ЗАЩИЩЕННЫЕ КАНАЛЫ СВЯЗИ

ЗАЩИЩЕННЫЕ ВИРТУАЛЬНЫЕ СЕТИ (Virtual Private Network - VPN)

Общие принцыпы построения защищенных каналов связи

Объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную сеть, обеспечивающую безопасность циркулирущих данных, называют ***защищенной виртуальной сетью*** (VPN)

Защита информации в процессе передачи по открытым каналам связи основана на выполнении следующих функций:

1) аутентификации взаимодействующих сторон;

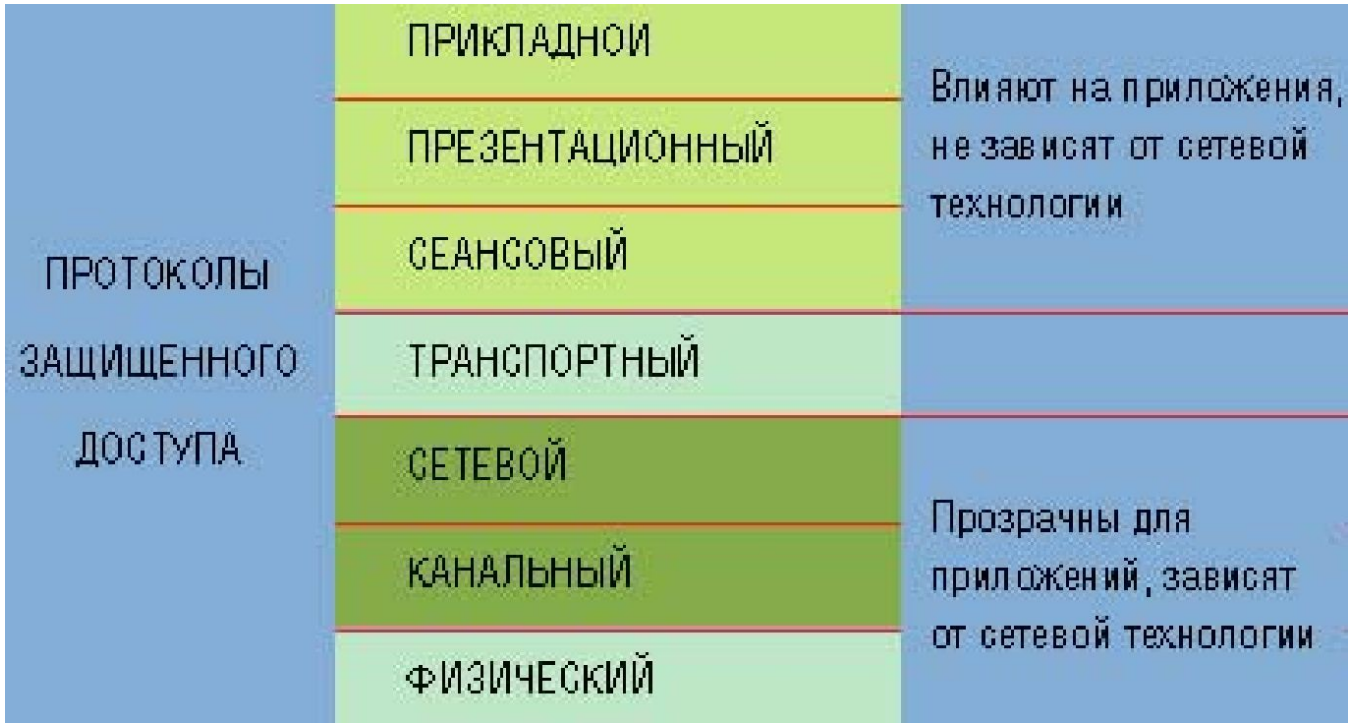
2) криптографическом закрытии передаваемых данных;

3) подтверждении подлинности и целостности передаваемых данных;

4) защите от повтора, задержки и удалении сообщений;

5) защите от отрицания фактов отправления и приема сообщений;

ЗАЩИЩЕННЫЕ КАНАЛЫ НА РАЗНЫХ УРОВНЯХ



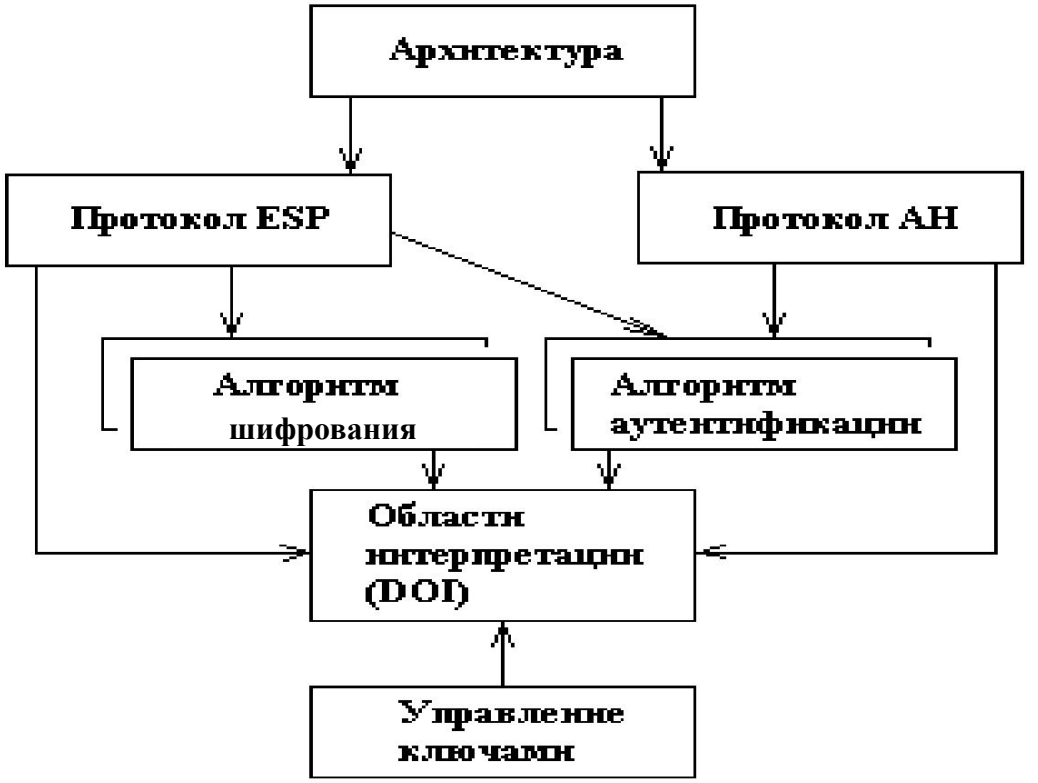
S/MIME

SSL (TLS)

IPSec

PPTP

Архитектура IPsec



Протокол аутентификации AH (Authentication Header)

Обеспечивает:

- целостность;
- аутентификацию.

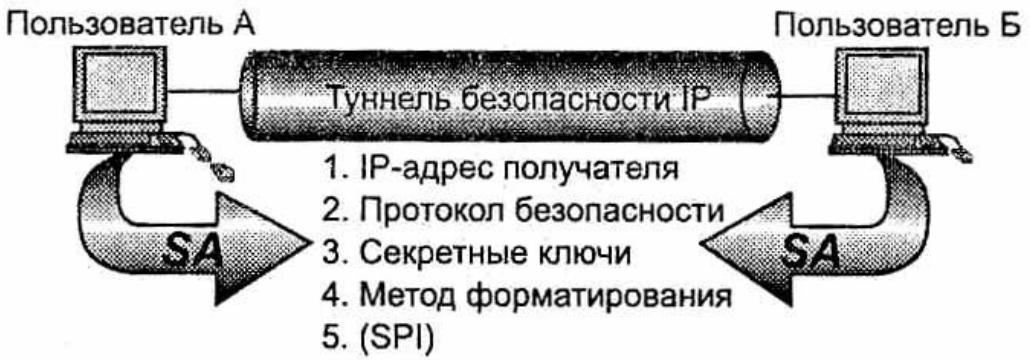
Протокол шифрования (Encapsulation Security Payload)

Обеспечивает:

- конфиденциальность;
- целостность;
- аутентификацию.

Ассоциация безопасности IPSec (SA - Sequrity Assosiation)

Ассоциация безопасности - набор правил, процедур, параметров, прменяемых для обеспечения сервиса защиты транспортного потока



Метод форматирования определяет, каким образом создаются заголовки и то, какая часть этих заголовков и данных пользователя будет защищена в процессе передачи данных

SPI (Security Parameter Index - индекс параметров защиты) - идентификатор SA. Он определяет то, как принимающая сторона будет обрабатывать поступающий поток данных

Режимы IPSec

Транспортный

Исходный пакет

IP-заголовок	Тело пакета

AH- или ESP-пакет

IP-заголовок	Преобразованное и дополненное тело пакета

Тоннельный

Исходный пакет

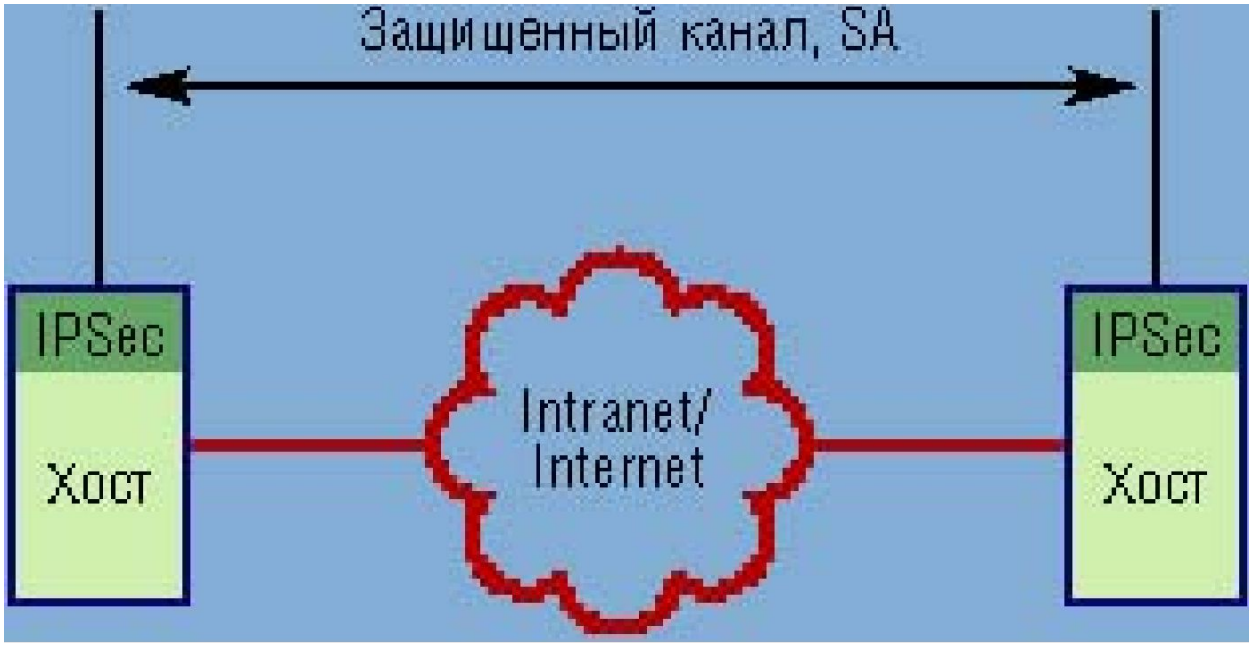
IP-заголовок	Тело пакета

AH- или ESP-пакет

Новый IP-заголовок	Преобразованный и дополненный исходный пакет

Случаи ассоциаций (обзор)

Случай 1

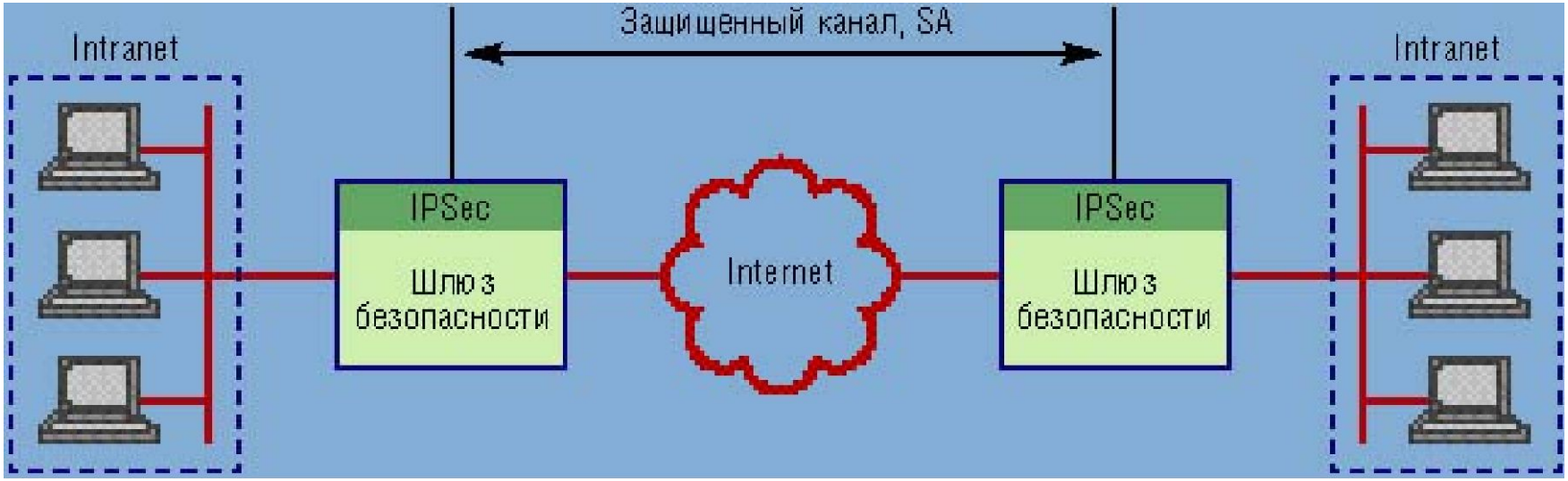


- обеспечивается сквозная защита;

- Internet не имеет понятия об SA и не участвует в ней.

Используется транспортный режим защиты, хотя разрешается и туннельный.

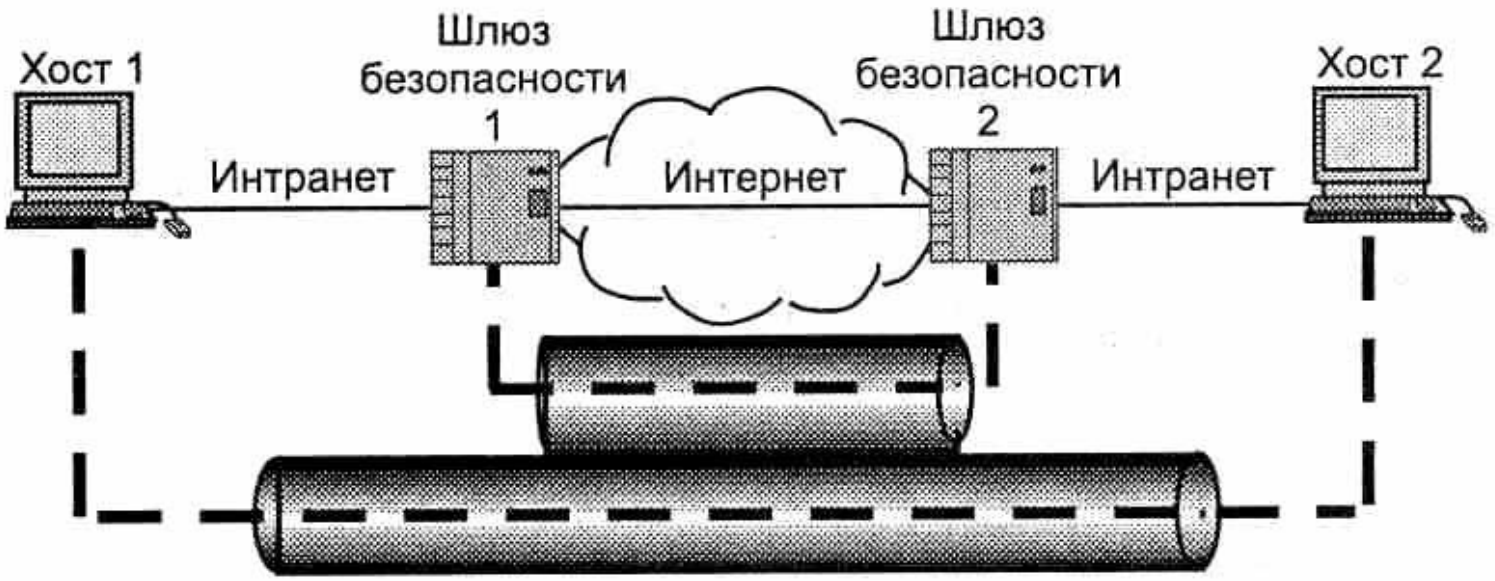
Случай 2



Хосты освобождены от заботы относительно применения SA. Предполагается, что хосты соединены со шлюзами безопасноти (IP-совместимый маршрутизатор) безопасными соединениями.

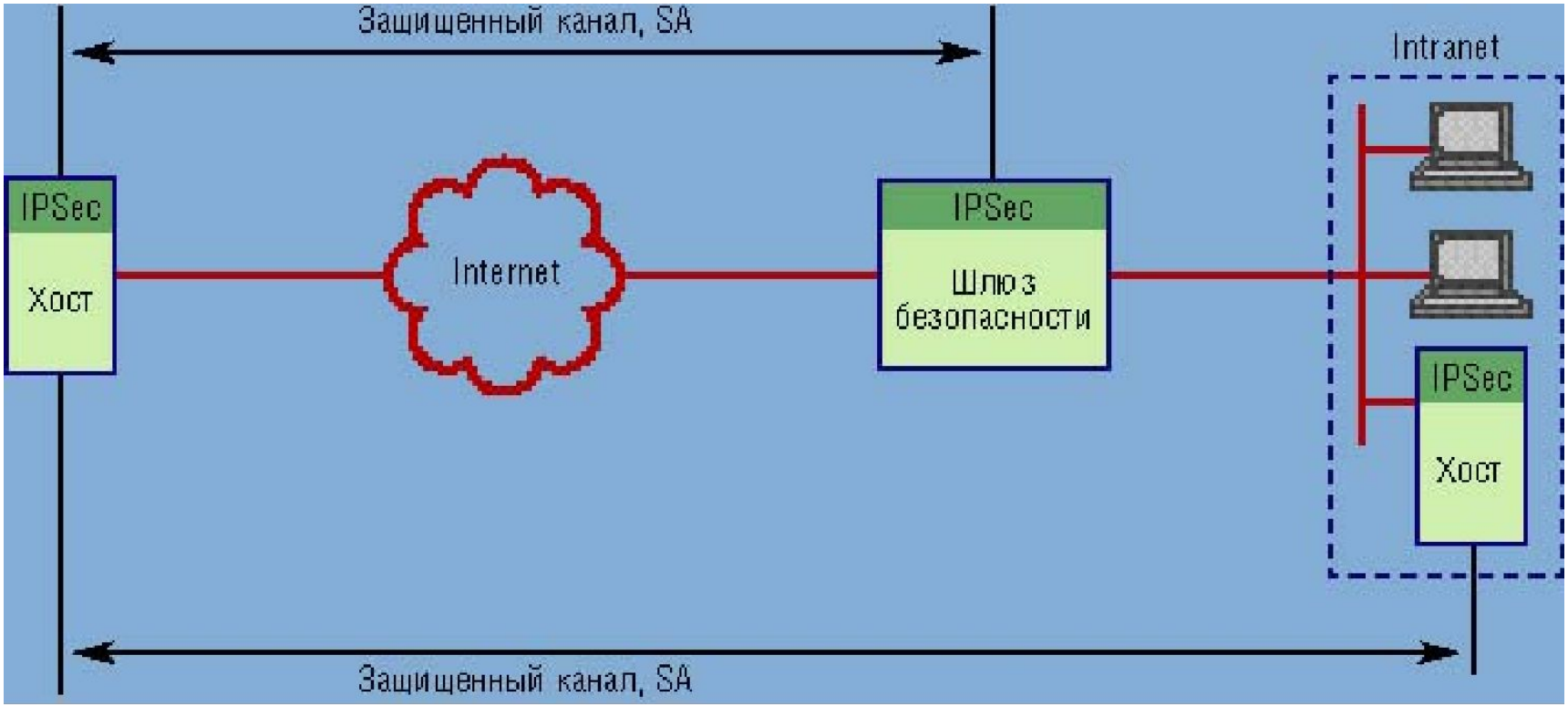
Используется туннельны режим защиты.

Случай 3



Комбинация случая 1 и случая 2

Случай 4



Защищенный канал организуется между удаленным хостом, на котором работает IPSec, и шлюзом, защищающим трафик для всех хостов, входящих в сеть Intranet предприятия.

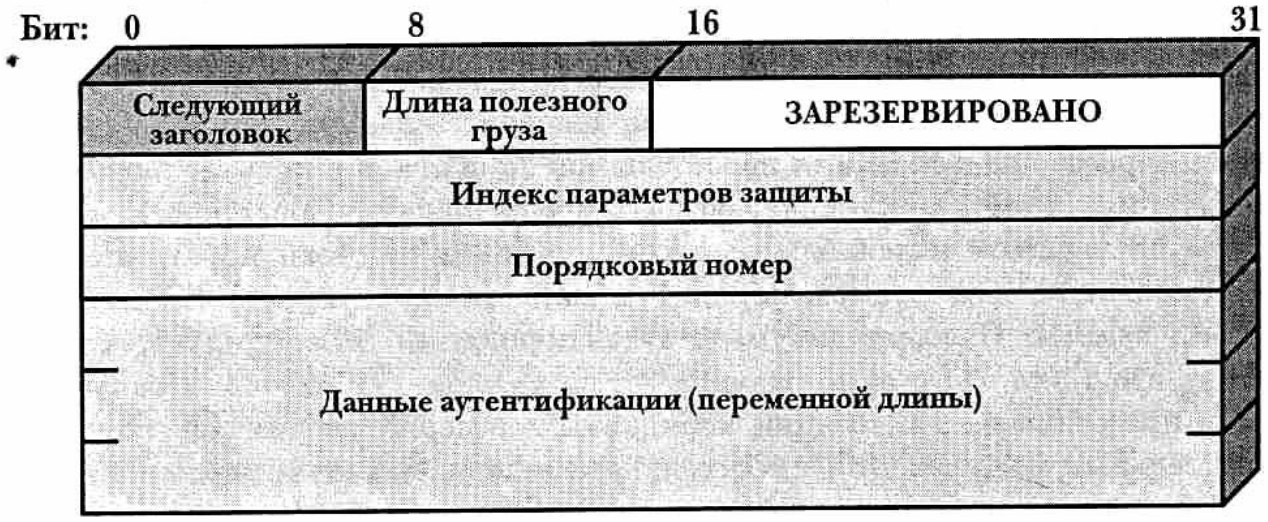
- Удаленный хост может использовать при отправке пакетов шлюзу как транспортный, так и туннельный режим,
- шлюз же отправляет пакет хосту только в туннельном режиме.

Протокол AH

Позволяет приемной стороне убедиться, что:

- пакет был отправлен стороной, с которой установлена данная ассоциация;
- содержимое пакета не было искажено;
- пакет не является дубликатом некоторого ранее полученного пакета

Заголовок аутентификации



Следующий заголовок - код протокола более высокого уровня (TCP, UDP, ICMP, может быть ESP)

Длина полезного груза - длина заголовка AH (в 32-битовых словах, уменьшенная на 2)

Индекс параметров защиты (SPI) - идентификатор для связи пакета с предусмотренной для него SA

Данные аутентификации - содержат код контроля целостности - ICV (код аутентичности сообщения - MAC)

Код контроля целостности

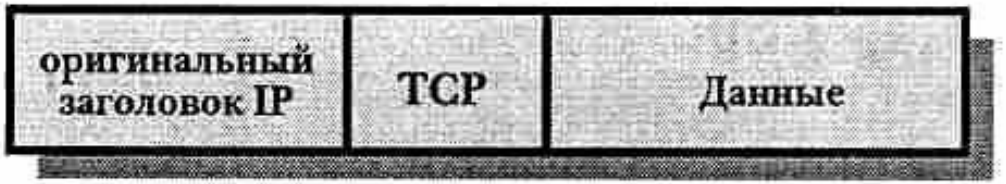
Для контроля целостности сообщения используется хэш-функция с ключом (MD5 или SHA1 или к.л. другая)

Для вычисления хэш функции берется следующая информация:

- Поля IP-заголовка, которые не изменяются в пути следования
- Заголовок AH (кроме поля данных аутентификации);
- Все данные протокола верхнего уровня

Транспортный и туннельный режимы

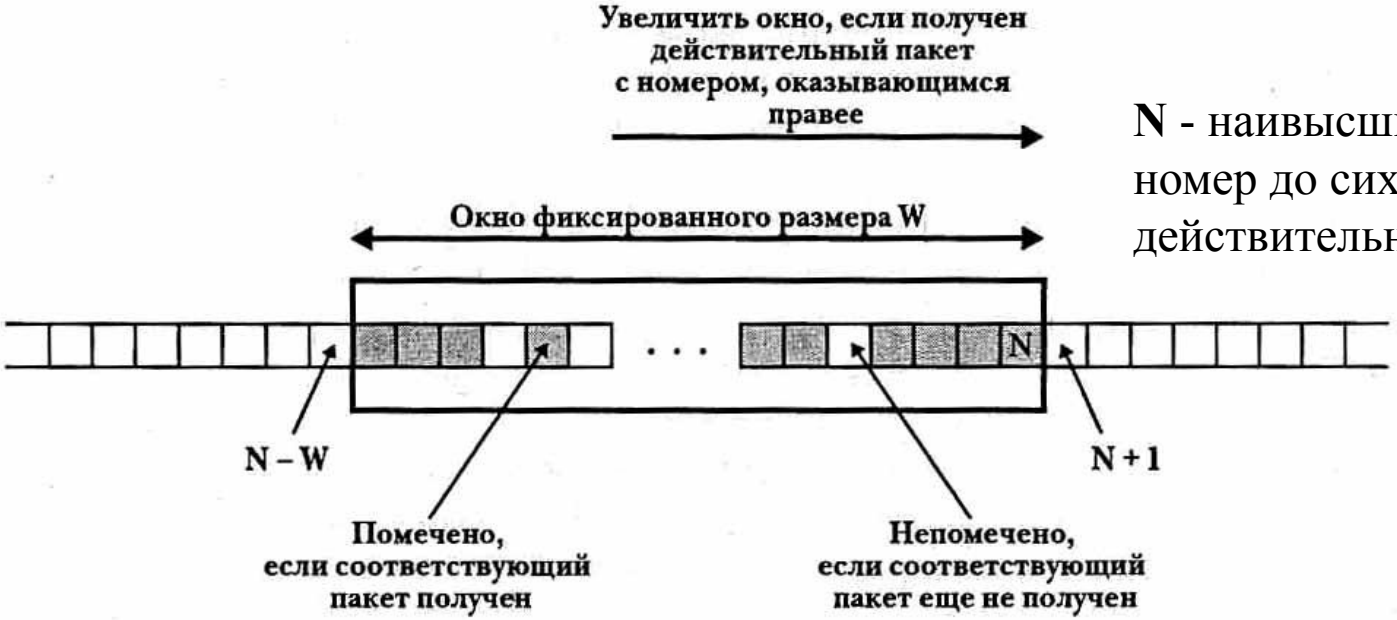
До применения AH



Транспортный режим

Туннельный режим

Сервис защиты от воспроизведения



N - наивысший порядковый номер до сих пор полученных действительных пакетов

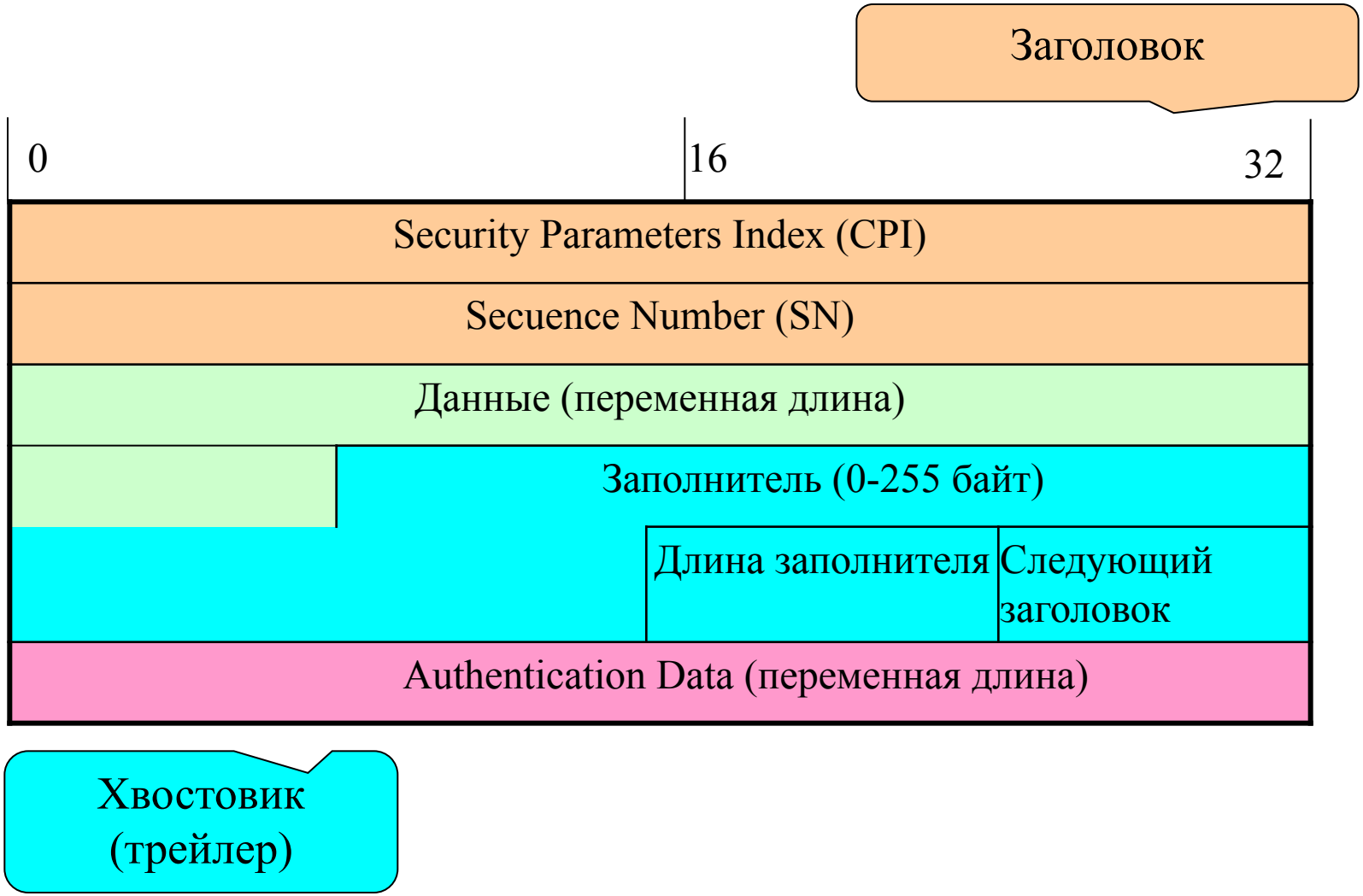
Когда принимается, его обработка выполняется следующим образом.

1. Если полученный пакет попадает в рамки окна и является Новым, проверяется значение MAC. Если аутентификация пакета завершается успешно,помечается соответствующий сегмент в окне.

2. Если полученный пакет попадает в область правее окна и является новым, проверяется значение MAC. Если аутентификация пакета завершается успешно, окно сдвигается так, чтобы новый порядковый номер оказался правой границей окна, а в окне помечается соответствующий сегмент.

3. Если полученный пакет оказывается слева от окна или аутентификация не удается, па будет отвергнут. Такое событие должно фиксироваться.

Протокол шифрования ESP
(Encapsulation Security Payload)



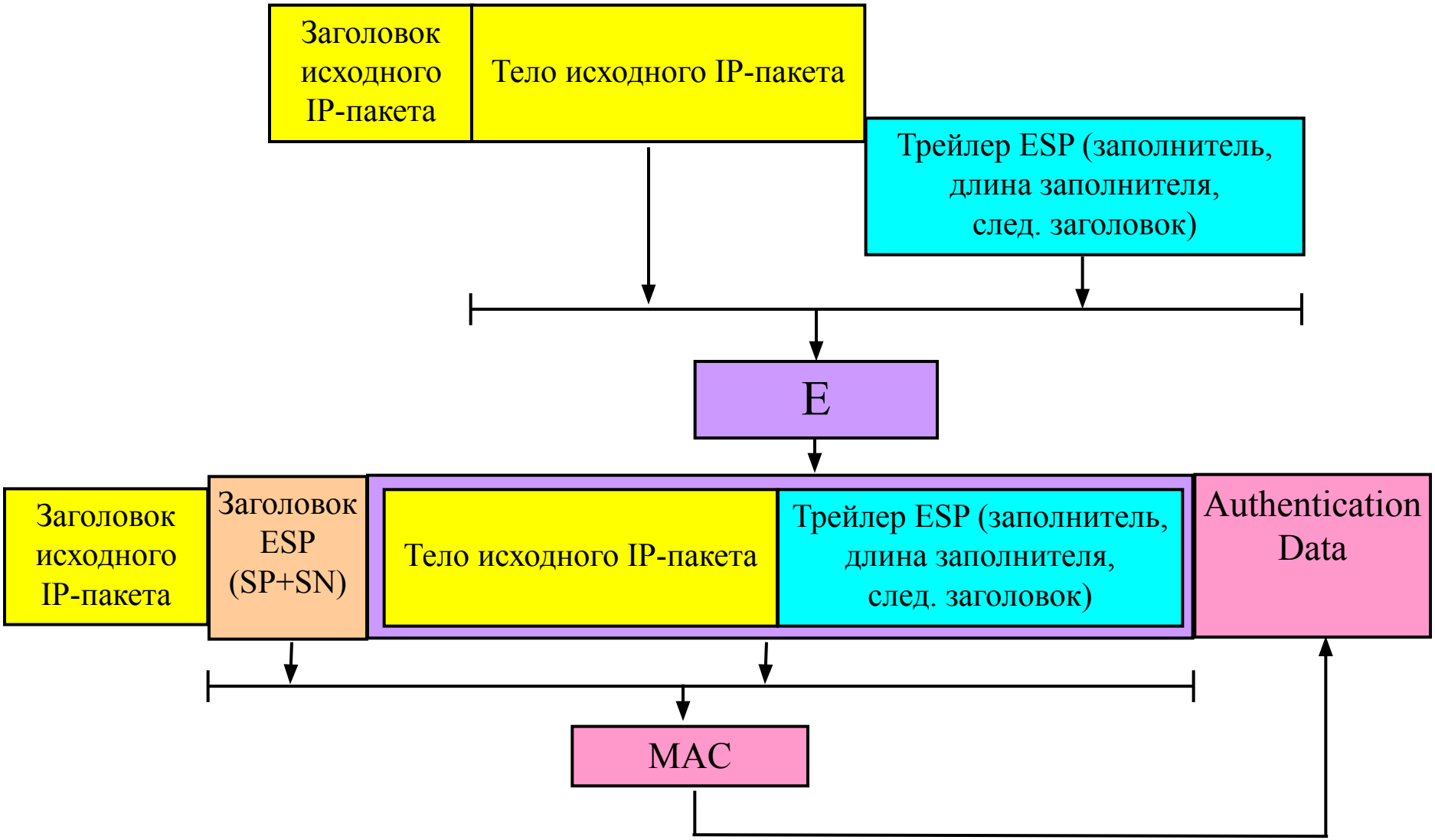
Заполнитель может понадобиться в трех случаях:

- для нормальной работы некоторых алгоритмов шифрования необходимо, чтобы шифруемый текст содержал кратное число блоков определенного размера.

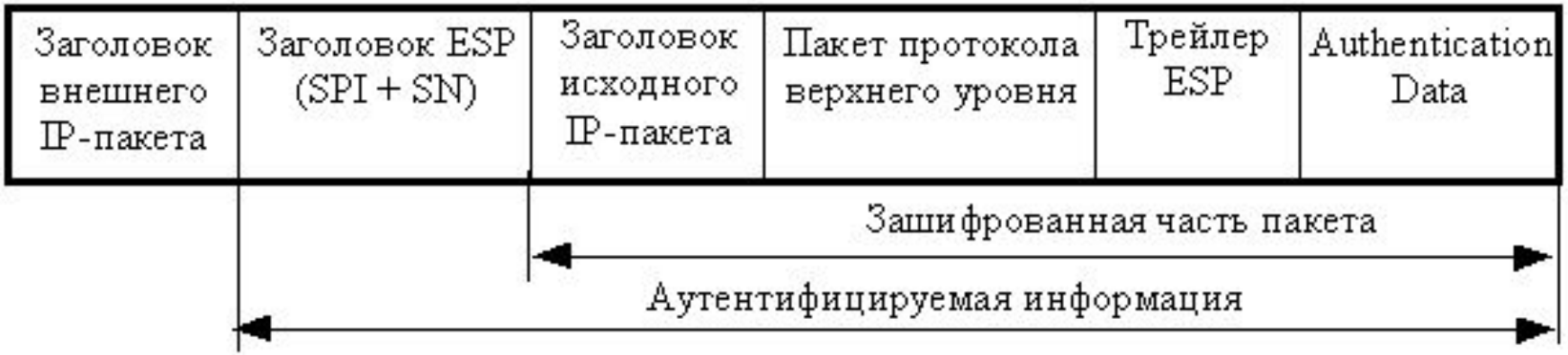
- формат заголовка ESP требует, чтобы поле данных заканчивалось на границе четырех байтов.

- заполнитель можно использовать для сокрытия действительного размера пакета в целях обеспечения так называемой частичной конфиденциальности трафика.

Размещение полей заголовка ESP в транспортном режиме, а также его области защиты по двум группам функций



Размещение полей заголовка ESP в тунельном режиме, а также его области защиты по двум группам функций



Селектор состоит из следующего набора признаков, на основании которых можно с большой степенью детализации выделить тип трафика, который нужно защищать определенным образом:

- IP-адресов источника и назначения;
- портов источника и назначения (т. е. портов TCP или UDP);
- типов протокола транспортного уровня (TCP, UDP);
- имени пользователя в формате DNS или X.500;
- имени системы (хоста, шлюза безопасности и т. п.) в формате DNS или X.500

Управление ключами в IPSec

Ручное

Автоматизированное

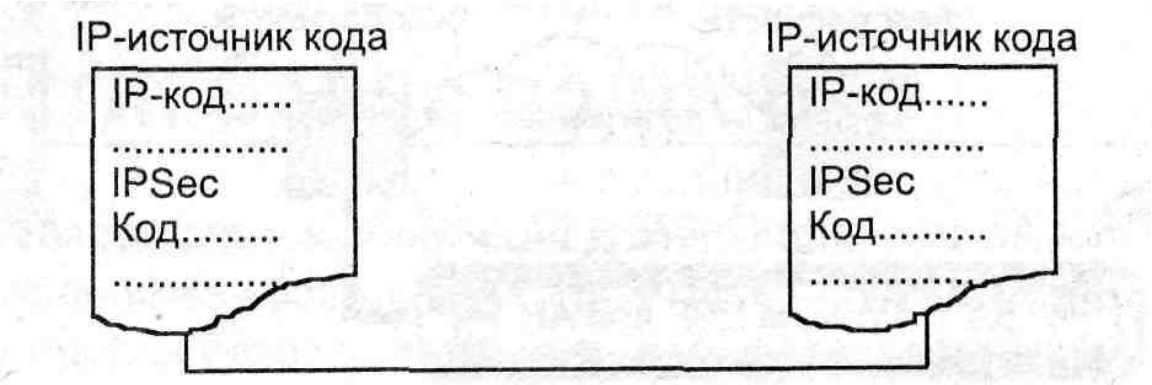
ISAKMP/Oakley

Oakley- протокол обмена ключами, основанный на алгоритме Диффи-Хеллмана, но обеспечивающий дополнительную защиту

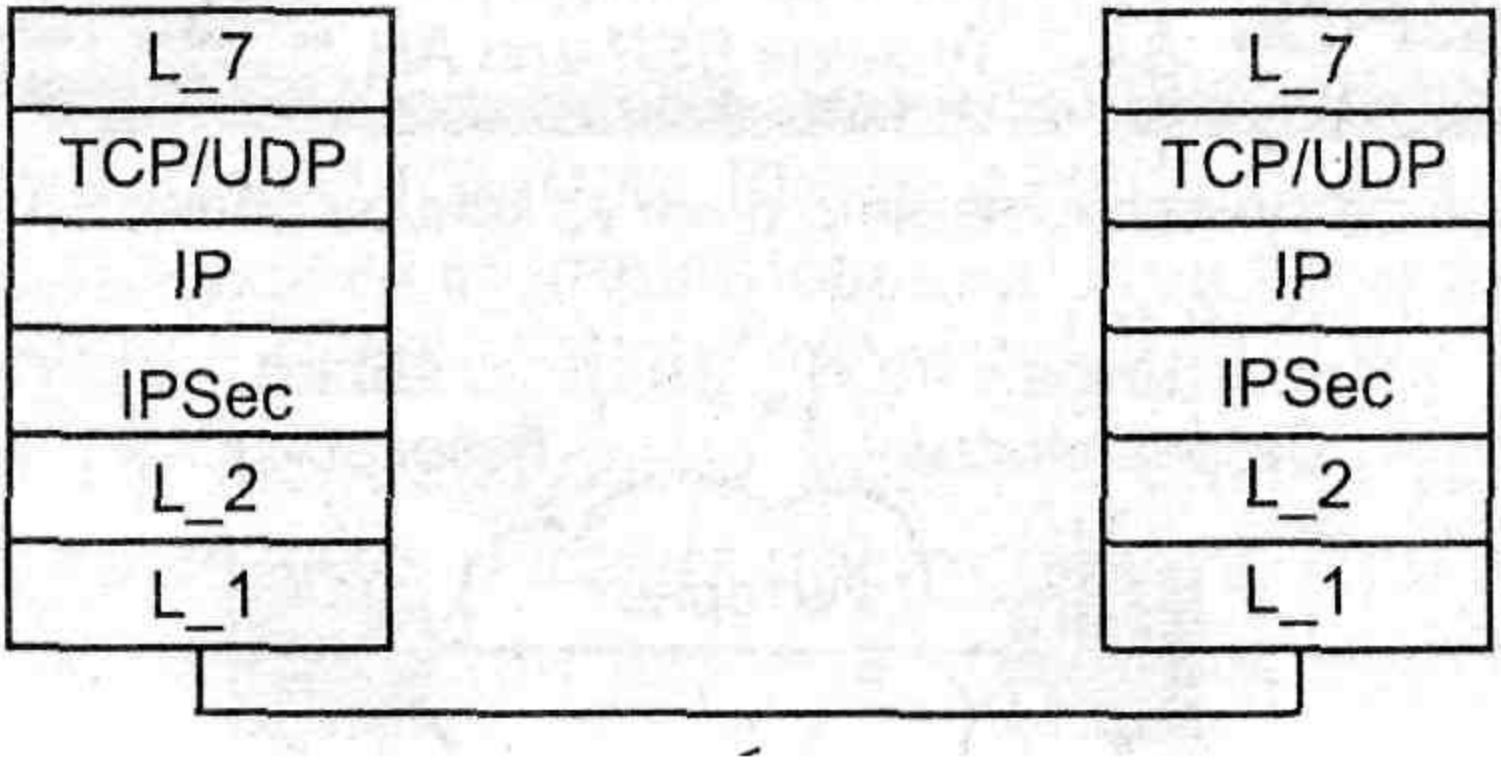
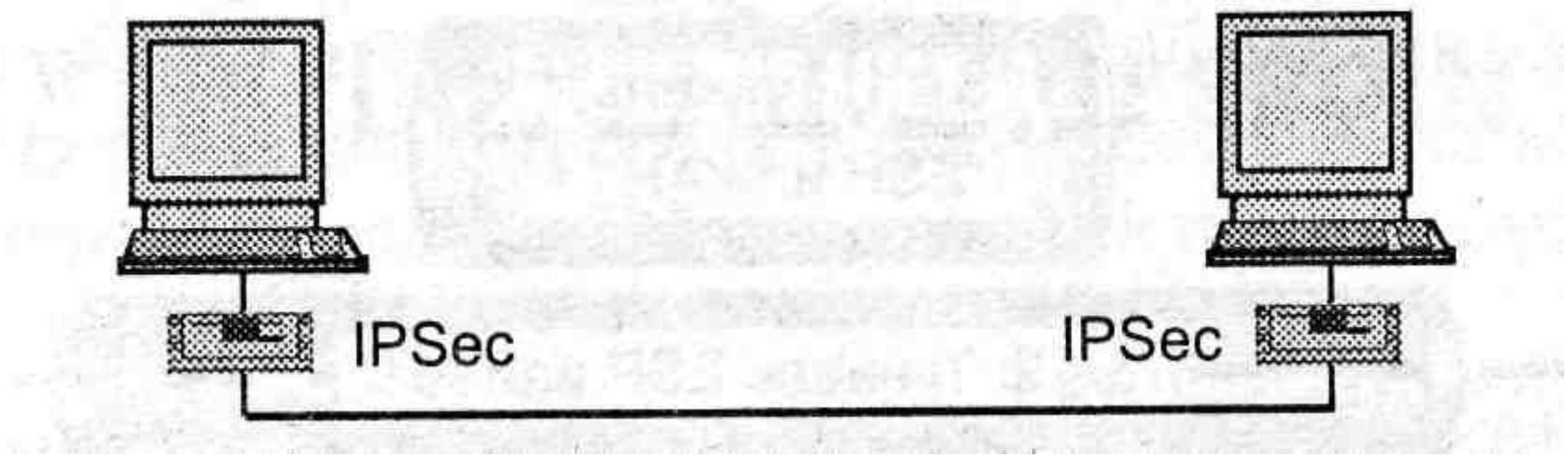
ISAKMP (Internet Security Association and Key Management Protocol) – защищенная связь в Internet и протокол управления ключами – каркас схемы управления ключами. Не привязан к конкретным протоколам управления ключами.

Местоположение IPSec

Сценарий «Запихнуть-в-код»
(bump-in-the-code - BITC)



Сценарий «Запихнуть-в-стек» (bump-in-the-stack - BITS)



Сценарий «Запихнуть-в-железо» (bump-in-the-wire - BITW)