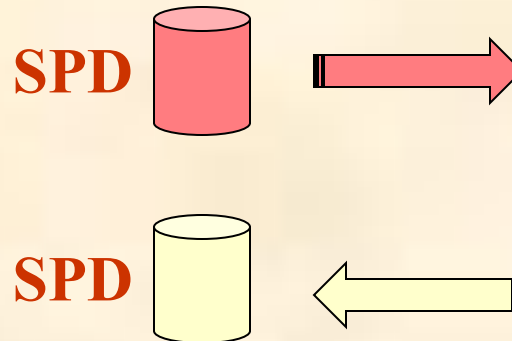
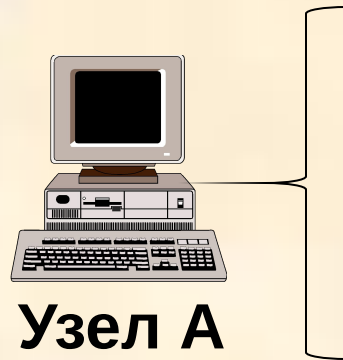


## IP-пакет может быть:

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

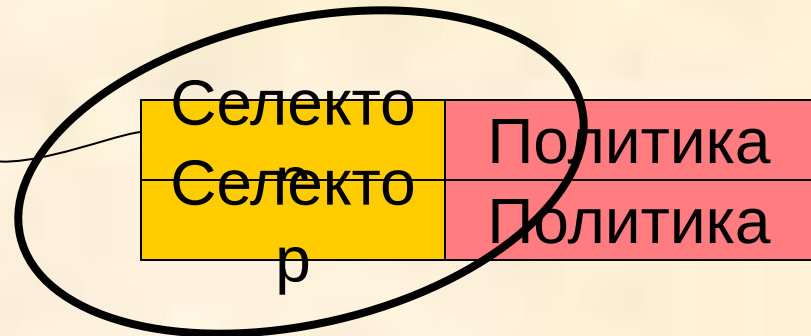


# База данных SPD

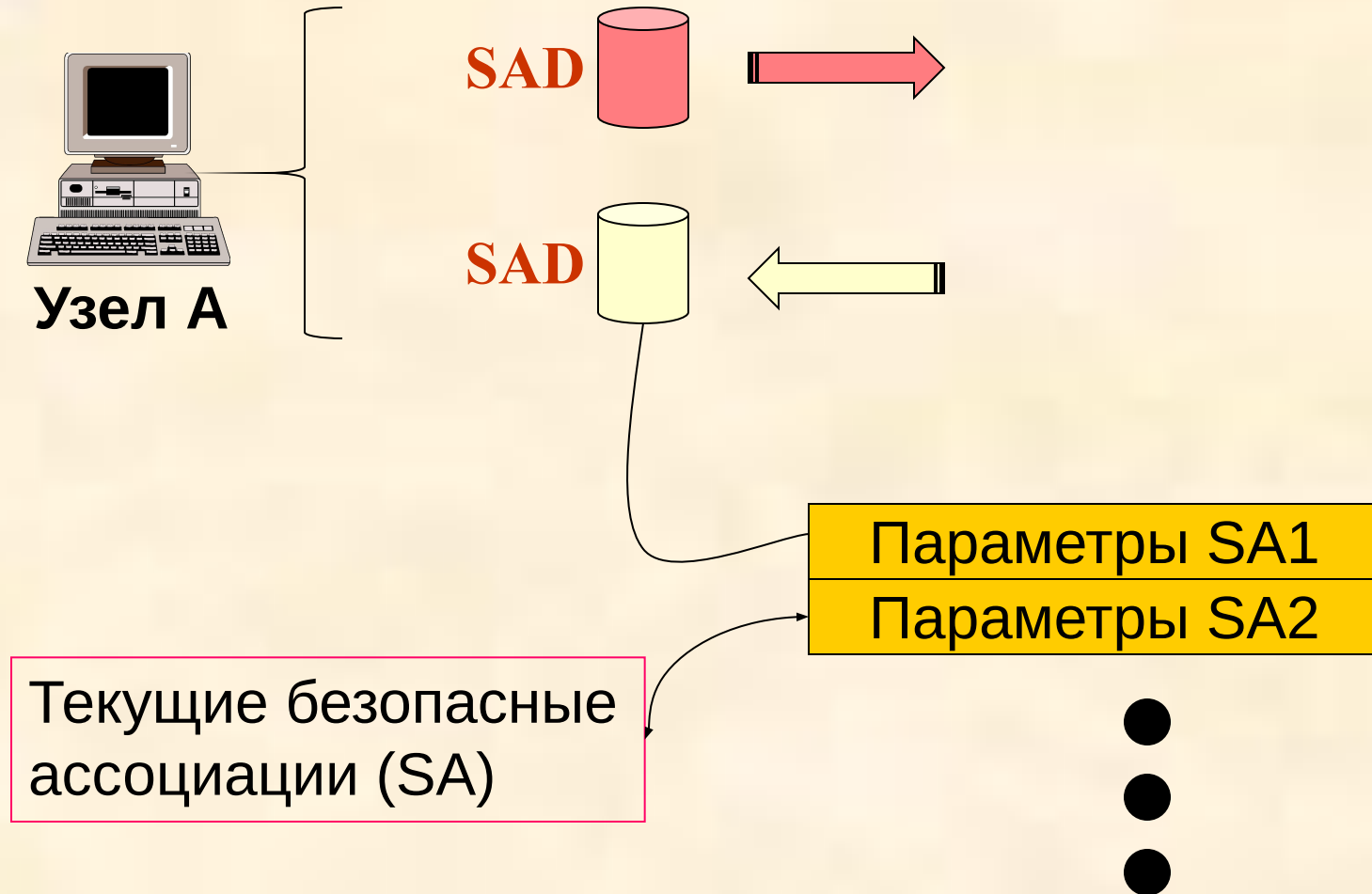


## Селектор

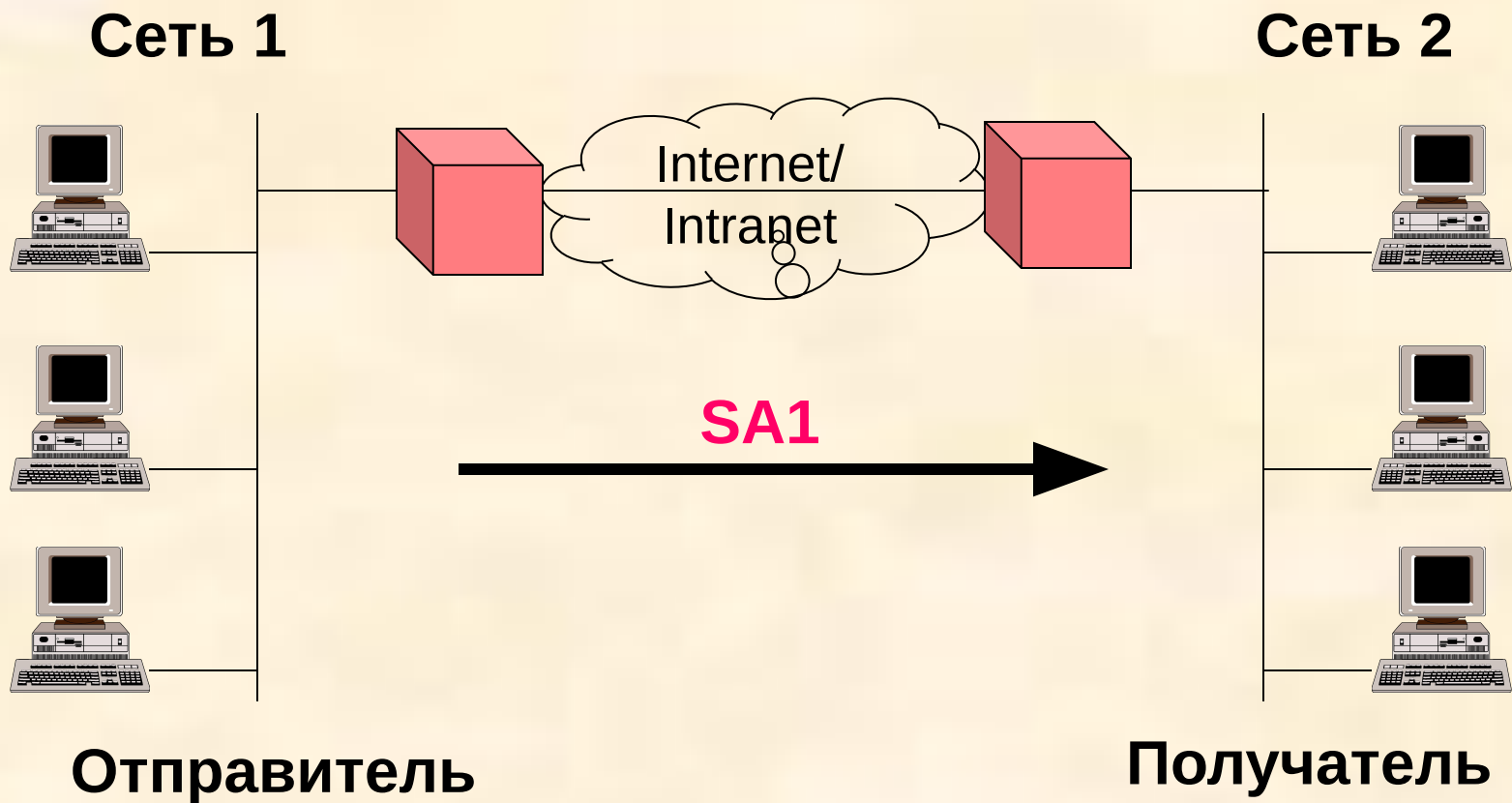
- IP-адрес получателя
- IP-адрес отправителя
- Протокол (TCP или UDP)
- Имя FQDN или X.500
- Порт отправителя
- Порт получателя



# База данных SAD

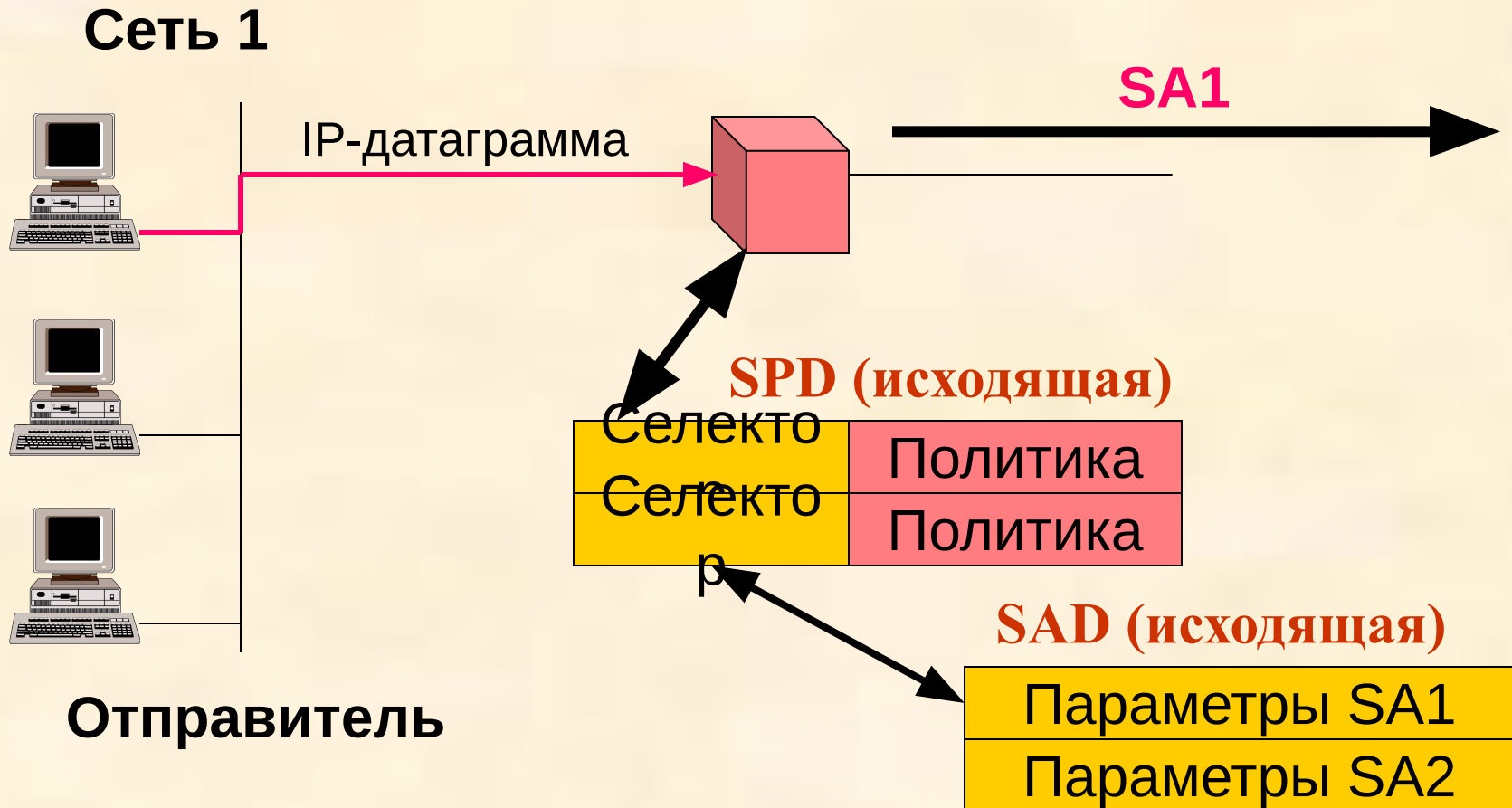


# Пример работы IPSec



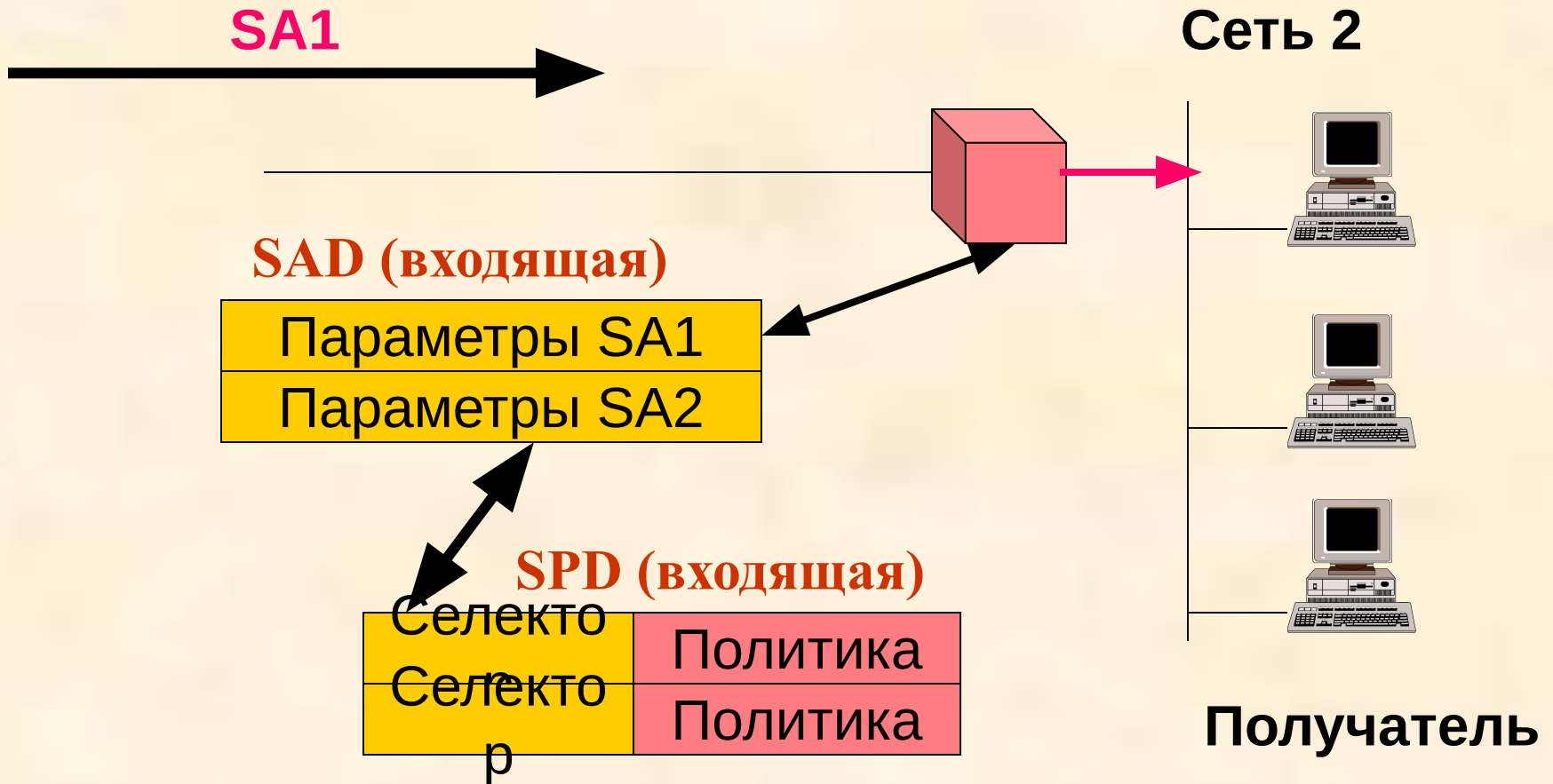


# Пример работы IPSec



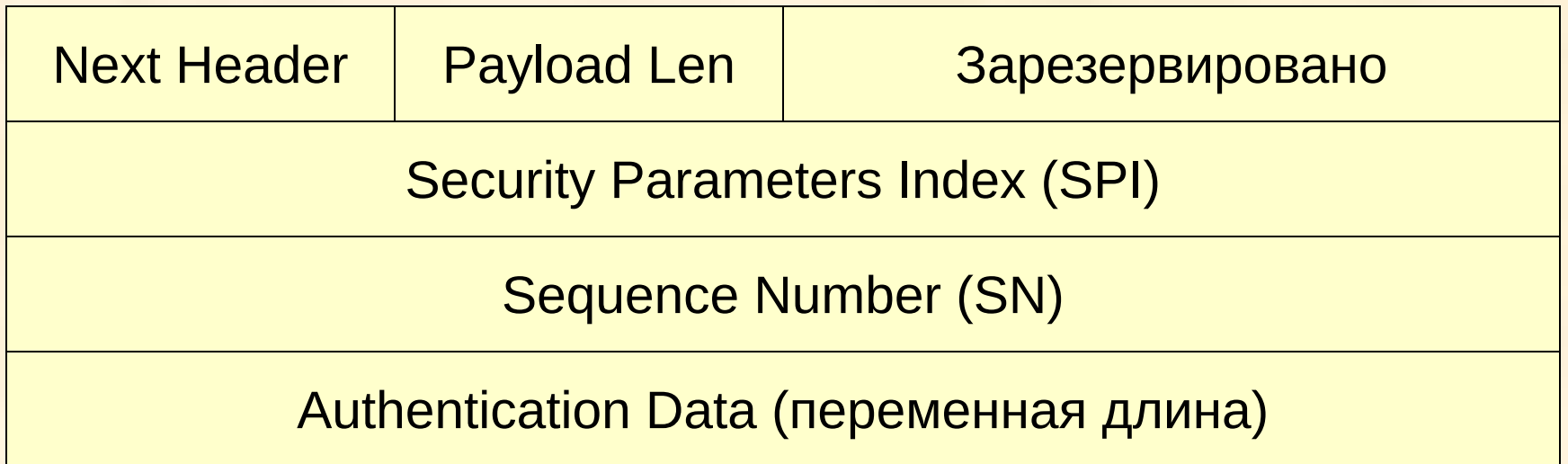
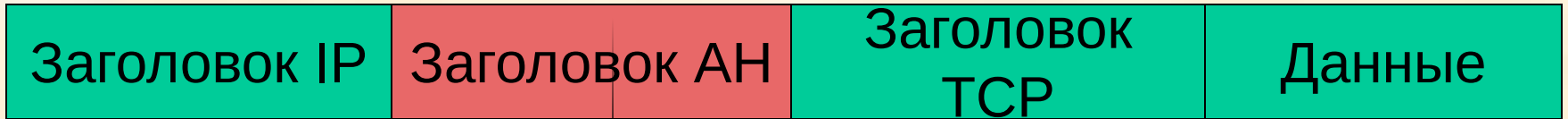
Отправка пакета

# Пример работы IPSec



Получение пакета

# Протокол АН



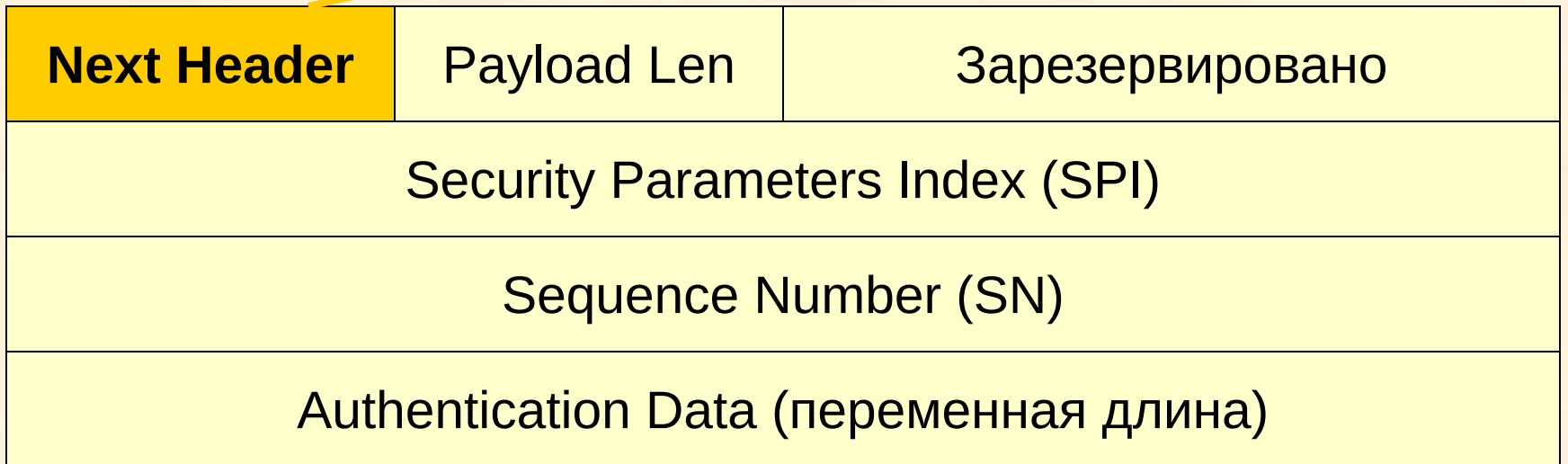
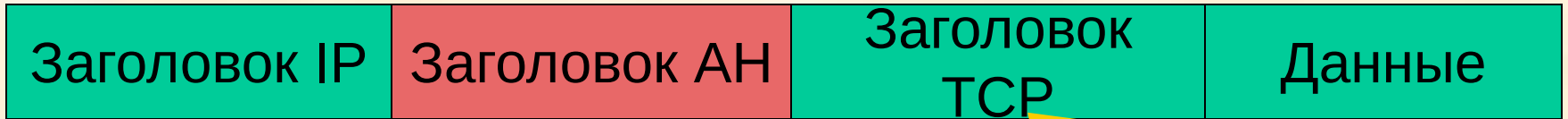
0

8

16

31

# Протокол АН



0                                      8                                      16                                      31

**Поле Next Header**

# Протокол АН

Длина

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

0

8

16

31

**Поле Payload Len**

# Протокол АН



Метка безопасной ассоциации

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

0

8

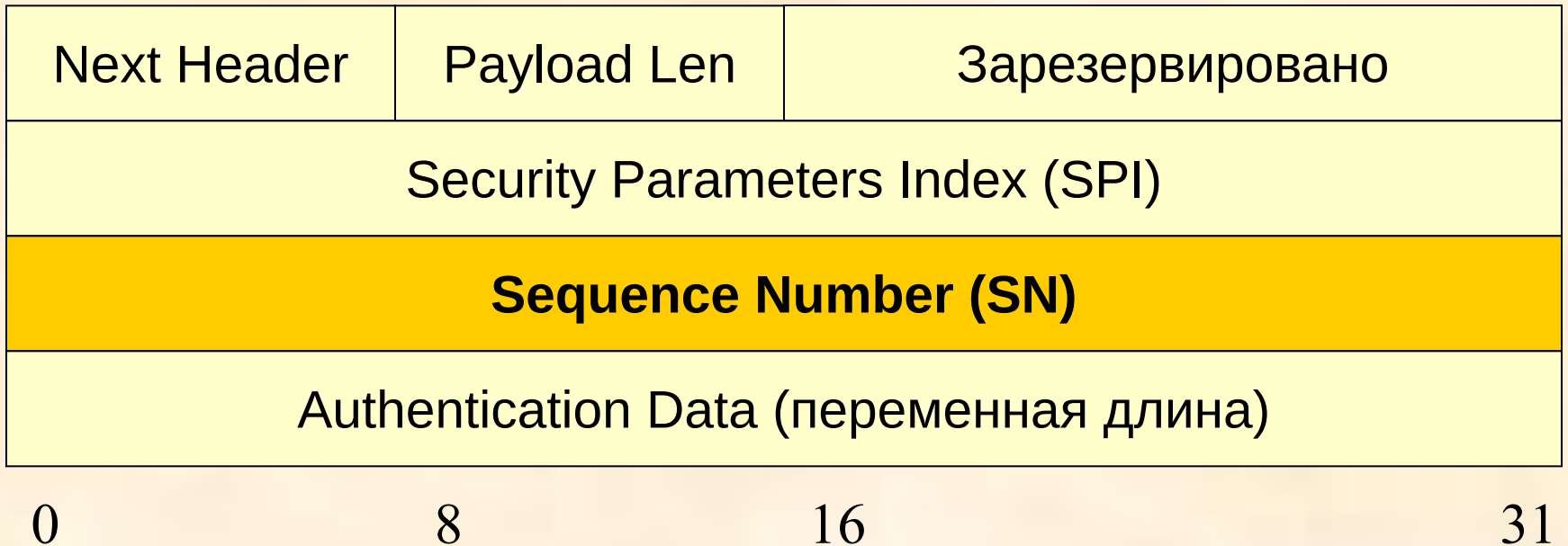
16

31

**Поле SPI**

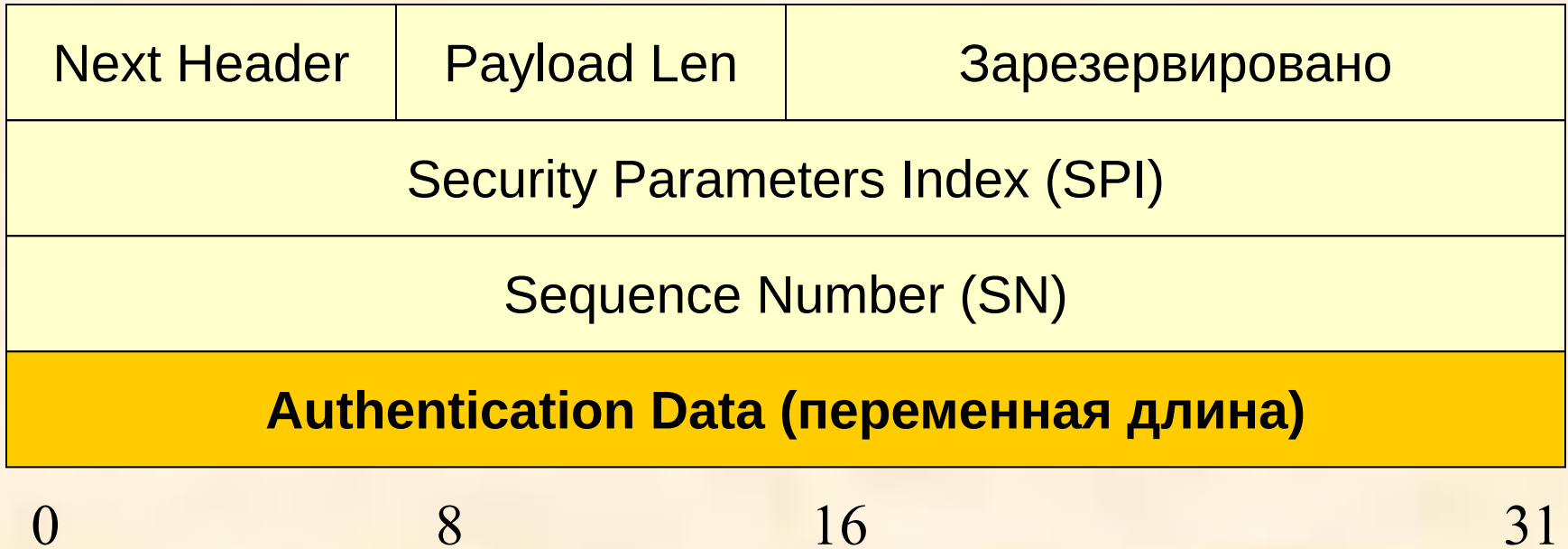
# Протокол АН

└ Нарастивается для каждого  
следующего пакета



**Поле SN**

# Протокол АН

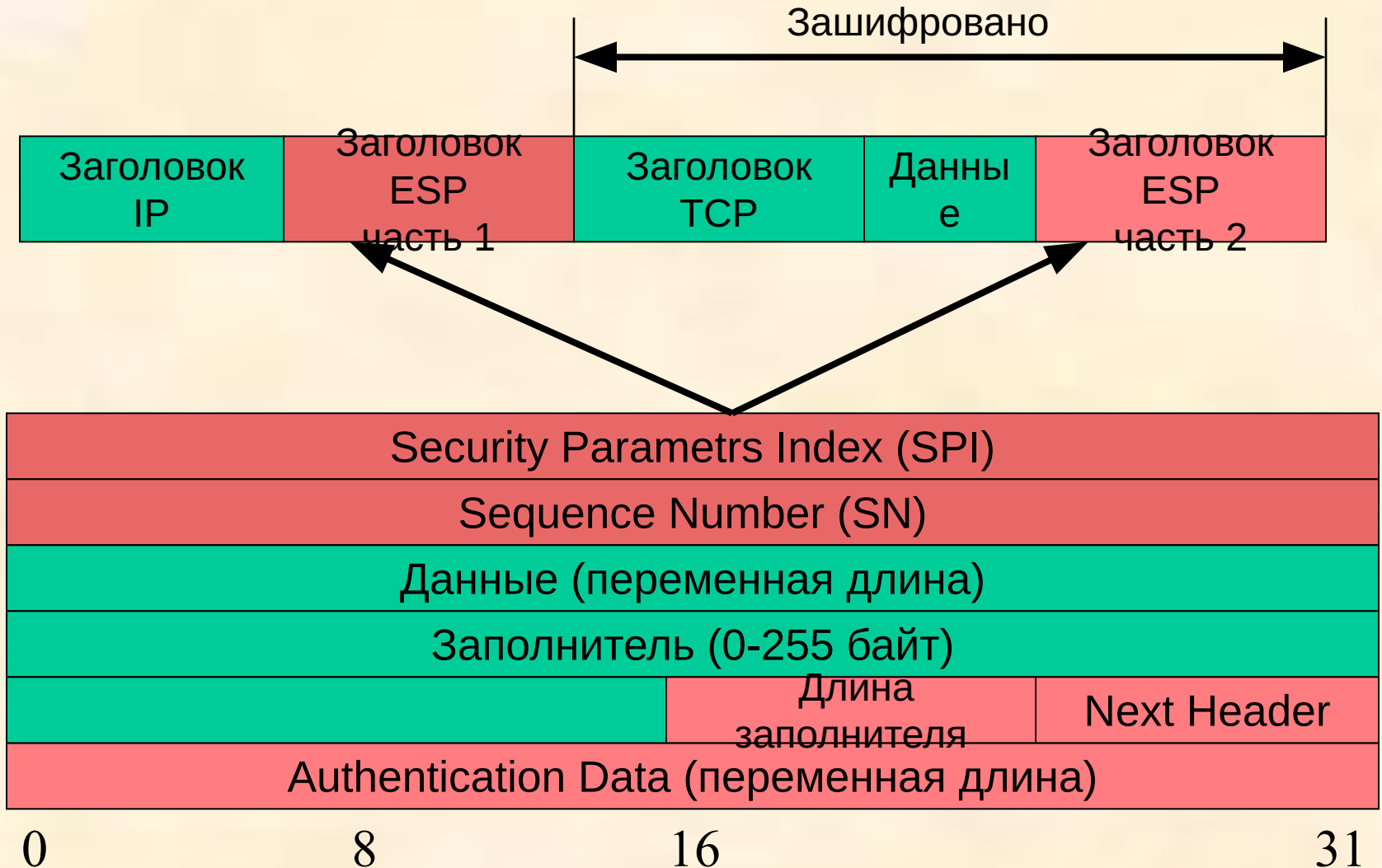


хэш-функция (содержимое пакета,  
симметричный секретный ключ)

**Поле Authentication Data**



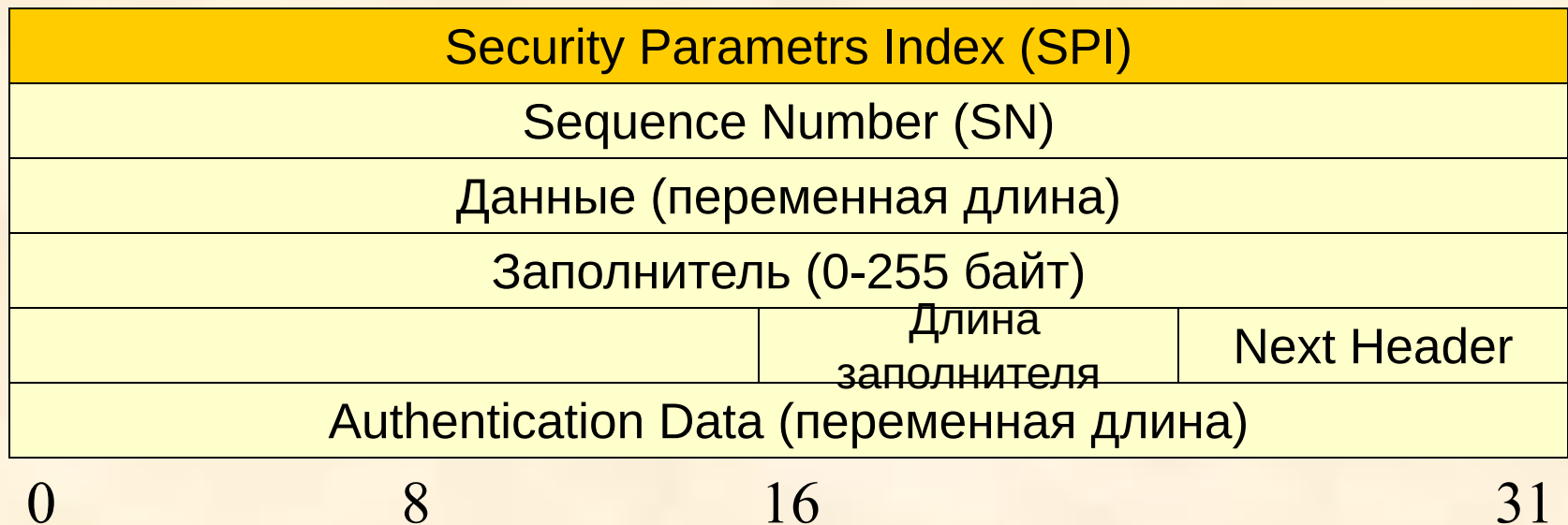
# Протокол ESP



# Протокол ESP



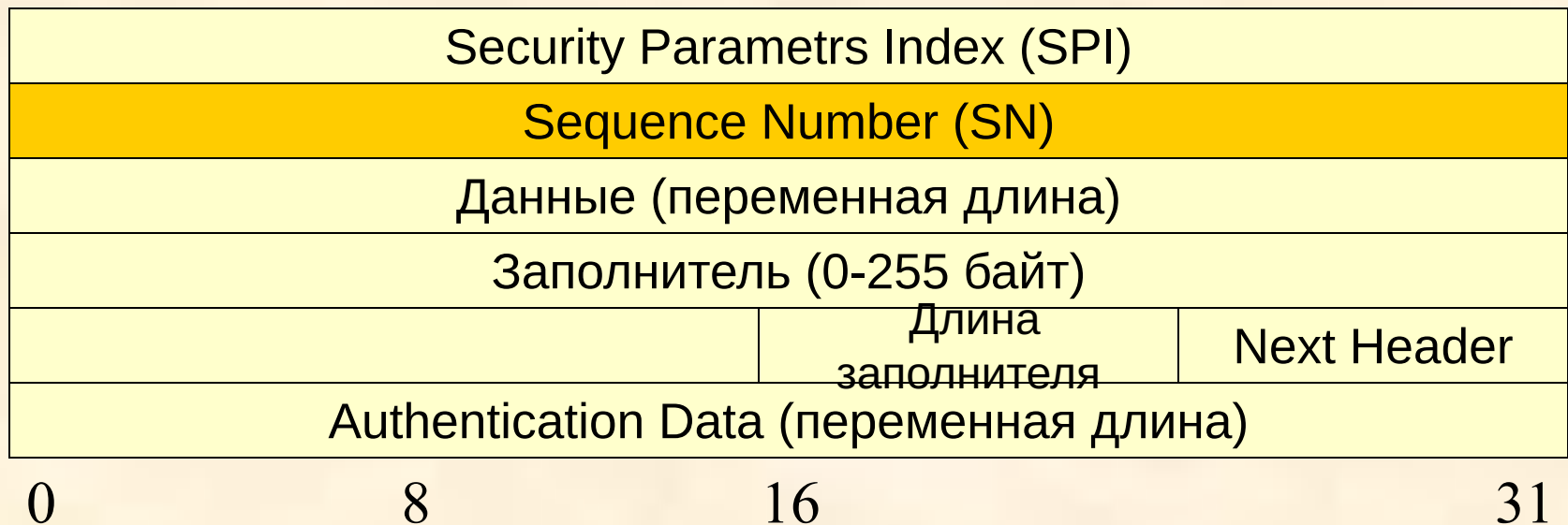
Метка безопасной ассоциации



Поле SPI

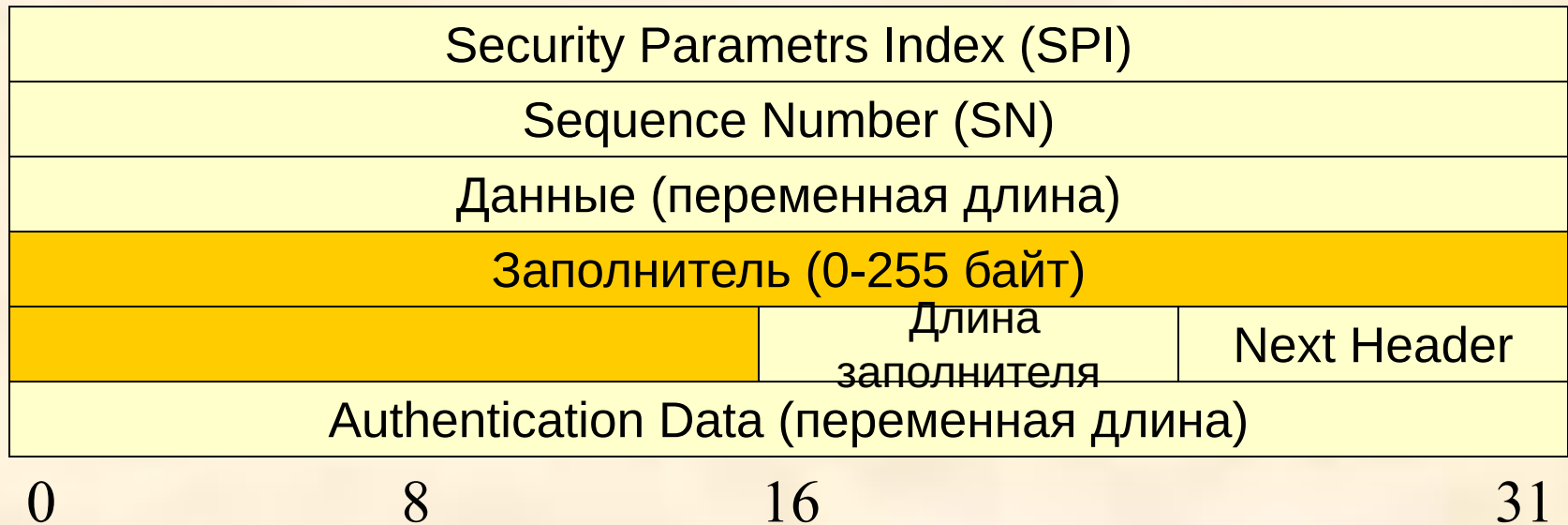
# Протокол ESP

- Нарращивается для каждого следующего пакета



**Поле SN**

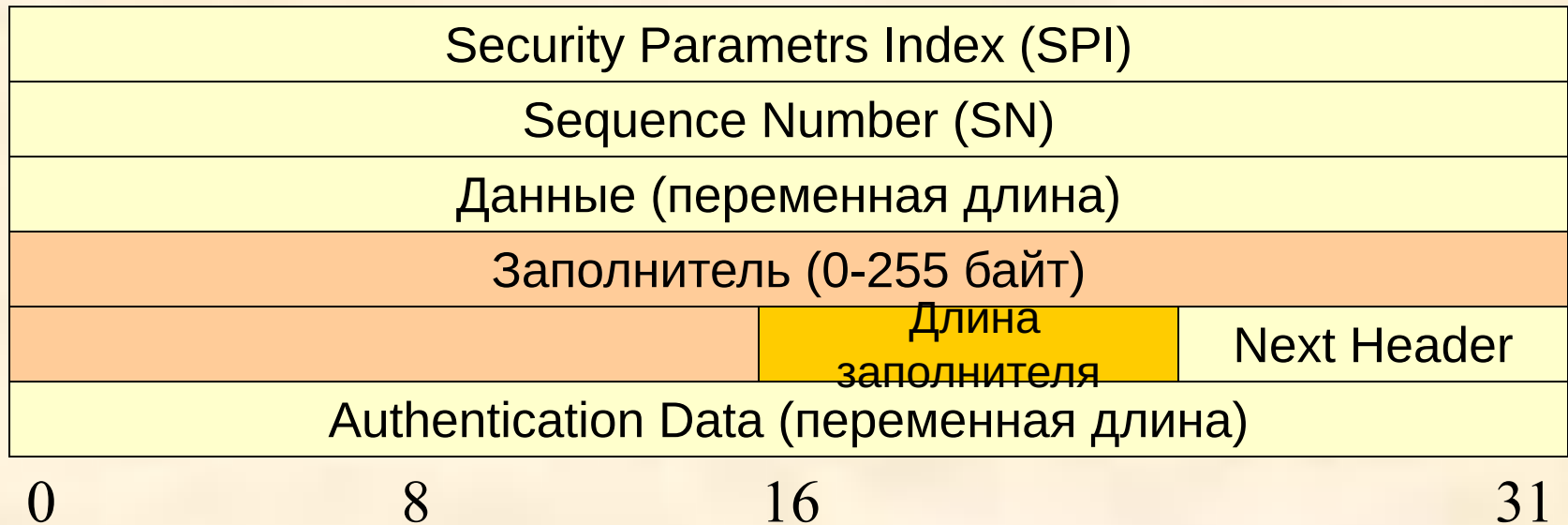
# Протокол ESP



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

**Поле заполнителя**

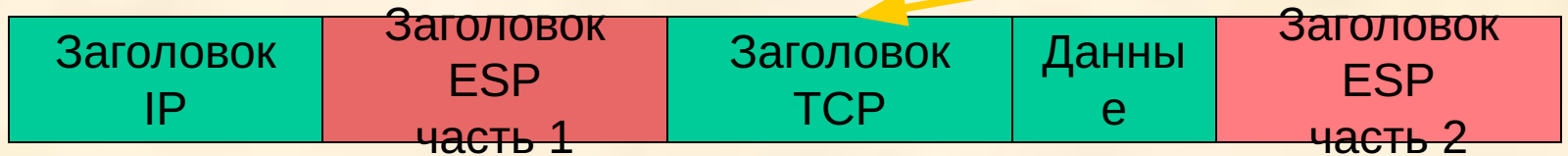
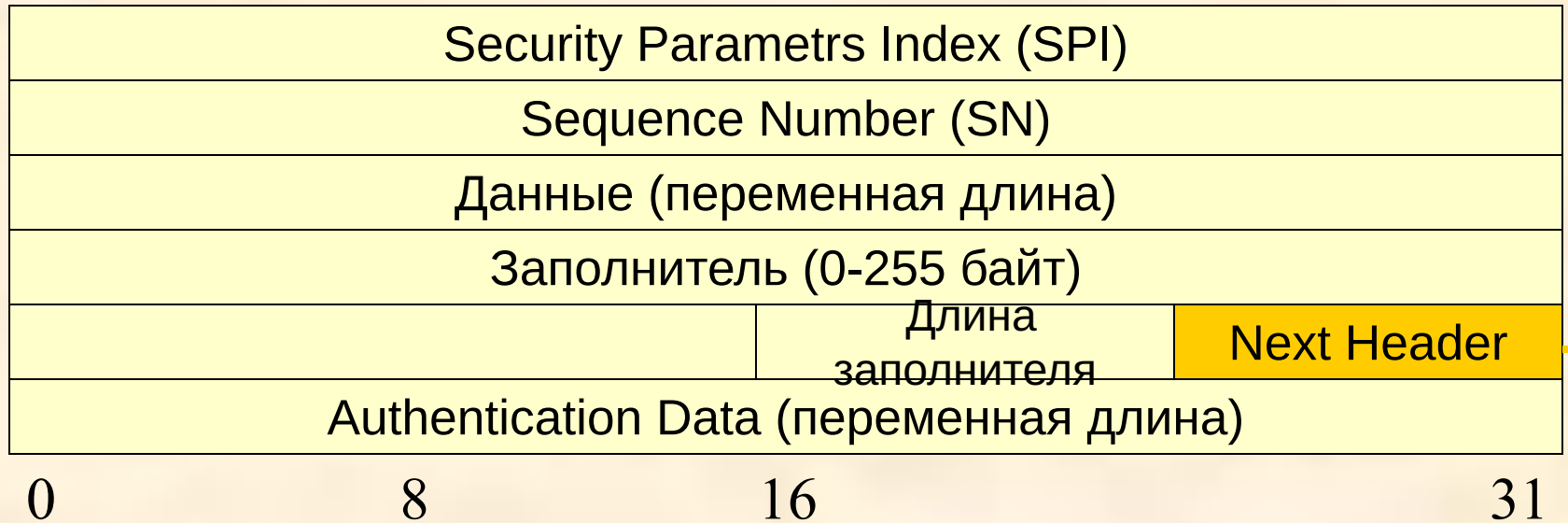
# Протокол ESP



Длина заполнителя в байтах

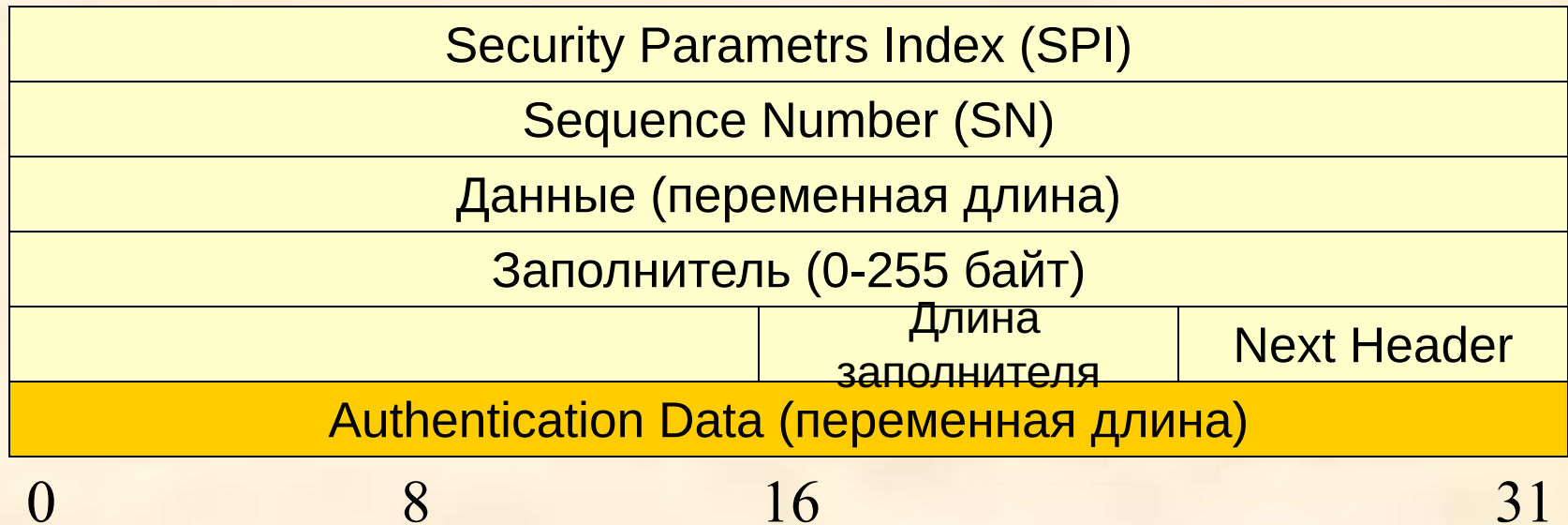
**Поле длины заполнителя**

# Протокол ESP



**Поле Next Header**

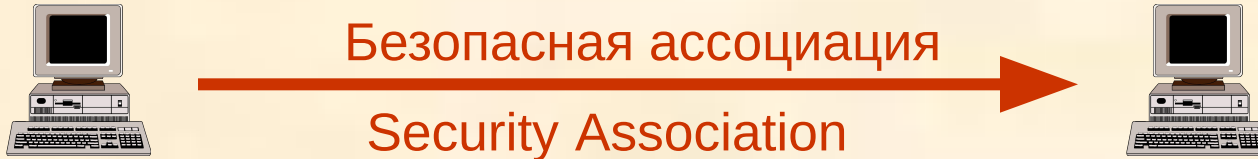
# Протокол ESP



хэш-функция (содержимое пакета,  
симметричный секретный ключ)

**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

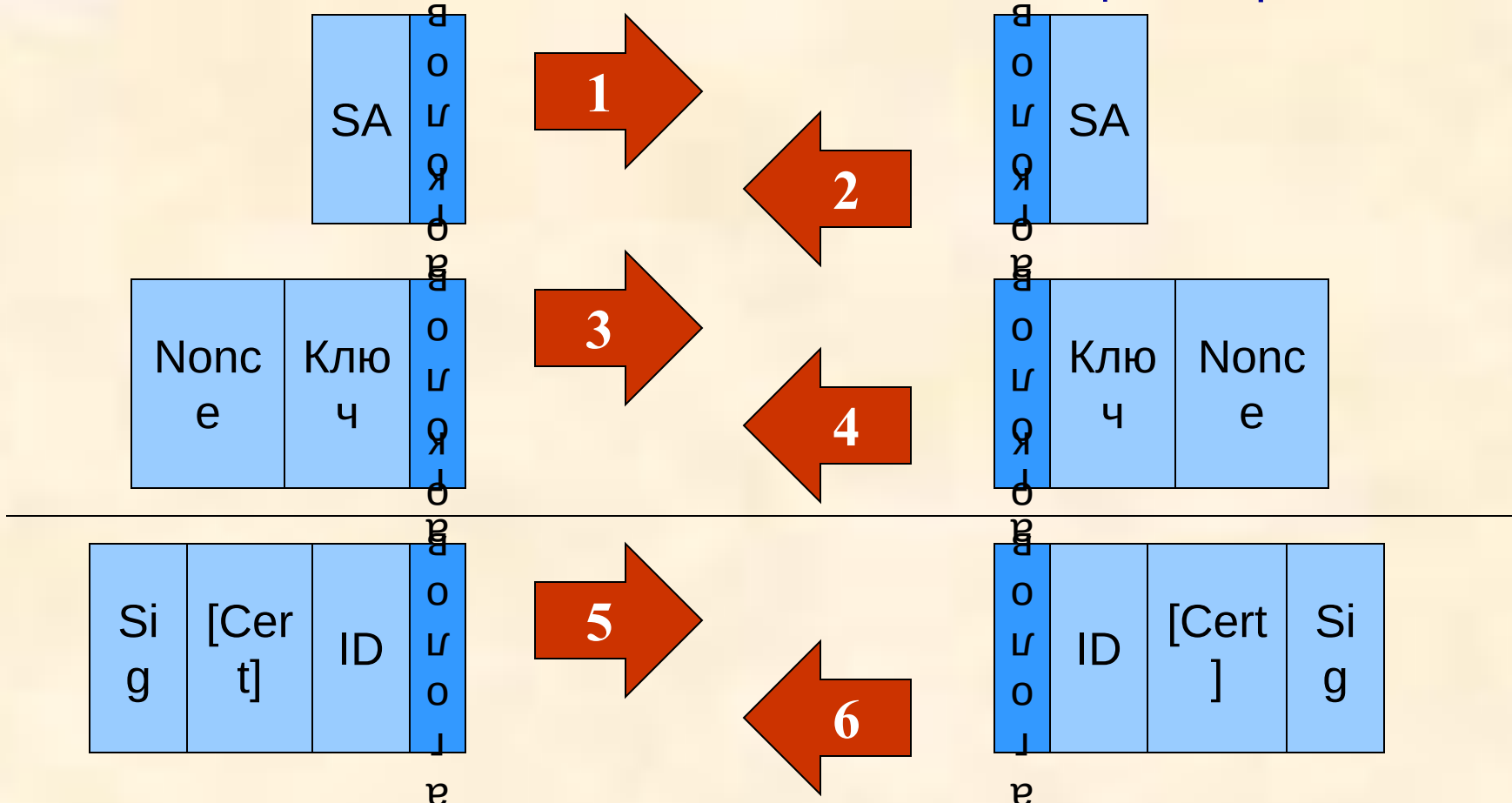
- Согласование всех параметров, ассоциируемых с общим каналом SA

**Этапы функционирования протокола IKE**

# Протокол IKE (фаза 1)

Иницилирующая сторона

Отвечающая сторона



Основной режим установления канала IKE SA

# Протокол IKE (фаза 1)

The screenshot displays the Microsoft Network Monitor interface for a captured IKE packet. The main window shows a list of frames, with frame 6 selected. The details pane below shows the following information:

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
2	26.317843	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir
3	26.317843	0050BF7C791C	NETRON934D1E	ISAKMP	Major Version: 1 Mir
4	26.327858	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir
5	26.327858	0050BF7C791C	NETRON934D1E	ISAKMP	Major Version: 1 Mir
6	26.347886	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir

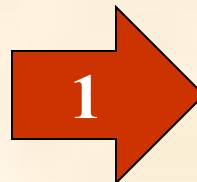
Expanded details for the selected frame (Frame 6):

- FRAME: Base frame properties
- ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
- IP: ID = 0x7AB9; Proto = UDP; Len: 160
- UDP: Src Port: ISAKMP, (500); Dst Port: ISAKMP (500); Length = 140 (0x8C)
- ISAKMP: Major Version: 1 Minor Version: 0 Length: 132
  - ISAKMP: Initiator cookie = 3D 38 43 B3 69 AB C2 28
  - ISAKMP: Responder cookie = 00 00 00 00 00 00 00 00
  - ISAKMP: Next payload = Security Association
  - ISAKMP: Major version = 1 (0x1)
  - ISAKMP: Minor version = 0 (0x0)
  - ISAKMP: Exchange type = Identity Protection
  - ISAKMP: Flags summary = 0 (0x0)
  - ISAKMP: Message ID = 0 (0x0)
  - ISAKMP: Length = 132 (0x84)
  - ISAKMP: Payload type = Security Association
  - ISAKMP: Payload type = Vendor ID

Initiator Cookie

SA

Vendor ID



# Протокол IKE (фаза 1)

Microsoft Network Monitor - [C:\IKE.cap (Detail)]

File Edit Display Tools Options Window Help

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
2	26.317843	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir
3	26.317843	0050BF7C791C	NETRON934D1E	ISAKMP	Major Version: 1 Mir
4	26.327858	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir
5	26.327858	0050BF7C791C	NETRON934D1E	ISAKMP	Major Version: 1 Mir
6	26.347886	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir

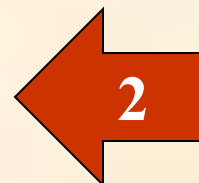
FRAME: Base frame properties  
ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol  
IP: ID = 0x7AB9; Proto = UDP; Len: 160  
UDP: Src Port: ISAKMP, (500); Dst Port: ISAKMP (500); Length = 140 (0x8C)  
ISAKMP: Major Version: 1 Minor Version: 0 Length: 132  
ISAKMP: Initiator cookie = 3D 38 43 B3 69 AB C2 28  
ISAKMP: Responder cookie = 00 00 00 00 00 00 00 00  
ISAKMP: Next payload = Security Association  
ISAKMP: Major version = 1 (0x1)  
ISAKMP: Minor version = 0 (0x0)  
ISAKMP: Exchange type = Identity Protection  
ISAKMP: Flags summary = 0 (0x0)  
ISAKMP: Message ID = 0 (0x0)  
ISAKMP: Length = 132 (0x84)  
ISAKMP: Payload type = Security Association  
ISAKMP: Payload type = Vendor ID

Summary of the ISAKMP Packet F#: 2/21 Off: 42 (x)

Responder Cookie

SA

Vendor ID



# Протокол IKE (фаза 1)

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
2	26.317843	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir
3	26.317843	0050BF7C791C	NETRON934D1E	ISAKMP	Major Version: 1 Mir
4	26.327858	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir
5	26.327858	0050BF7C791C	NETRON934D1E	ISAKMP	Major Version: 1 Mir
6	26.347886	NETRON934D1E	0050BF7C791C	ISAKMP	Major Version: 1 Mir

FRAME: Base frame properties  
ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol  
IP: ID = 0x7AD0; Proto = UDP; Len: 276  
UDP: Src Port: ISAKMP, (500); Dst Port: ISAKMP (500); Length = 256 (0x100)  
ISAKMP: Major Version: 1 Minor Version: 0 Length: 248  
ISAKMP: Initiator cookie = 3D 38 43 B3 69 AB C2 28  
ISAKMP: Responder cookie = 26 B0 0F D9 DF 18 41 E4  
ISAKMP: Next payload = Key Exchange  
ISAKMP: Major version = 1 (0x1)  
ISAKMP: Minor version = 0 (0x0)  
ISAKMP: Exchange type = Identity Protection  
ISAKMP: Flags summary = 0 (0x0)  
ISAKMP: Message ID = 0 (0x0)  
ISAKMP: Length = 248 (0xF8)  
ISAKMP: Payload type = Key Exchange  
ISAKMP: Payload type = Nonce  
ISAKMP: Payload type = Certificate Request

Summary of the ISAKMP Packet F#: 4/21 Off: 42 (x)

Открытый ключ

Случайное число

Запрос сертификата

3

# Протокол IKE (фаза 1)

Microsoft Network Monitor - [C:\IKE.cap (Summary)]

File Edit Display Tools Options Window Help

Option	Src Other Addr	Dst Other Addr	T
Version: 1 Minor Version: 0 Length:...	192.168.192.1	200.0.0.203	I
Version: 1 Minor Version: 0 Length:...	200.0.0.203	192.168.192.1	I
Version: 1 Minor Version: 0 Length:...	192.168.192.1	200.0.0.203	I
Version: 1 Minor Version: 0 Length:...	200.0.0.203	192.168.192.1	I
Version: 1 Minor Version: 0 Length:...	192.168.192.1	200.0.0.203	I

FRAME: Base frame properties

ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol

IP: ID = 0xDD89; Proto = UDP; Len: 276

UDP: Src Port: ISAKMP, (500); Dst Port: ISAKMP (500); Length = 256 (0x100)

ISAKMP: Major Version: 1 Minor Version: 0 Length: 248

ISAKMP: Initiator cookie = 3D 38 43 B3 69 AB C2 28

ISAKMP: Responder cookie = 26 B0 0F D9 DF 18 41 E4

ISAKMP: Next payload = Key Exchange

ISAKMP: Major version = 1 (0x1)

ISAKMP: Minor version = 0 (0x0)

ISAKMP: Exchange type = Identity Protection

ISAKMP: Flags summary = 0 (0x0)

ISAKMP: Message ID = 0 (0x0)

ISAKMP: Length = 248 (0xF8)

ISAKMP: Payload type = Key Exchange

ISAKMP: Payload type = Nonce

ISAKMP: Payload type = Certificate Request

Summary of the ISAKMP Packet F#: 5/21 Off: 42 (x)

Открытый ключ

Случайное число

Запрос сертификата



# Протокол IKE (фаза 1)

The screenshot shows the Microsoft Network Monitor interface with a summary of an IKE Phase 1 packet. The packet list at the top shows five packets between 192.168.192.1 and 200.0.0.203. The selected packet details are as follows:

Option	Src Other Addr	Dst Other Addr	T
Version: 1 Minor Version: 0 Length:...	192.168.192.1	200.0.0.203	I
Version: 1 Minor Version: 0 Length:...	200.0.0.203	192.168.192.1	I
Version: 1 Minor Version: 0 Length:...	192.168.192.1	200.0.0.203	I
Version: 1 Minor Version: 0 Length:...	200.0.0.203	192.168.192.1	I
Version: 1 Minor Version: 0 Length:...	192.168.192.1	200.0.0.203	I

Packet details:

- FRAME: Base frame properties
- ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
- IP: ID = 0x7B9D; Proto = UDP; Len: 968
- UDP: Src Port: ISAKMP, (500); Dst Port: ISAKMP (500); Length = 948 (0x3B4)
- ISAKMP: Major Version: 1 Minor Version: 0 Length: 940**
- ISAKMP: Initiator cookie = 3D 38 43 B3 69 AB C2 28
- ISAKMP: Responder cookie = 26 B0 0F D9 DF 18 41 E4
- ISAKMP: Next payload = Identification
- ISAKMP: Major version = 1 (0x1)
- ISAKMP: Minor version = 0 (0x0)
- ISAKMP: Exchange type = Identity Protection
- ISAKMP: Flags summary = 1 (0x1)
- ISAKMP: Message ID = 0 (0x0)
- ISAKMP: Length = 940 (0x3AC)
- ISAKMP: ISAKMP Payloads(encrypted)

Summary of the ISAKMP Packet F#: 6/21 Off: 42 (x)

ID

5

В нескольких пакетах

# Протокол IKE (фаза 1)

The screenshot shows the Microsoft Network Monitor interface. The top pane displays a list of network packets. The selected packet is an IP packet from 200.0.0.203 to 192.168.192.1. The bottom pane shows the expanded details of the ISAKMP payload within a UDP packet.

Protocol	Src Other Addr	Dst Other Addr	Type
IP	192.168.192.1	200.0.0.203	IP
IP	200.0.0.203	192.168.192.1	IP
IP	192.168.192.1	200.0.0.203	IP
IP	200.0.0.203	192.168.192.1	IP
IP	192.168.192.1	200.0.0.203	IP

Expanded packet details:

- FRAME: Base frame properties
- ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
- IP: ID = 0xDE59; Proto = UDP; Len: 968
- UDP: Src Port: ISAKMP, (500); Dst Port: ISAKMP (500); Length = 948 (0x3B4)
- ISAKMP: Major Version: 1 Minor Version: 0 Length: 940**
- ISAKMP: Initiator cookie = 3D 38 43 B3 69 AB C2 28
- ISAKMP: Responder cookie = 26 B0 0F D9 DF 18 41 E4
- ISAKMP: Next payload = Identification
- ISAKMP: Major version = 1 (0x1)
- ISAKMP: Minor version = 0 (0x0)
- ISAKMP: Exchange type = Identity Protection
- ISAKMP: Flags summary = 1 (0x1)
- ISAKMP: Message ID = 0 (0x0)
- ISAKMP: Length = 940 (0x3AC)
- ISAKMP: ISAKMP Payloads(encrypted)

Summary of the ISAKMP Packet F#: 7/21 Off: 42 (x)

ID

6

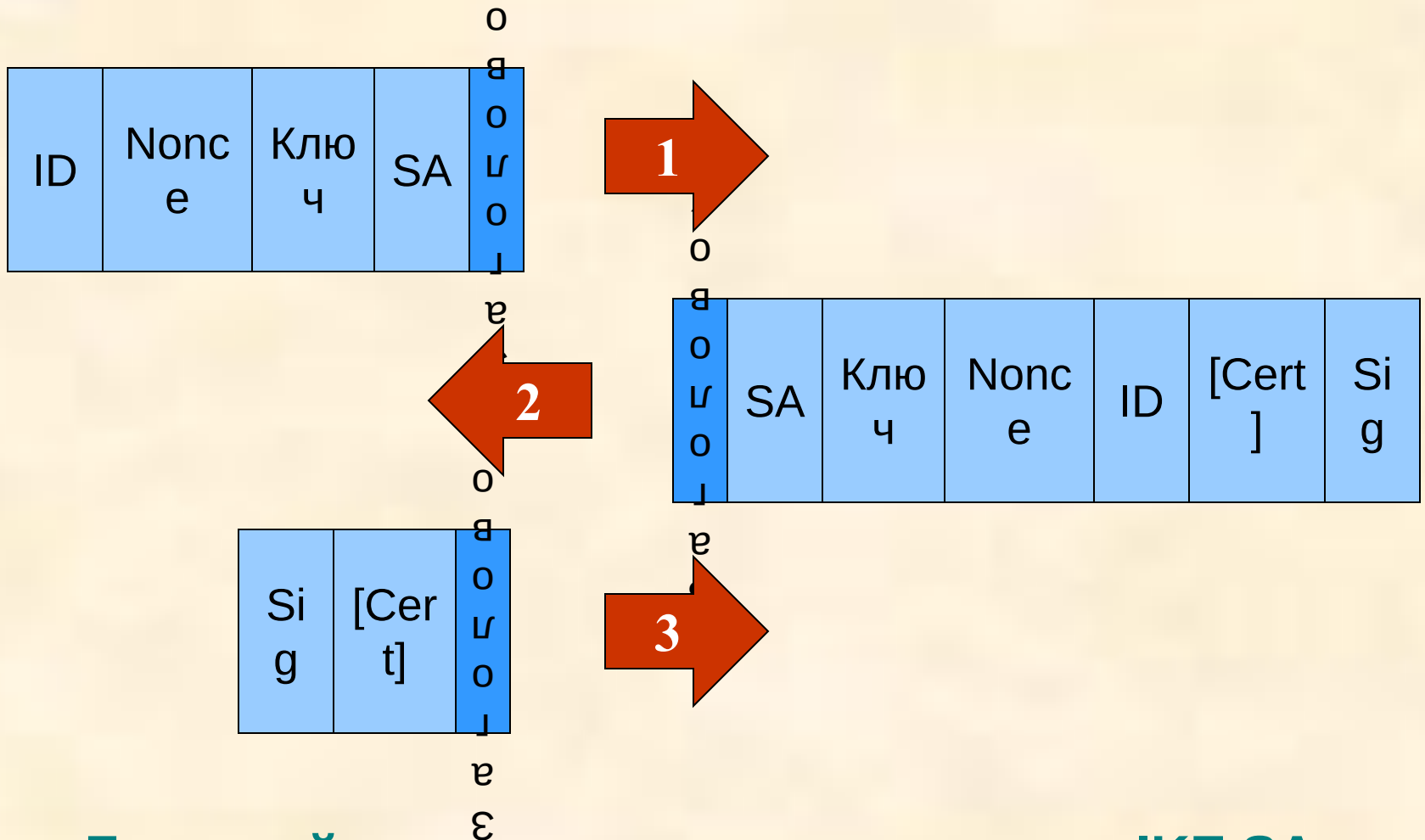
В нескольких пакетах



# Протокол IKE

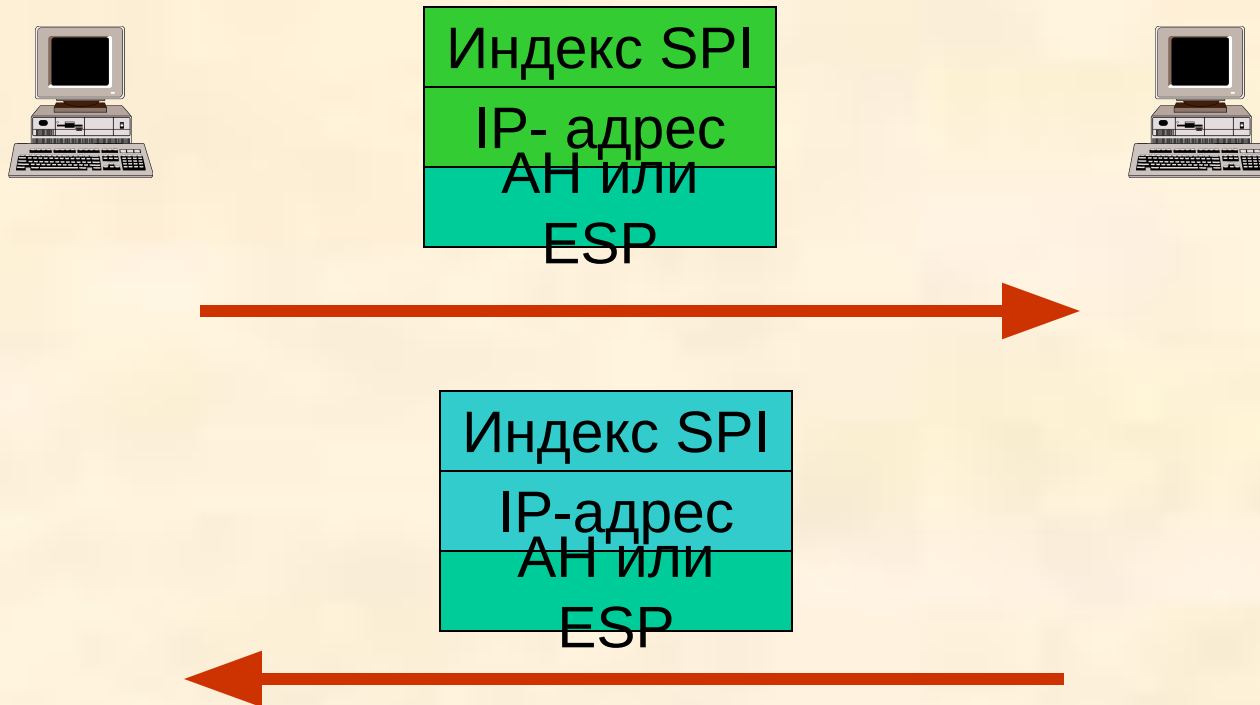
Иницилирующая сторона

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**