Лекция
ОСНОВЫ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

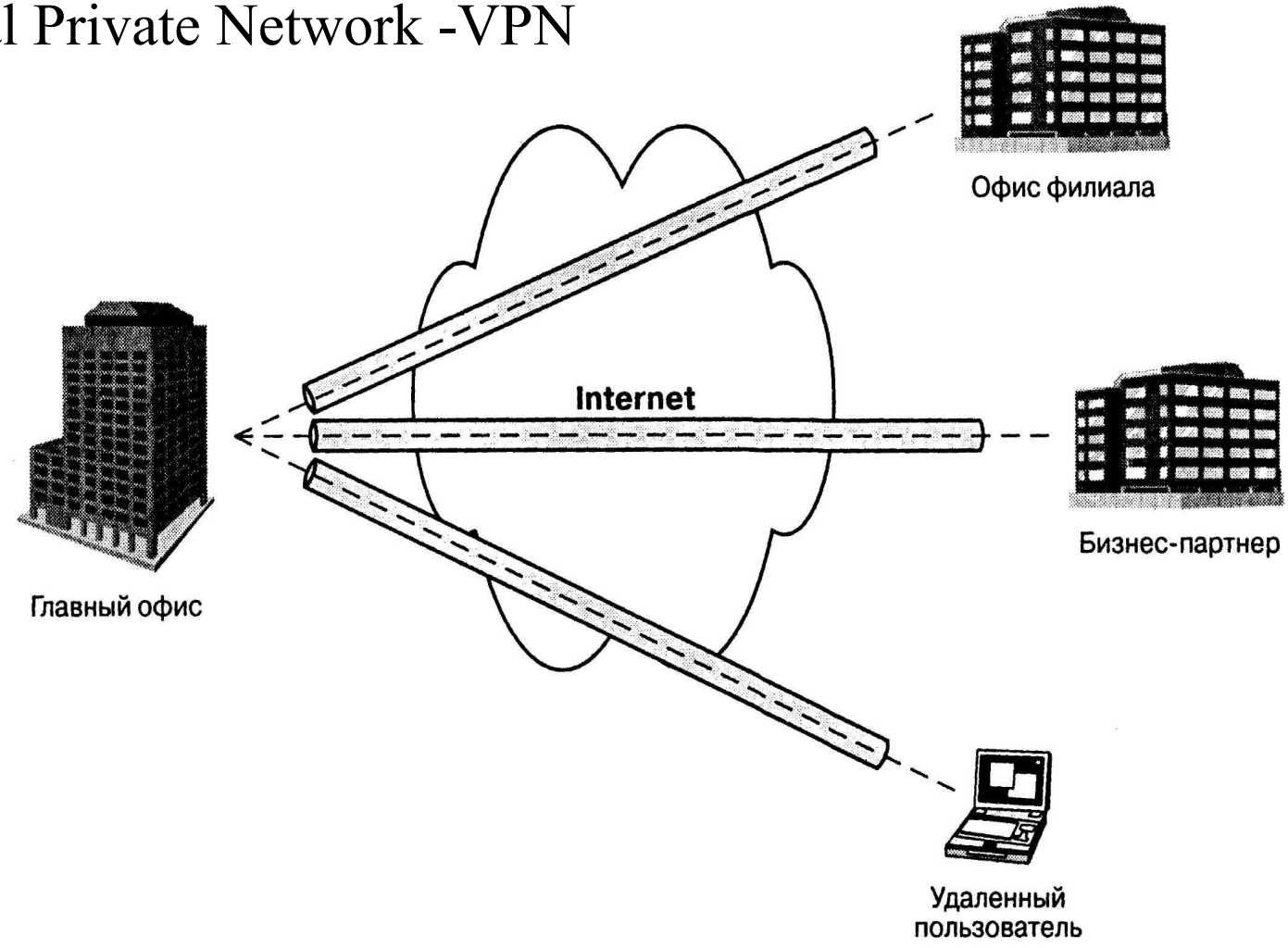
технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

Виртуальной защищенной сетью (VPN) называется технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

Virtual Private Network -VPN

Виртуальная защищенная сеть VPN

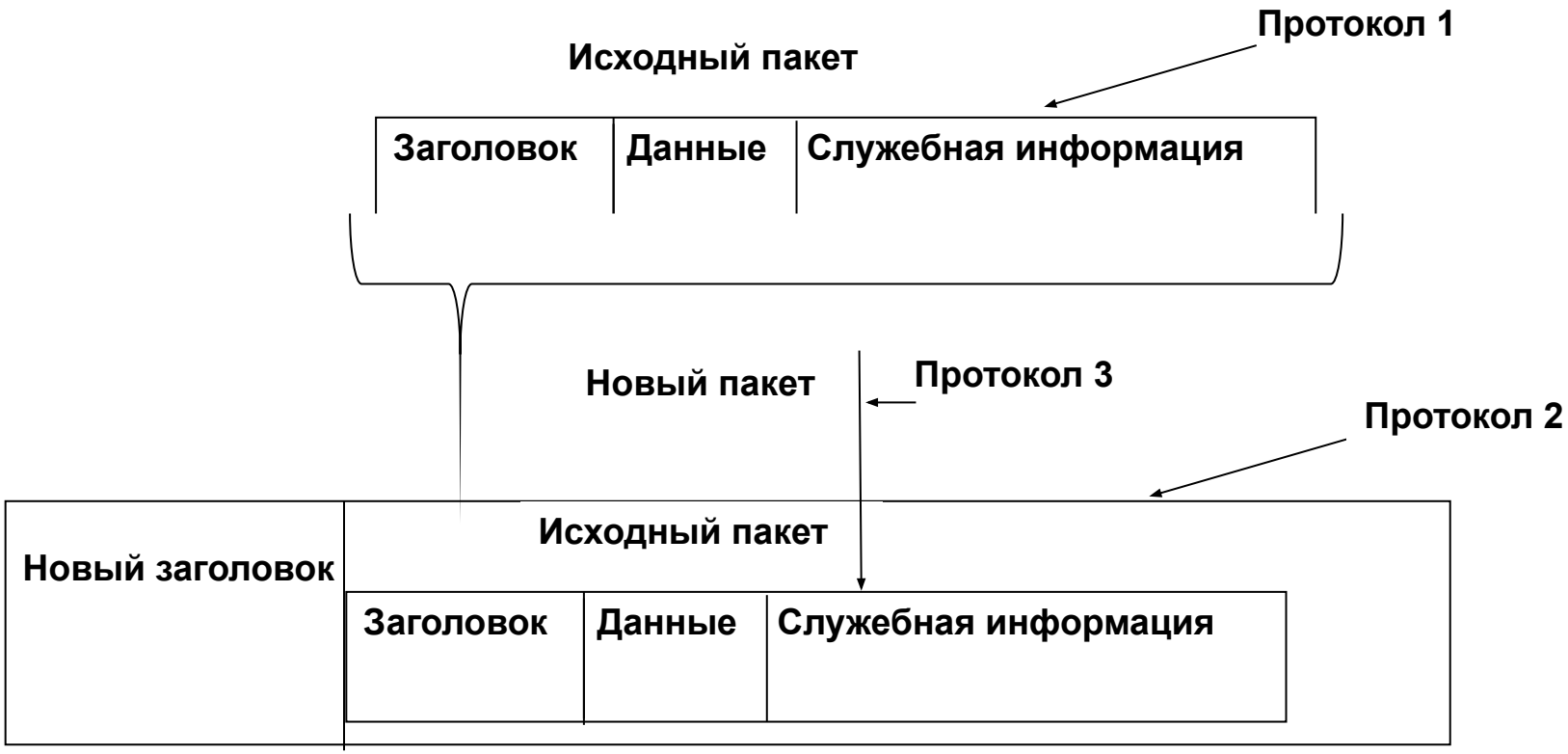
Virtual Private Network -VPN



Технологии VPN:

-туннелирование;
-криптографическая защита

Принцип туннелирования



Задачи, решаемые в VPN

- взаимная аутентификация абонентов при установлении соединения;

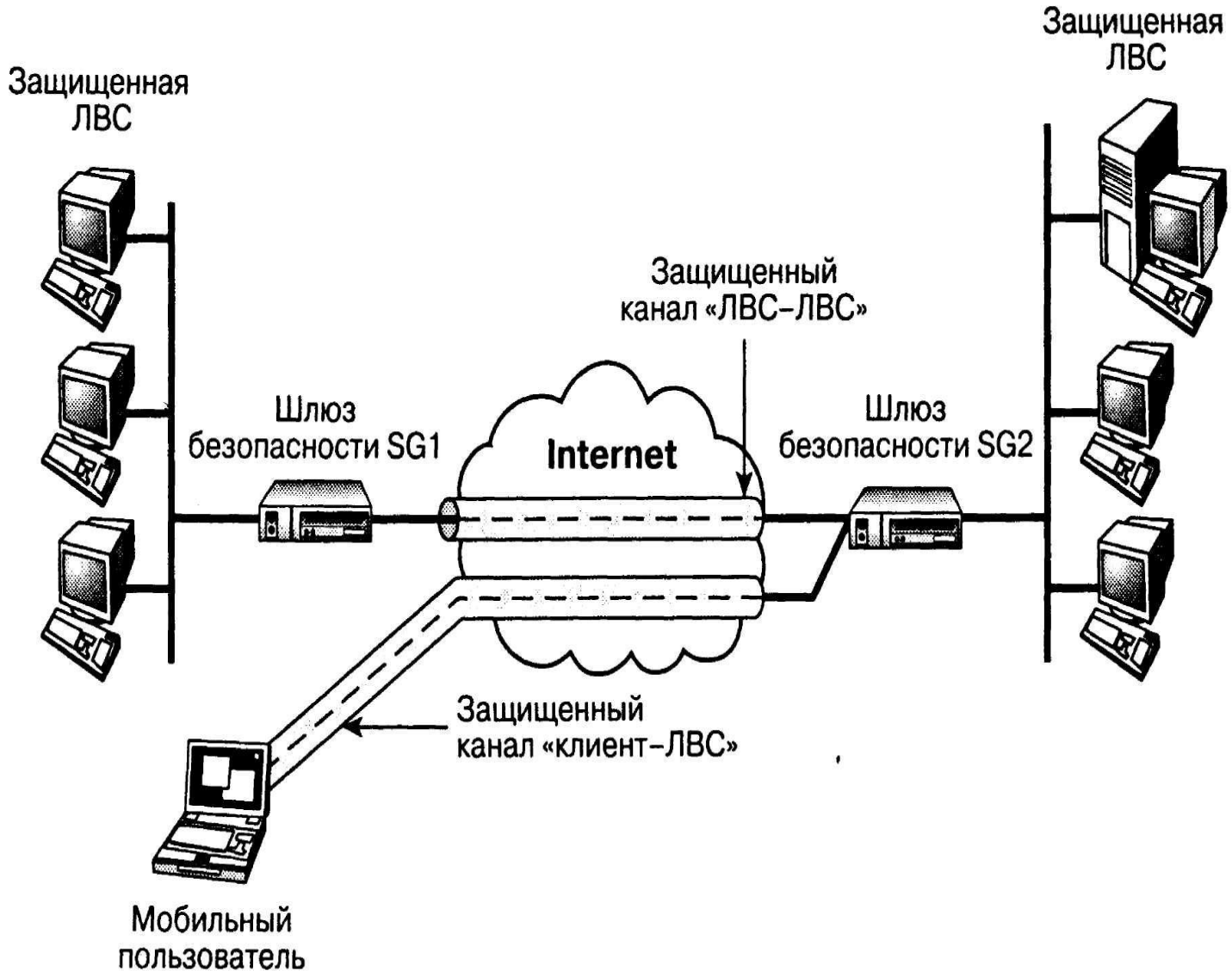
- обеспечение конфиденциальности и целостности передаваемых данных;

- авторизация и управление доступом;

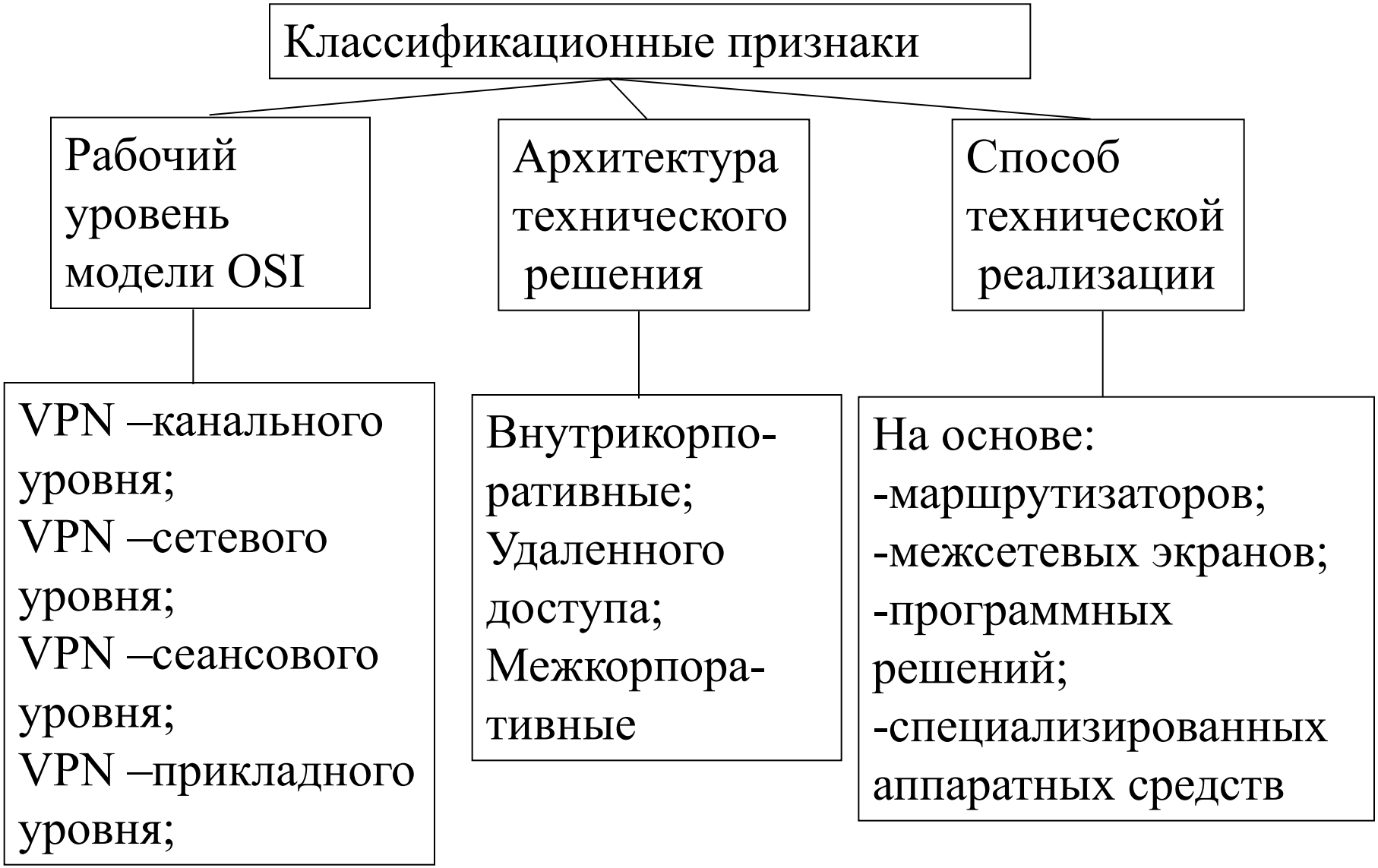
- обеспечение безопасности периметра сети, обнаружение вторжений;

- управление безопасностью сети, в том числе управление криптографическими ключами.

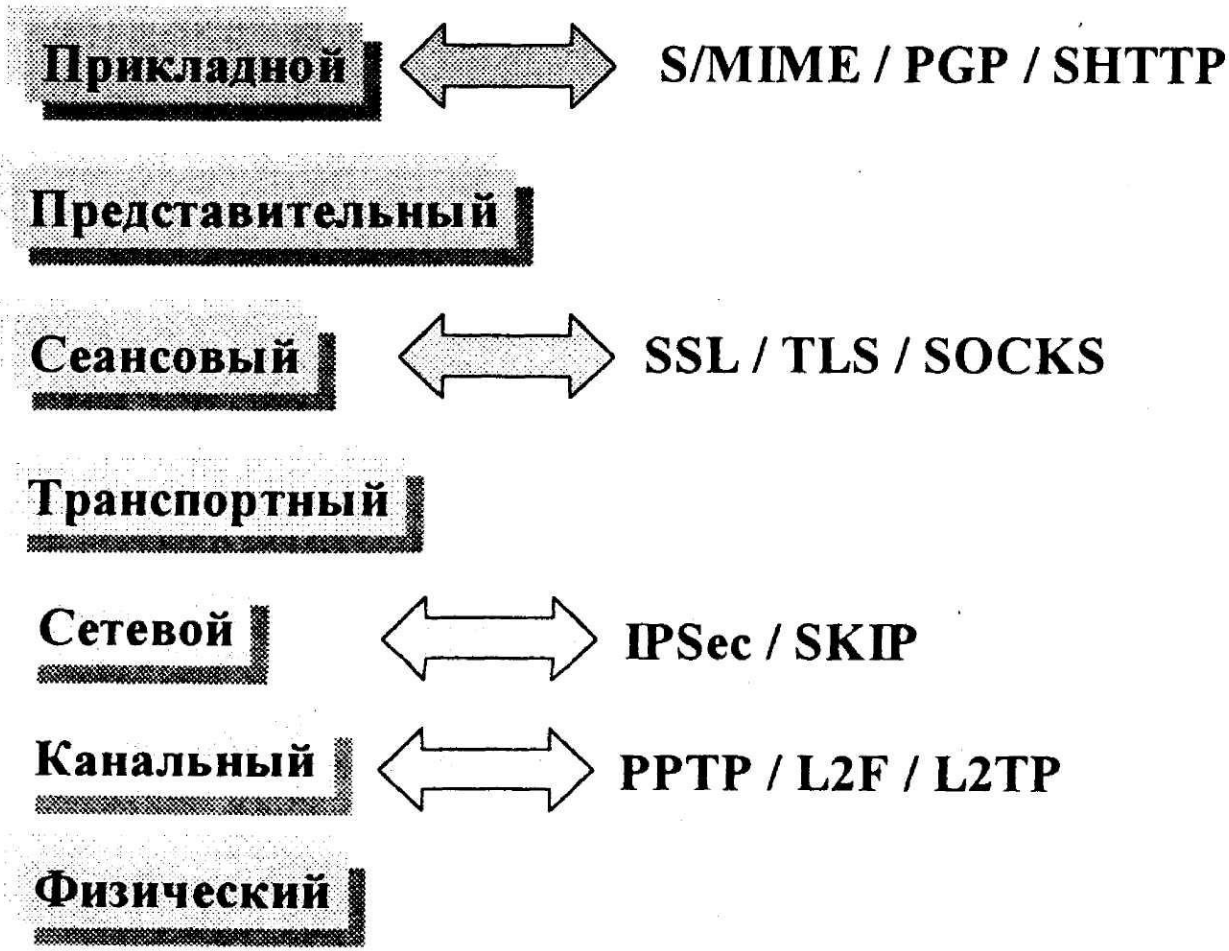
Основные схемы VPN



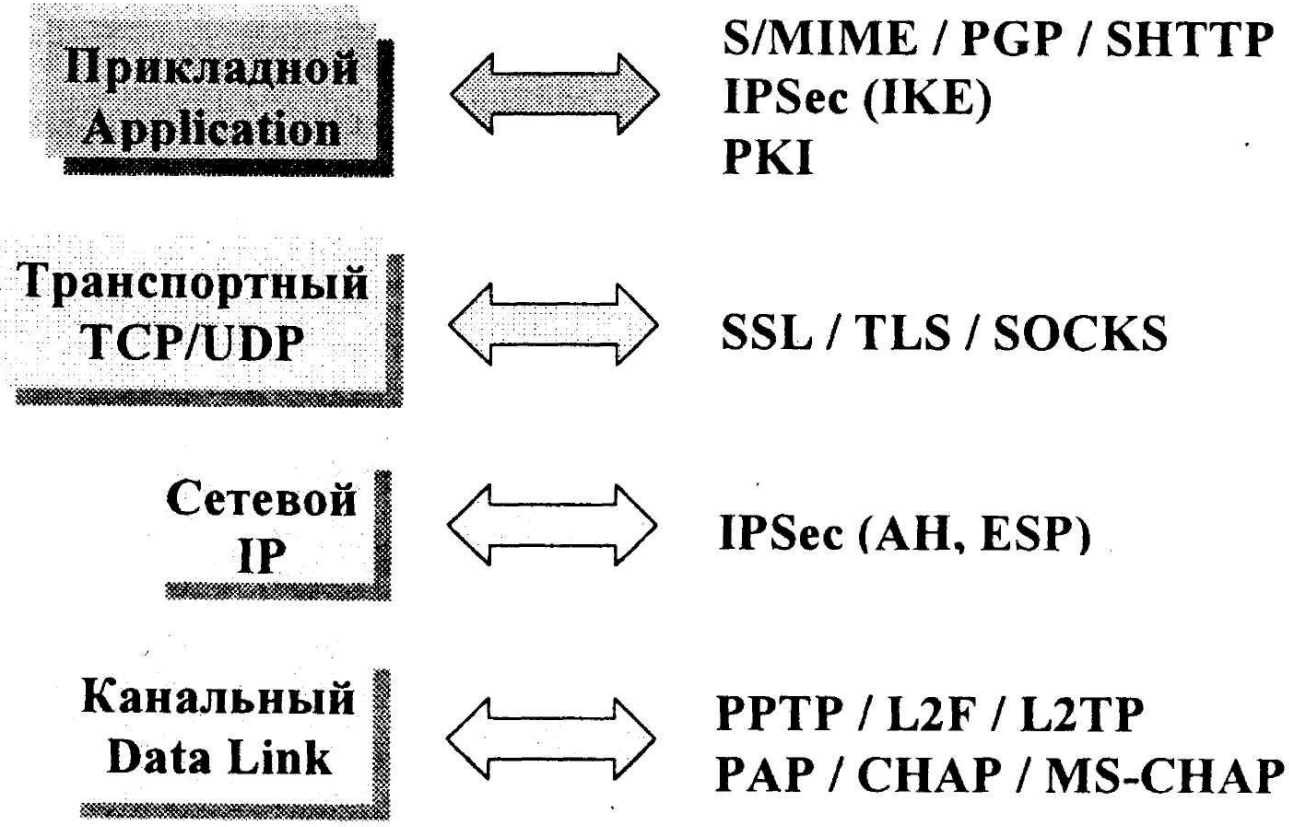
Классификация сетей VPN



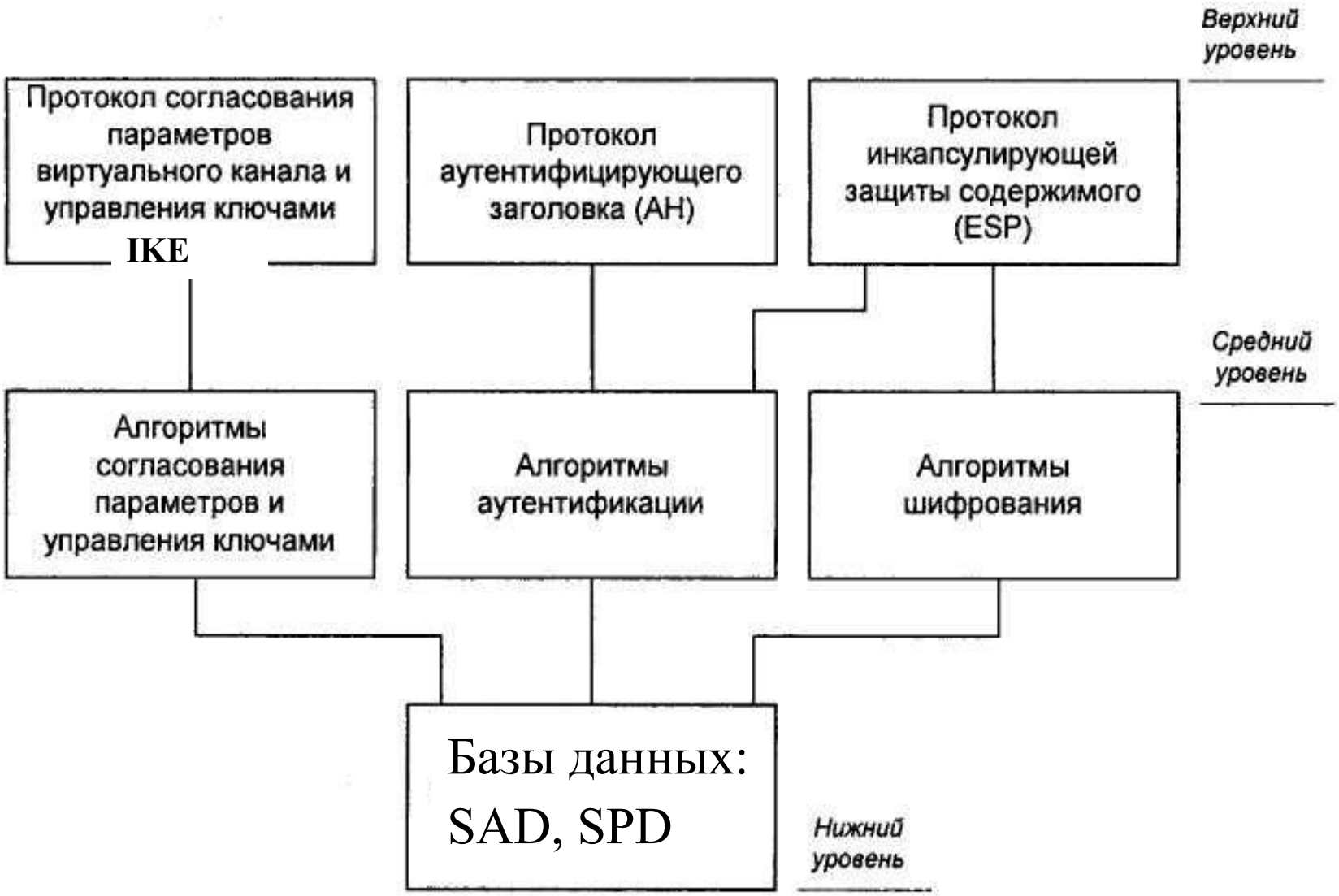
Протоколы защиты на различных уровнях модели ВОС



Протоколы защиты на различных уровнях протокола TCP/IP



Архитектура IPSec



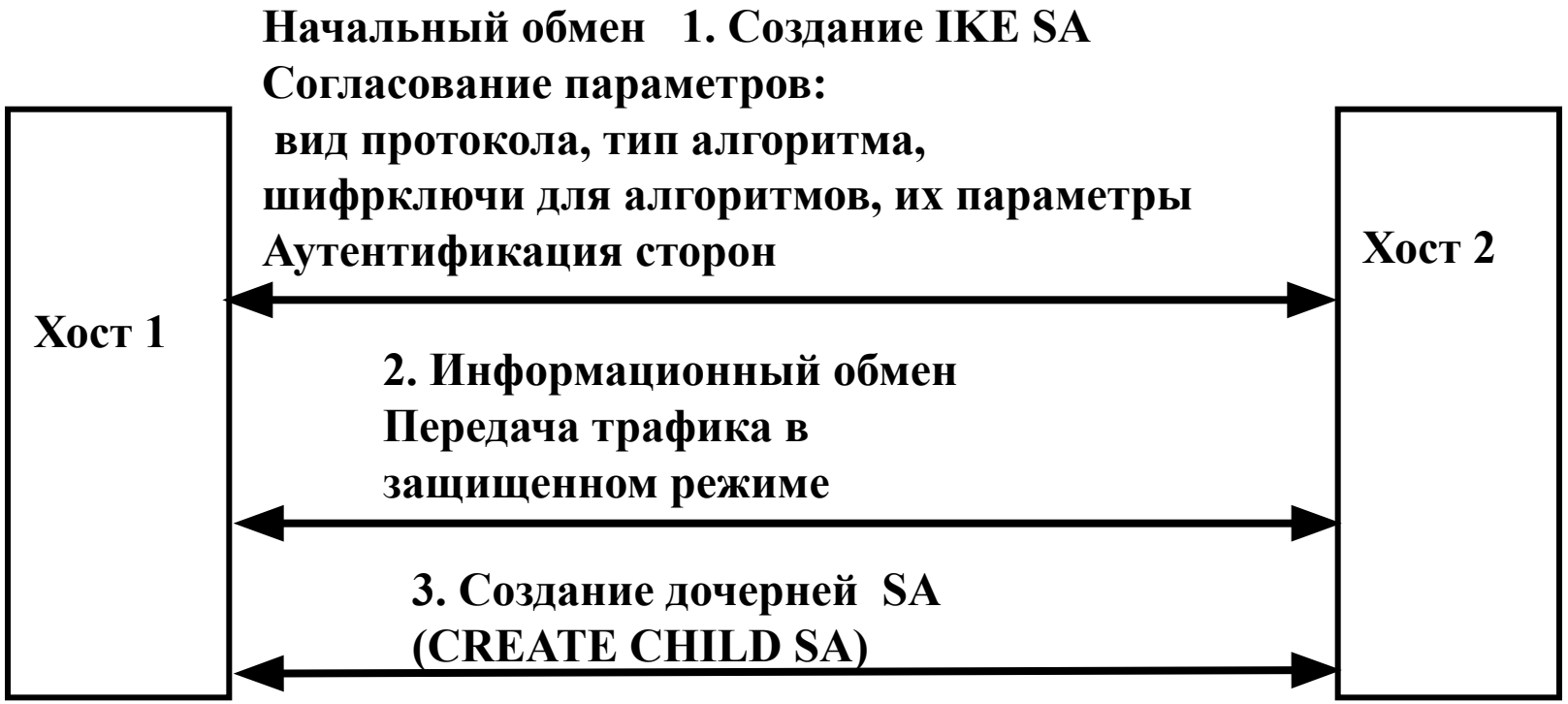
Security Association (SA)
Безопасная ассоциация
Контекст безопасности

SA однонаправленное логическое соединение, создаваемое для обеспечения безопасности.
SA – есть совокупность параметров соединения, позволяющим сервисам обеспечить безопасный трафик.

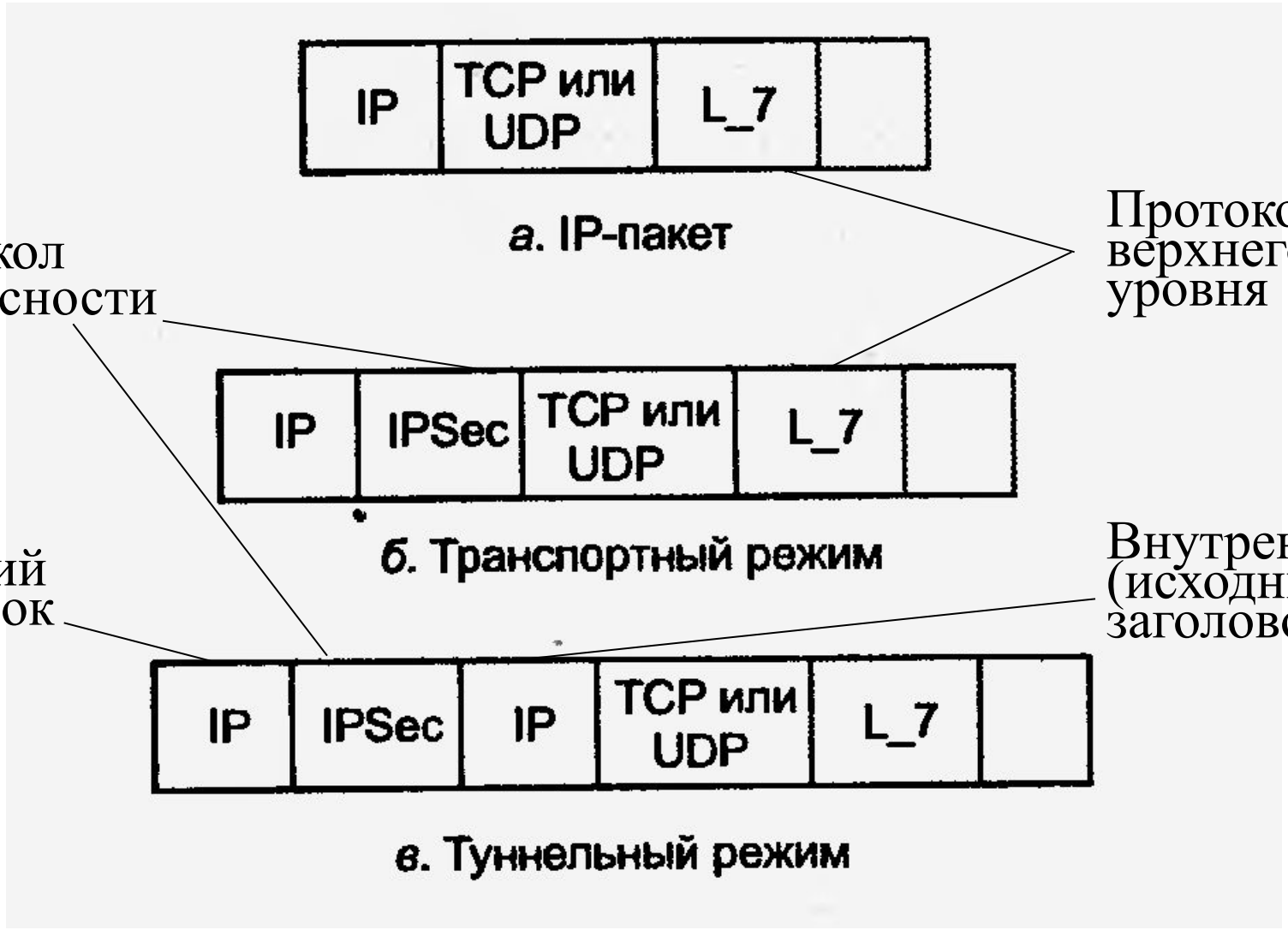
SA однозначно определяется тройкой:

-Security Parameter Index (SPI);
-IP Destination Address (Адрес назначения);
-Протокол безопасности: AH или ESP.

Установление безопасных ассоциации

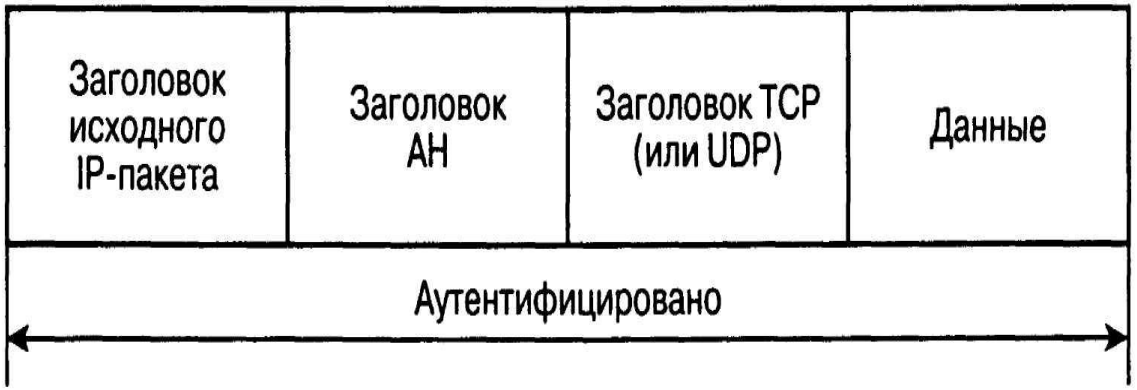


Режимы IPSec

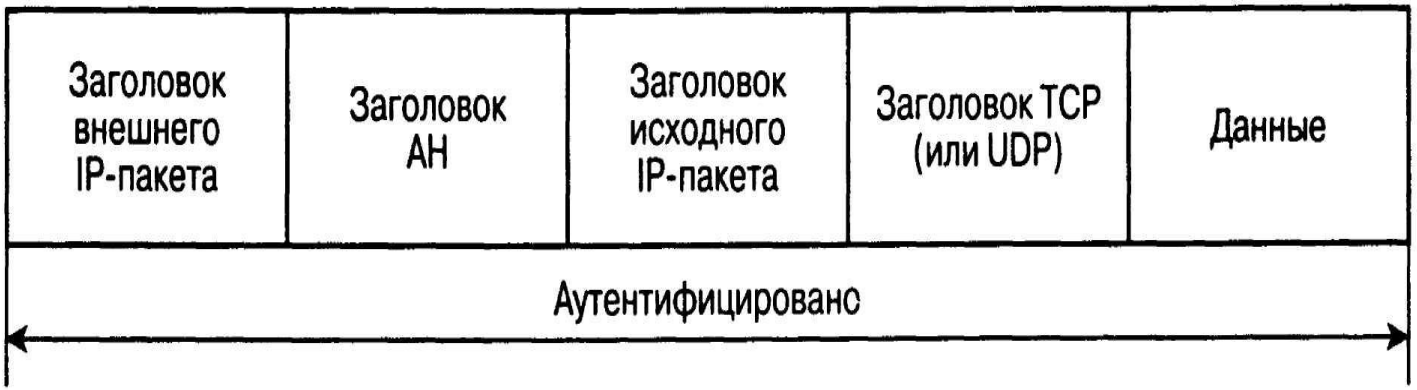


IP-пакет после применения протокола AH в транспортном и туннельном режимах

IP-пакет после применения протокола AH в транспортном режиме



IP-пакет после применения протокола AH в туннельном режиме



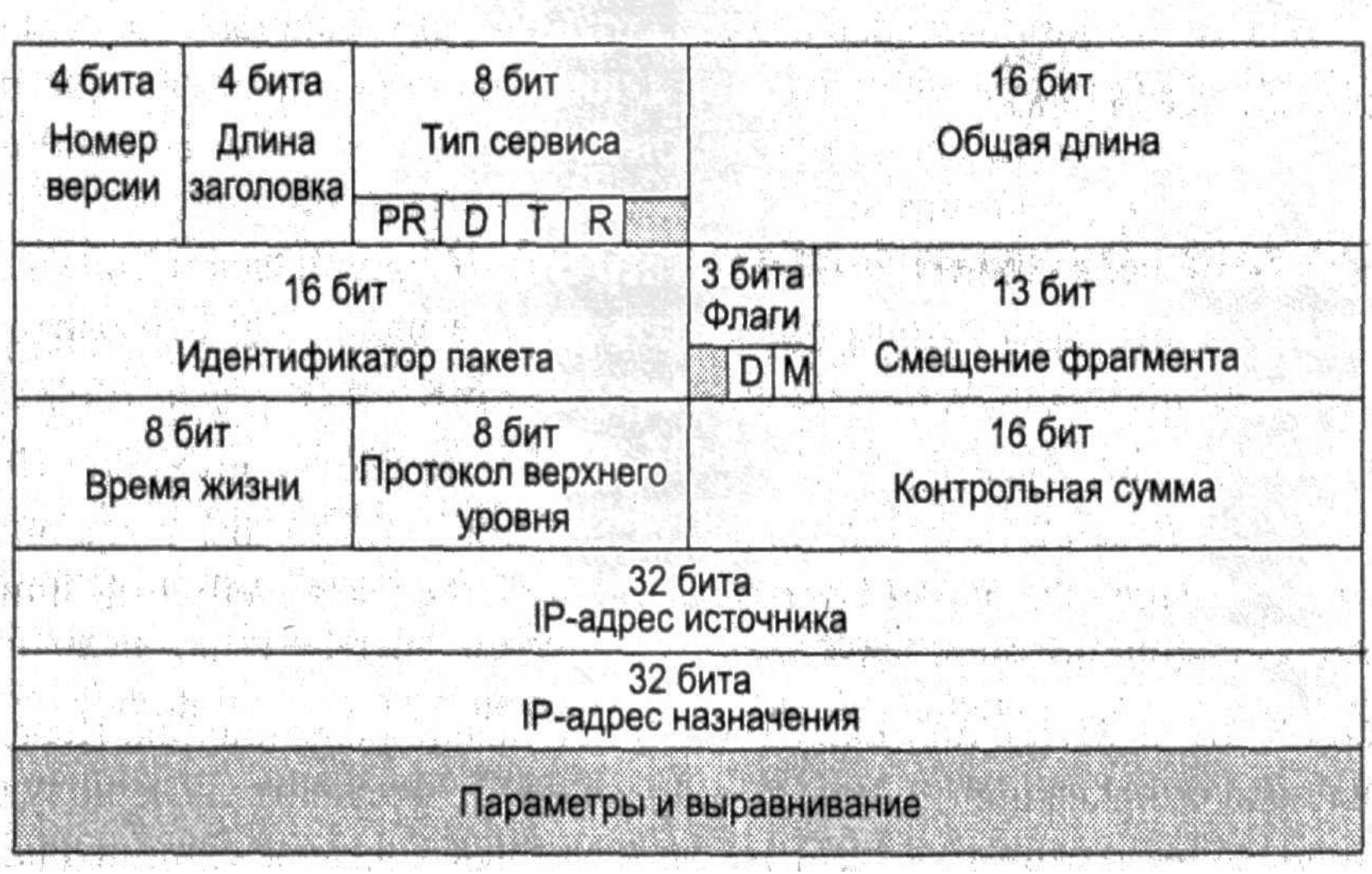
Характеристика протокола AH

Применение протокола AH позволяет принимающей стороне убедиться в следующем:

-содержание пакета не искажено, не изменено в процессе передачи (аутентификация сообщения);

-пакет не является дубликатом пакета переданного ранее

Структура заголовка IP-пакета



Формат заголовка AH

0	16	31
Следующий заголовок	Длина	Зарезервировано
Индекс параметров защиты SPI		
Порядковый номер SN		
Аутентификационные данные (переменная длина)		

Характеристика протокола ESP

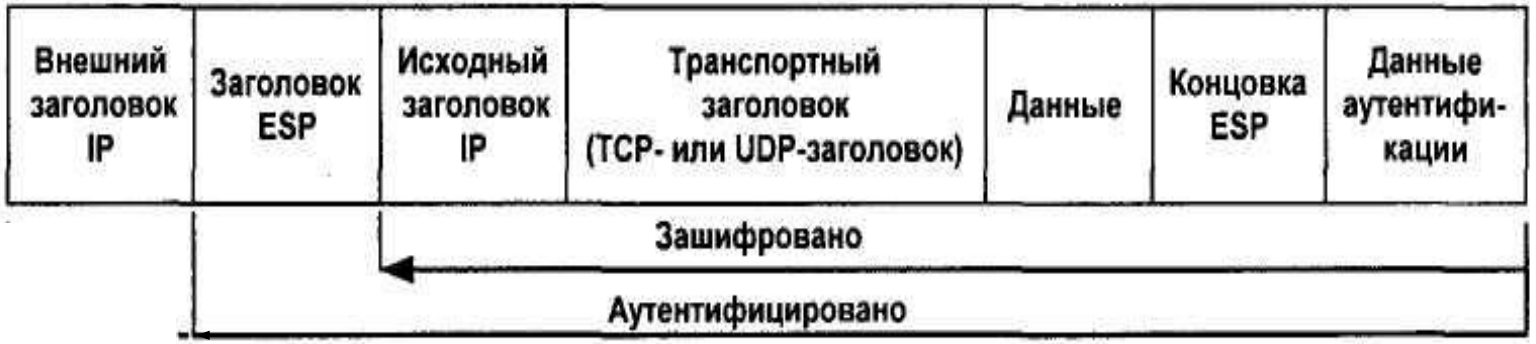
Применение протокола ESP обеспечивает:

- конфиденциальность передаваемых данных за счет их шифрования;
-целостность передаваемых данных;
-защиту от повторной передачи пакетов.

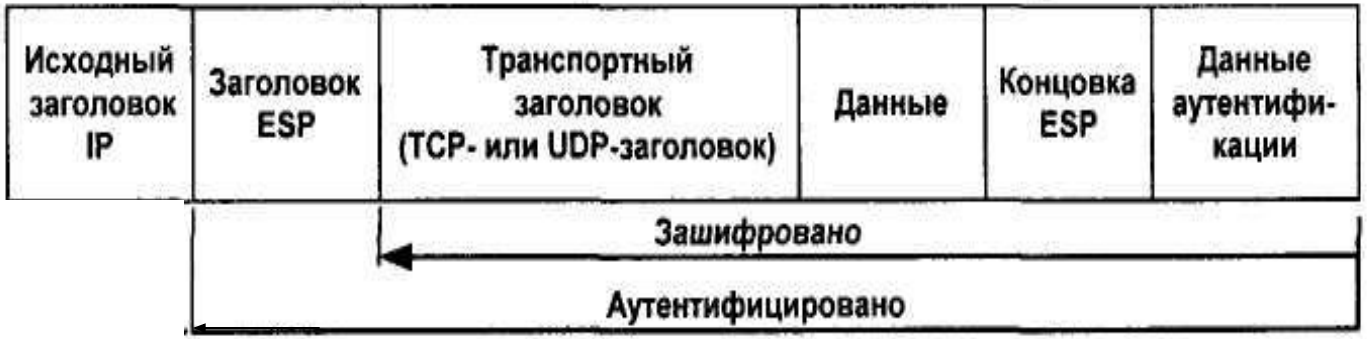
IP-пакет до и после применения протокола ESP

Исходный IP-пакет

IP-пакет после применения протокола ESP в туннельном режиме



IP-пакет после применения протокола ESP в транспортном режиме



Формат заголовка ESP

0	16	31
Индекс параметров защиты SPI		
Порядковый номер SN		
Данные (переменная длина)		
	Заполнитель Pad	
Заполнитель Pad	**Длина заполнителя**	**Следующий заголовок**
Аутентификационные данные (переменная длина)		

Хэширующие функции в АН

Хэширующие функции:

1) MD5-HMAC Длина ключа 128 бит, Хэш-код 96 бит.
2) SHA1-HMAC Длина ключа 160 бит, Хэш-код 96 бит.

Хэширующие функции MD2, MD5

MD5 (улучшенная версия MD4) :
-хэшируемое сообщение – блоки длиной 512 бит
- хэш-код- 128 бит,
-число раундов хэширования – 4.
- ориентирован на 32-разрядный процессор
MD2 :
-хэшируемое сообщение – блоки длиной 512 бит
- хэш-код- 128 бит,
-ориентирован на 8-разрядный процессор

Хэширующие функция SHA (Secure Hash Algorithm)

-хэшируемое сообщение – блоки длиной 512 бит

- хэш-код- 160 бит,

-число раундов хэширования – 4 (по 20 операций).

-ориентирован на 32-разрядный процессор

Алгоритмы шифрования в ESP

DES, 3-DES, CAST-128, RC-5, IDEA, Blowfish, AES

Алгоритмы аутентификации на основе хэш-функций:
MD5-HMAC , SHA1-HMAC.

Internet Key Exchange (IKE)

IKE v1
RFC 2409

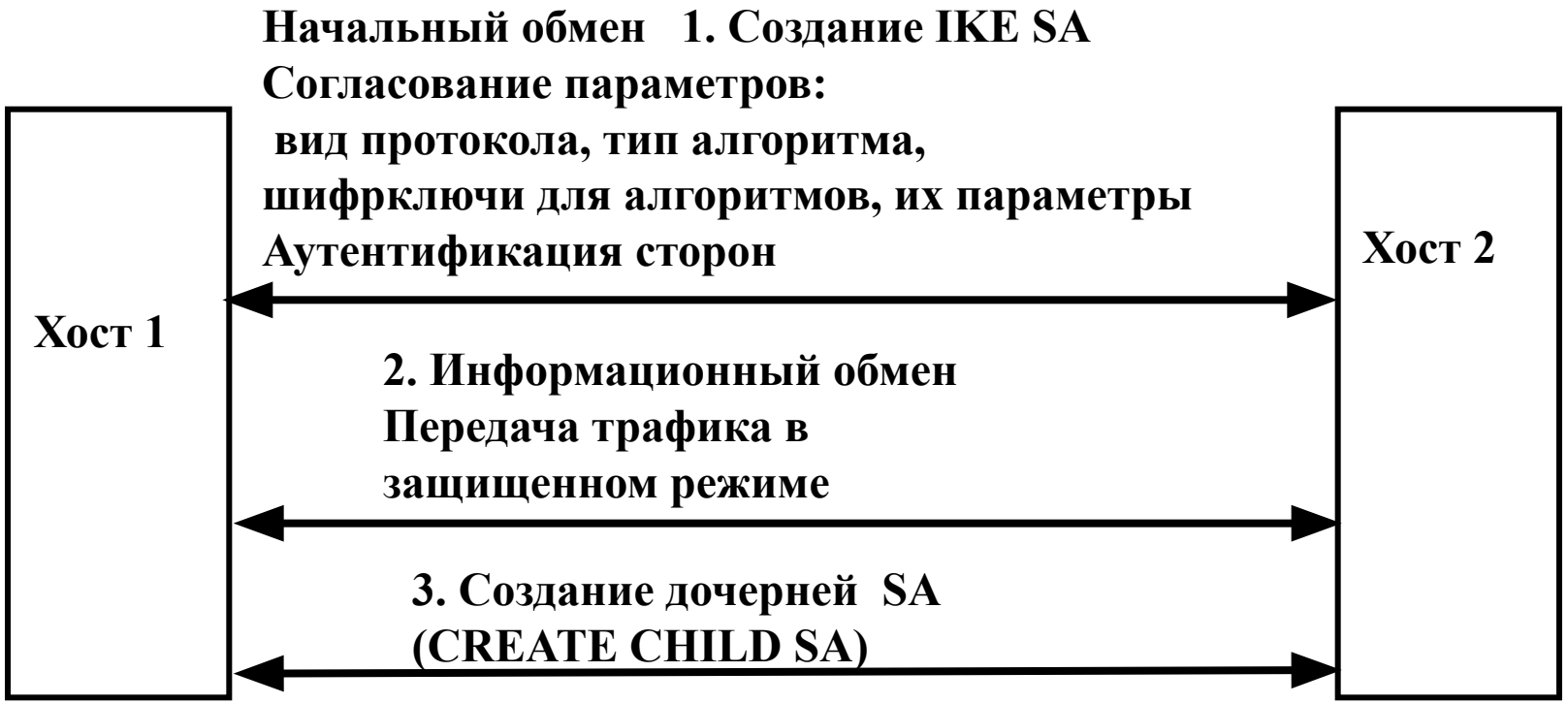
IKE v2
RFC 4306

ISAKMP
RFC 2408

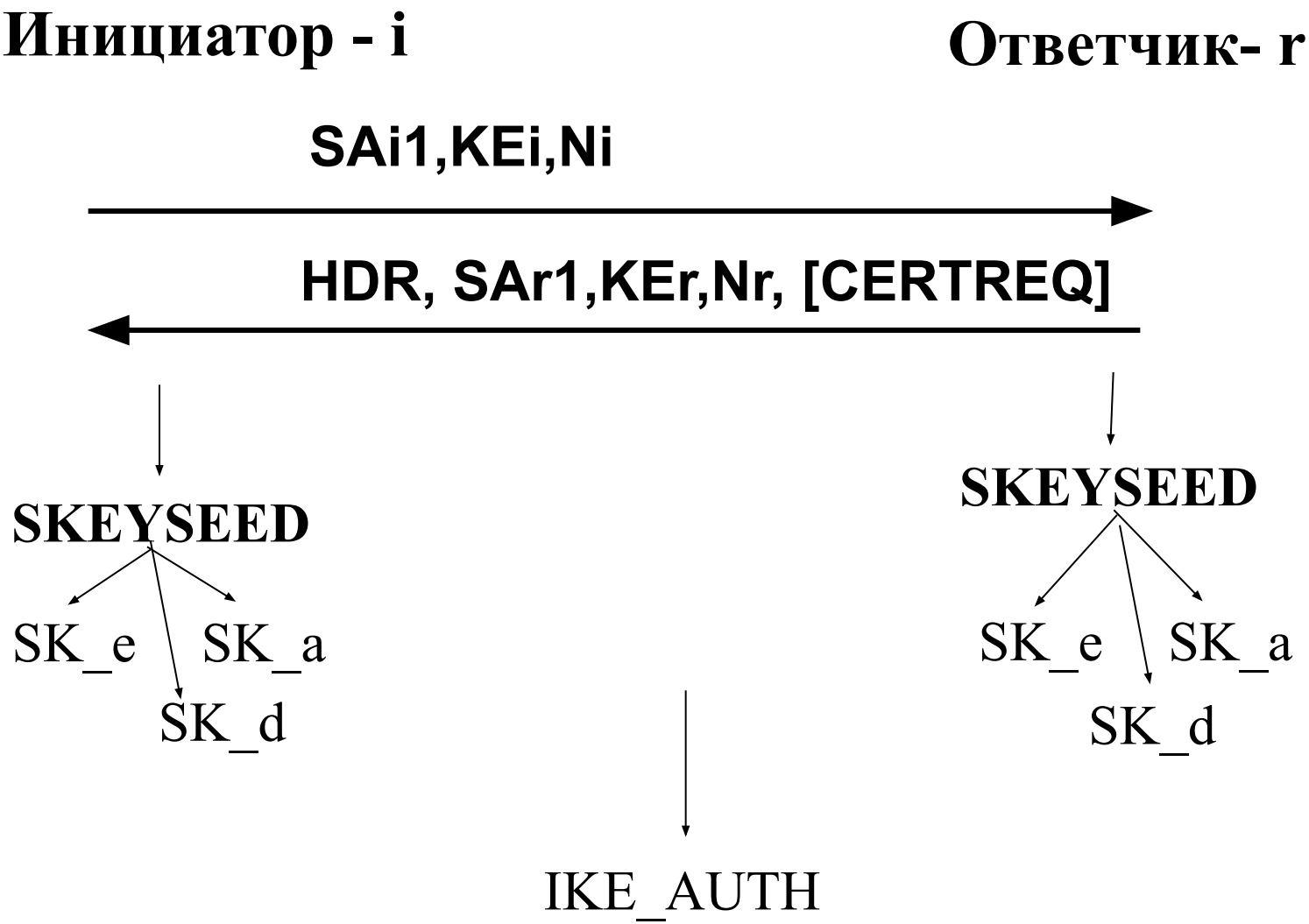
DOI
RFC 2407

Oakley

Установление безопасных ассоциации



Начальный обмен IKE_UNIT_ SA



Типы блоков данных

Тип следующего блока данных	Обозначение	Значение
No Next Payload (Следующий блок данных отсутствует)		0
RESERVED (зарезервированы)		1-32
Security Association (Контекст Безопасности)	SA	33
Key Exchange (Обмен Ключами)	KE	34
Identification - Initiator (Идентификация - инициатор)	IDi	35
Identification - Responder (Идентификация - ответчик)	IDr	36
Certificate (Сертификат)	CERT	37
Certificate Request (Запрос Сертификата)	CERTREQ	38
Authentication (Аутентификация)	AUTH	39
Nonce (Одноразовый Номер)	Ni, Nr	40
Notify (Уведомление)	N	41
Delete (Удаление)	D	42
Vendor ID (Идентификатор Поставщика)	V	43
Traffic Selector - Initiator (Селектор Трафика - инициатор)	TSi	44
Traffic Selector - Responder (Селектор Трафика - ответчик)	TSr	45
Encrypted (Шифр)	E	46
Configuration (Конфигурирование)	CP	47
Extensible Authentication (Расширяемая Аутентификация)	EAP	48
RESERVED TO IANA (Зарезервированы для IANA)		49-127
PRIVATE USE (Для частного использования)		128-255

Обмен IKE_AUTH

Инициатор - i **Ответчик- r**

SK{IDi, [CERT], [CERTREQ], IDr, AUTH, SAi2, }

SK{IDr, [CERT], AUTH, SAr2},

(AH,ESP) CHILD_SA

Типы и идентификаторы преобразований

Тип пробразо-вания	Значение типа пробразования	Алгоритмы преобразования	Используется в протоколах
1	Шифрование (ENCR)	DES, DES IV32, DES IV128, 3DES, IDEA, RC5, CAST, Blowfish, 3IDEA, AES CBC, AES CTR	IKE, ESP
2	Псевдослучайная функция (PRF)	HMAC MD5, HMAC SHA1, HMAC TIGER, AES 128 CBC	IKE
3	Проверка целостности (INTEG)	HMAC MD5 96, HMAC SHA1 96, DES MAC, KPDK MD5, AES XCBC 96	IKE, AH, ESP
4	Тип группы Диффи-Хеллмана (DH)	Указывается номер группы	IKE, опция в AH, ESP
5	Расширение порядкового номера (ESN)		IKE, опция в AH, ESP

Содержимое поля Аутентификационные данные при аутентификации с использованием цифровых подписей

Инициатор - i

AUTH = SIGi{(SAi1,KEi,Ni),Nr,prf(SK_pi,IDi’}

Ответчик- r

AUTH = SIGr{(SAr1,KEr,Nr),Ni,prf(SK_pr,IDr’}

Содержимое поля Аутентификационные данные при аутентификации с использованием заранее распределенного ключа

AUTH = prf(prf(Shared Secret, “Key Pad for IKEv2”,

(<msg octets’}

Генерация ключевого материала для IKE_SA

```
SKEYSEED = prf(Ni | Nr, g^ir)

{SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr }
        = prf+ (SKEYSEED, Ni | Nr | SPIi | SPIr )
```

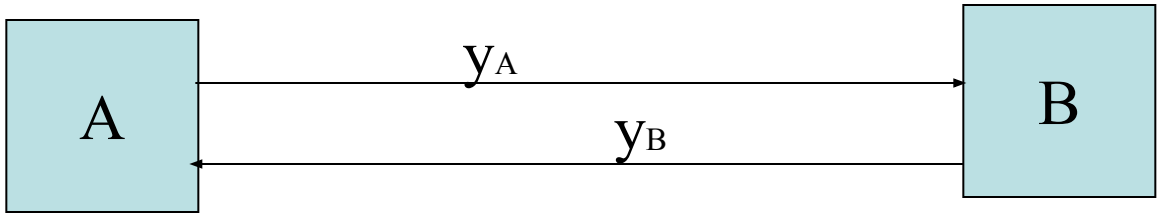
SK_d используется для получения новых ключей для CHILD_SA;
SK_ai, SK_ar – ключи аутентификации сообщений в
SK_ei, SK_er - ключи шифрования сообщений
SK_pi, SK_pr - ключи хэширующей функции

Генерация ключевого материала в дополнительном обмене CREATE_CHILD_SA

```
KEYMAT = prf+(SK_d, Ni | Nr)
```

Ключи шифрования берутся из первых октетов KEYMAT
ключи аутентификации из следующих октетов

Алгоритм формирования ключей на основе однонаправленных функций (алгоритм Диффи-Хеллмана)



А генерирует большое случайное число x_A, $1 \le x_A \le p-1$, p - простое число. Число x_A сохраняется в секрете. Вычисляет число $y_A = \alpha^{x_A} (\mathrm{mod}\, p)$, где α - примитивный элемент поля $GF(p)$, которое передает корреспонденту В.

В генерирует x_B, аналогичным образом вычисляет число y_B, которое передает корреспонденту А.

А, приняв от В y_B, вычисляет

$$K_A = (y_B)^{x_A} \bmod p = (\alpha^{x_B})^{x_A} \bmod p = \alpha^{x_B x_A} \bmod p .$$

В, приняв y_A, вычисляет

$$K_B = (y_A)^{x_B} \bmod p = (\alpha^{x_A})^{x_B} \bmod p = \alpha^{x_A x_B} \bmod p .$$

$$K_A = K_B = K .$$

Ключ K может быть использован в симметричной системе шифрования.

Сравнительная характеристика VPN продуктов отечественного производства

	ШИП	Застава	ФПСУ-IP	VipNet	Континент-К	Криптон-IP
Производитель	**МО ПНИЭИ**	**Элвис+**	**Амикон**	**Инфо-Текс**	**Информзащита**	**Анкад**
Операц. система	FreeBSD	Win NT/95/98 Sparc/Intel Solaris	Собственная	Win NT/95/98/ ME/2000 Linux	Win NT	MS-DOS 5.0 и выше
Сертификат ГТК или ФАПСИ	Сертиф. ФАПСИ	Класс 3	Класс 3	Класс 1В для АС и класс 3 МЭ	Класс 3	Принят в сертиф.
Использование ГОСТ	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89
Фильтрация с учетом любых значимых полей сетевых пакетов	Да	Да	Да	Да	Да	Н/д
Фильтрация на транспортн. уровне запросов	Да (TCP/ UDP)	Да (TCP/ UDP)	Да (TCP/ UDP)	Да (TCP/ UDP)	Да (TCP/ UDP)	Н/д

Сравнительная характеристика российских VPN-продуктов

Трансляция номеров портов/сетев. адресов	**-/+**	**-/+**	**-/+**	**-/+**	**-/+**	**Н/д**
Аутентифика-ция трафика	**Да, хэш-е по ГОСТ Р 34.11-94**	**Да, хеш ф-ция по алг. MD-5**	**Да, хэш-е по ГОСТ Р 34.11-94**	**Нет**	**Да, реж. ими-вки по ГОСТ 28147-89**	**Да, односто-рон. аутент. с имитовст.**
Базовый протокол	**SKIP**	**SKIP**	**Собствен ный**	**Собствен ный**	**Собствен ный**	**Собствен ный**
Расходы на поддержку туннелей	**112 байт на пакет**	**112 байт на пакет**	**18-20 байт на пакет**	**30-80 байт на пакет**	**26-36 байт на пакет**	**Н/д**
Кол-во одновременно туннелей	**Н/д**	**1400**	**до1024 на кажд. сет. интерф.**	**Win. 50, Linux -300**	**не более 500 на кажд КШ**	**Н/д**
Возможность каскадирован. туннелей	**Да**	**Да**	**Да**	**Н/д**	**Н/д**	**Н/д**
Пропускная способность Мбит/с	**8 (P-200)**	**8 (P-200)**	**11 (P-200)**	**9,5 (P-III/450)**	**17,4 (Cel. 500)**	**1,2-1,8 (Intel 486)**
Цена, долл.	**Н/д**	**2500-3000**	**1000-1500**	**Н/д**	**Н/д**	**350**