Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра сетей и устройств телекоммуникаций

М.Н. Бобов

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ VPN

УЧЕБНОЕ ПОСОБИЕ
по курсам «Защита информации в банковских технологиях»,
«Защита программного обеспечения и баз данных в сетях телекоммуникаций»,
«Криптографическая защита информации в телекоммуникациях»
для студентов специальности 45 01 03 «Сети телекоммуникаций»
дневной и заочной форм обучения

Минск 2005

УДК 621.395.3 (075.8)
ББК 32.882 я 73
Б 72

Р е ц е н з е н т:
доцент кафедры радиотехнических систем А.И. Митюхин

Бобов М.Н.

Б 72 Механизмы защиты информации в корпоративных VPN: Учеб. пособие по курсам «Защита информации в банковских технологиях», «Защита программного обеспечения и баз данных в сетях телекоммуникаций», «Криптографическая защита информации в телекоммуникациях» для студ. спец. 45 01 03 «Сети телекоммуникаций» дневной и заочной форм обуч. / М.Н. Бобов.– Мн.: БГУИР, 2005. – 22 с.: ил.
ISBN 985-444-775-8

В учебном пособии рассмотрены методы защиты информации при построении корпоративных VPN. Рассмотрены технология построения VPN и архитектура безопасности на уровне спецификаций IPSec. Приведено описание протоколов спецификаций IPSec, реализующих механизмы защиты информации при передаче сообщений по незащищённым каналам связи, и изложены рекомендации по их использованию.

УДК 621.395.3 (075.8)
ББК 32.882 я 73

ISBN 985-444-775-8

ТЕХНОЛОГИЯ VPN

Термином VPN (virtual private network – виртуальная частная сеть) обозначают участников защищённого соединения, где в качестве транспорта используется протокол IP и механизмы защиты применяются на сетевом уровне. Технология VPN заключается в применении криптографических методов для обеспечения конфиденциальности и целостности данных, пересылаемых по незащищённой сети, и характеризуется двумя основными признаками:

• средой передачи данных обычно служат сети общего пользования, такие, как Интернет или корпоративная сеть без дополнительных механизмов защиты;

• криптографические механизмы накладываются на третьем (сетевом) уровне модели OSI или между третьим и вторым уровнем.

Это создаёт у пользователя иллюзию изолированности от подавляющего большинства узлов сети общего пользования и создания «внутри неё» *виртуальной сети* из нескольких абонентов, которые владеют одинаковыми VPN-средствами с одинаковыми криптографическими ключами.

В рассматриваемой технологии имеют место две возможные схемы применения механизмов защиты.

1. Схема «сеть – сеть», когда протоколы безопасности применяются только к пакетам, выходящим из локальной сети, и прекращают своё действие при входе пакета в локальную сеть (обмен данными осуществляется между двумя хостами двух локальных сетей). В этом случае необходимо учитывать, что внутри локальных сетей пакеты не защищены.

2. Схема «точка – сеть» – обычно используется при удалённой работе пользователя с сетью организации. При этом как типовой вариант предполагается, что удалённый компьютер по модемной линии через сеть общего пользования подключается к серверу удалённого доступа локальной сети. В

этом случае предполагается, что трафик, идущий между сервером доступа и удалённым компьютером, может быть не защищён.

Смысловое содержание VPN поясняется на схеме, приведенной на рис.1.

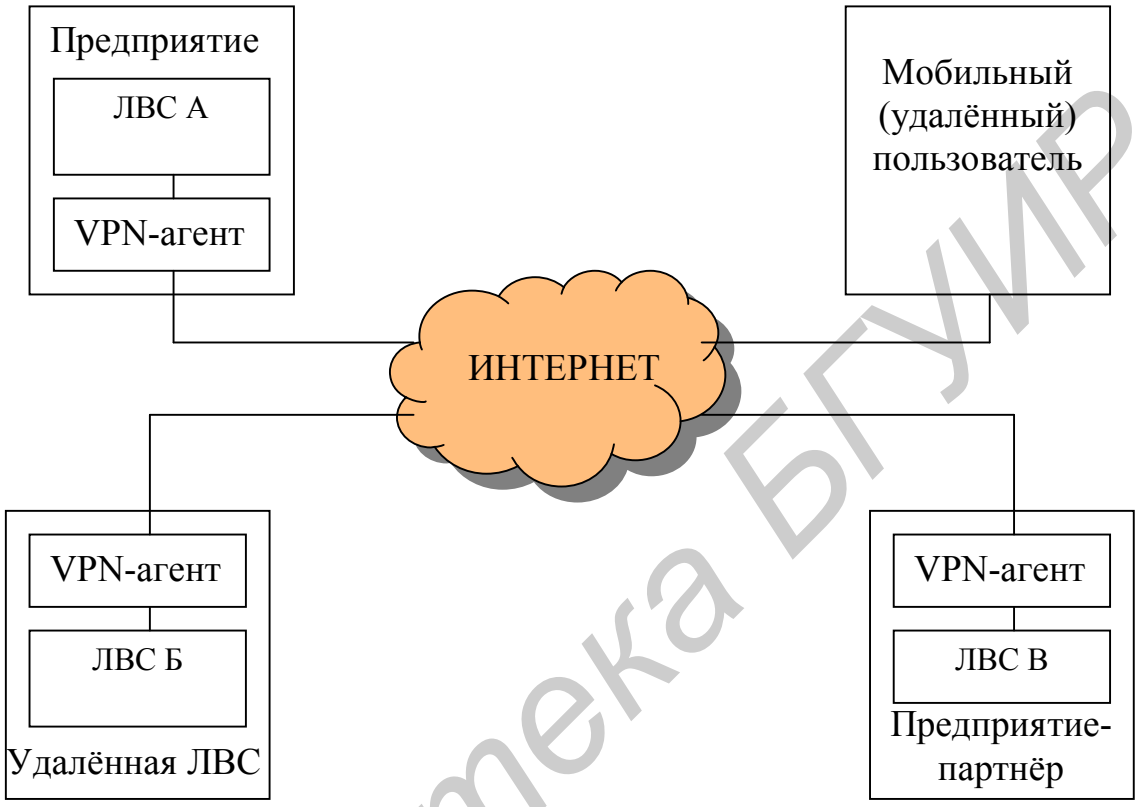


Рис.1. Схема VPN

Здесь защита передаваемой по сети информации осуществляется на выходе из каждой ЛВС с помощью VPN-агента, причём никаких других связей, минующих барьер в виде VIP-агента, категорически не допускается. Другими словами, должен быть определён защищаемый периметр, связь с которым может осуществляться только через соответствующее средство защиты.

VPN-агенты могут быть реализованы на базе:

• сетевых операционных систем;

• маршрутизаторов;

• межсетевых экранов;

• специализированного программного обеспечения.

VPN-агенты при отправке любого IP-пакета производят следующие действия:

1) из заголовка IP-пакета выделяется информация об его адресате, на основе которой выбираются алгоритмы защиты и криптографические ключи для данного пакета;

2) формируется и добавляется в IP-пакет код проверки целостности или электронная цифровая подпись;

3) производится зашифрование IP-пакета;

4) зашифрованный IP-пакет инкапсулируется в пакет, адресатом которого является VPN-агент получателя, производится отправка пакета.

При приёме IP-пакета VPN-агенты выполняют следующие действия:

1) из заголовка IP-пакета выделяется информация об отправителе, на основе которой выбираются алгоритмы защиты и криптографические ключи для расшифрования пакета и проверки его целостности;

2) выделяется информационная (инкапсулированная) часть пакета и производится её расшифрование;

3) осуществляется проверка целостности пакета на основе выбранного алгоритма;

4) пакет отправляется адресату согласно информации, находящейся в его оригинальном заголовке.

Таким образом, вся передаваемая информация защищена как от несанкционированного просмотра, так и от модификации. Кроме того, инкапсуляция пакетов позволяет скрыть топологию внутренней сети и тем самым защититься от угрозы подмены пакетов.

Технологии VPN могут включать в себя схемы защиты собственной разработки различных производителей, однако предпочтительным является

использование стандартного протокола безопасности IP-Security Protocol (IPSec).

1. АРХИТЕКТУРА БЕЗОПАСНОСТИ НА УРОВНЕ IPSec

Спецификации IPSec определяются целым рядом документов. Наиболее важными из них являются следующие:

RFC 2401 – Архитектура безопасности для IP;

RFC 2402 – Описание расширений аутентификации пакетов IP;

RFC 2406 – Описание расширений шифрования пакетов IP;

RFC 2408 – Спецификации средств управления ключами.

В соответствии с указанными документами средства защиты реализуются в виде заголовков расширений, которые следуют за основным заголовком IP. Заголовок расширения аутентификации называют заголовком AH (Authentication Header – заголовок аутентификации), а заголовок расширения шифрования – заголовком ESP (Encapsulating Security Payload header – заголовок защищённого полезного груза или заголовок защищённого содержимого).

В дополнение к этим четырём документам протокол IPSec включает ещё семь групп документов (рис.2).

Архитектура. Содержит описание общих принципов, требований защиты, а также определения и механизмы реализации технологии IPSec.

Безопасное сокрытие значимых данных (ESP). Описание формата пакета и общих принципов использования ESP для шифрования и аутентификации пакетов.

Заголовок аутентификации (AH). Описание формата пакета и общих принципов использования AH для аутентификации пакетов.

Алгоритм шифрования. Набор документов, определяющих использование различных алгоритмов шифрования для ESP.

Рис.2. Общая структура документов IPSec.

Алгоритм аутентификации. Набор документов, определяющих использование различных алгоритмов аутентификации для AH и для опции аутентификации ESP.

Управление ключами. Документы, описывающие схемы управления ключами.

Область интерпретации. Содержит значения, необходимые для соответствия одних документов другим. Это, в частности, идентификаторы проверенных алгоритмов шифрования и аутентификации, а также некоторые параметры, например, продолжительность жизненного цикла ключей.

IPSec обеспечивает сервис защиты на уровне IP, позволяя системе выбрать необходимые протоколы защиты, определить алгоритм для соответствующего сервиса и задать значения любых криптографических ключей, требующихся для запрашиваемого сервиса. Для защиты используется два протокола: протокол аутентификации, указанный заголовком аутентификации

АН, и комбинированный протокол шифрования/аутентификации, определённый форматом пакета для протокола ESP. В таблице 1 показаны сервисы, обеспечиваемые применением указанных протоколов.

Ключевым элементом реализации указанных сервисов является защищённая связь (SA – security association). Связь представляет собой одностороннее отношение между отправителем и получателем, применяющим сервис защиты к транспортному потоку. Если требуется равноправное отношение для двухстороннего защищённого обмена, необходимы две защищённые связи. Сервис защиты даёт возможность для защищённой связи использовать либо АН, либо ESP, но никак не оба протокола одновременно.

Табл. 1

Наименование сервиса	Протокол АН	Протокол ESP (только шифрование)	Протокол ESP (шифрование и аутентификация)
Управление доступом	×	×	×
Целостность без установки соединений	×		×
Аутентификация источника данных	×		×
Защита от воспроизведения пакетов	×	×	×
Конфиденциальность		×	×
Конфиденциальность потока		×	×

Защищённая связь однозначно определяется следующими тремя параметрами.

Индекс параметров защиты. Строка битов, присваиваемая конкретной защищённой связи. Индекс параметров защиты передаётся в заголовках AH и ESP, чтобы принимающая система имела возможность выбрать защищённую связь, в рамках которой должен обрабатываться принимаемый пакет.

Адрес IP пункта назначения. Адрес пункта назначения защищённой связи, который может представлять систему конечного пользователя или сетевой объект тапа VPN-агента.

Идентификатор протокола защиты. Этот идентификатор указывает, является ли данная защищённая связь защищённой связью AH или это защищённая связь ESP.

Механизм управления ключами связывается с механизмами аутентификации и конфиденциальности только через параметры защиты. Таким образом, он может быть определён независимо от механизмов аутентификации и конфиденциальности.

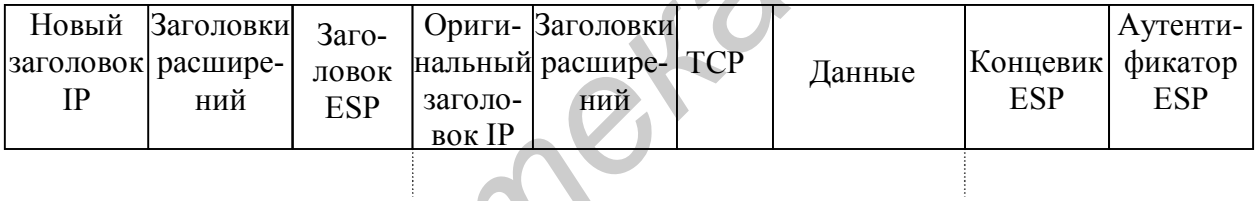
2. ПРОТОКОЛЫ ЗАЩИТЫ VPN

Протоколы защиты реализуются VPN-агентами с использованием механизма защищённых связей. Рассмотрим пример реализации защищённой связи между абонентами ЛВС А и ЛВС Б (рис.1.). Абонент ЛВС А генерирует пакет IP с адресом абонента получателя в ЛВС Б, который направляется к VPN-агенту. VPN-агент выполняет функции IPSec, т.е. добавляет заголовок AH или ESP, и инкапсулирует оригинальный пакет во внешний пакет IP. Адресом IP отправителя этого внешнего пакета будет данный VPN-агент, формирующий границу ЛВС А. Теперь пакет направляется VPN-агенту ЛВС Б, а промежуточные маршрутизаторы будут иметь дело только с внешним заголовком IP. В VPN-агенте ЛВС Б внешний заголовок IP удаляется, а внутренний пакет доставляется абоненту ЛВС Б. На рис.3. показано преобразование

пакета IP в VPN-агенте для образования защищенной связи между ЛВС А и ЛВС Б.

При использовании протокола AH весь внутренний пакет, включая весь оригинальный заголовок IP, защищается средствами AH. Внешний заголовок IP защищается с исключением изменяемых и непрогнозируемых по значению полей во время прохождения пакета по сети.

а



б

Рис. 3. Область действия VPN-агента:
а – протокол AH; б – протокол ESP

При использовании протокола ESP заголовок ESP добавляется к пакету как префикс, а затем пакет вместе с концевиком ESP зашифровываются. Поскольку заголовок IP содержит адрес пункта назначения и директивы исходной маршрутизации вместе с информацией о параметрах транзита, нельзя просто передать зашифрованный пакет с добавленным к нему в виде префикса заголовком ESP. Промежуточные маршрутизаторы не смогут обработать

такой пакет. Таким образом, необходимо включить весь блок (заголовок ESP, зашифрованные данные и данные аутентификации) во внешний пакет IP с новым заголовком.

2.1. Протокол AH

Заголовок аутентификации (AH) обеспечивает поддержку целостности данных и аутентификацию пакетов IP. Функция аутентификации позволяет VPN-агенту идентифицировать пользователя или приложение, а также защититься от очень распространённых сегодня в Интернете атак с подменой сетевых адресов и несанкционированного воспроизведения сообщений. Аутентификация опирается на использование кодов аутентичности сообщений, при этом две стороны должны использовать общий секретный ключ.

Заголовок аутентификации состоит из следующих полей (рис. 4).

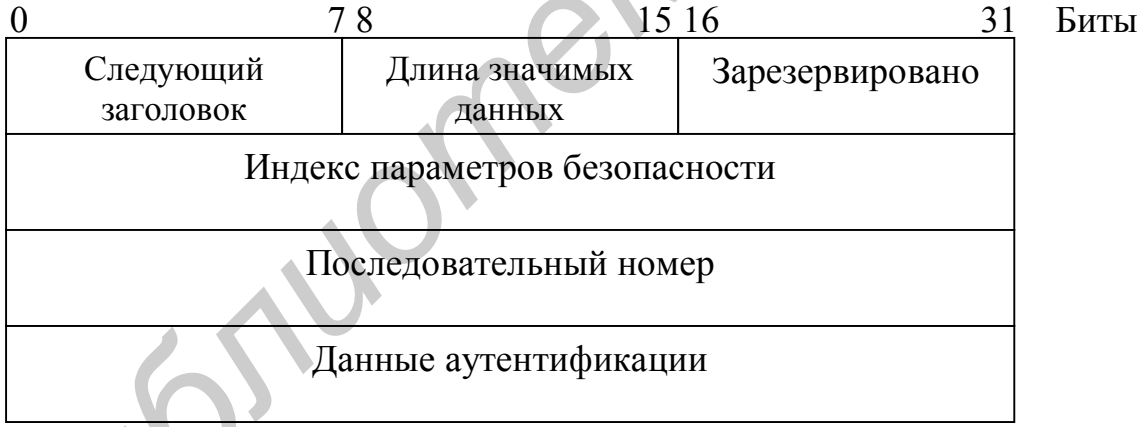


Рис.4. Формат AH

Следующий заголовок (8 бит). Идентифицирует тип заголовка, следующего непосредственно за данным заголовком.

Длина значимых данных (8 бит). Длина заголовка аутентификации в 32-битных словах.

Зарезервировано (16 бит). Значение поля должно быть нулевым.

Индекс параметров защиты (32 бит). Идентифицирует защищённую связь.

Последовательный номер (32 бит). Монотонно возрастающий номер в диапазоне от 0 до $2^{32} – 1$, использующийся для нумерации пакетов.

Данные аутентификации (переменной длины). Поле переменной длины, содержащее код аутентификации сообщения для данного пакета.

Когда устанавливается новая защищённая связь, отправитель инициализирует счётчик последовательных номеров, установив соответствующее значение равным 0. Каждый раз, когда по соответствующей защищённой связи посылается пакет, отправитель увеличивает значение данного счётчика и размещает его в поле последовательных номеров. На приёмной стороне осуществляется контроль последовательности номеров принимаемых пакетов, и пакеты с одинаковыми номерами отбрасываются. Когда значение счётчика превысит значение $2^{32} – 1$, отправитель должен завершить данную защищённую связь и инициализировать новую защищённую связь с новым ключом.

Для вычисления кода аутентификации сообщения выбирается следующая информация.

- Поля заголовка IP, которые либо не изменяются в пути следования (неизменяемые поля), либо имеют прогнозируемые значения в пункте назначения защищённой связи. Поля, которые могут измениться в пути следования и значения которых в конечной точке нельзя предсказать, обнуляются для вычислений и в пункте отправления, и в пункте назначения.
- Заголовок AH, за исключением поля данных аутентификации, которое обнуляется для вычислений в пунктах отправления и назначения.
- Все данные протокола следующего выше уровня, которые должны оставаться неизменными в пути следования, т.е. внутренний пакет IP (см. рис. 3, а).

Имеющиеся на сегодня спецификации протокола требуют, чтобы любая реализация поддерживала следующие алгоритмы для вычисления кода

аутентификации сообщения: HMAC – MD5 и HMAC – SHA-1. Кроме того, в VPN-агентах протокол AH может быть реализован с использованием отечественных алгоритмов хеширования и формирования цифровой подписи СТБ 1176.1-99 и СТБ 1176.2-99, а также российских алгоритмов хеширования и формирования цифровой подписи ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 или алгоритма криптографического преобразования ГОСТ 28147-89 в режиме выработки имитовставки.

2.2. Протокол ESP

Отличительной функцией протокола ESP является обеспечение конфиденциальности путём шифрования внутреннего пакета IP (см. рис.3, б). Пакет ESP содержит следующие поля (рис.5).

Рис.5. Формат ESP

Индекс параметров защиты (32 бита). Идентифицирует защищённую связь.

Последовательный номер (32 бита). Значение счётчика, используемого для защиты от атак воспроизведения, как и при использовании протокола AH.

Значимые данные (переменной длины). Внутренний пакет IP, который защищается шифрованием.

Заполнитель (0 – 255 байт). Поле заполняется нулями до кратности целому числу байтов в соответствии с форматами блоков используемых алгоритмов шифрования.

Длина заполнителя (8 бит). Указывает число байтов заполнителя, предшествующего данному полю.

Следующий заголовок (8 бит). Идентифицирует тип данных, содержащихся в поле значимых данных, указывая первый заголовок значимых данных.

Данные аутентификации (переменной длины). Поле переменной длины, содержащее код аутентификации сообщения, вычисляемый для данного пакета ESP, без поля данных аутентификации.

Сервис ESP предполагает шифрование полей значимых данных, заполнителя, длины заполнителя и следующего заголовка. Если для алгоритма, используемого при зашифровании значимых данных, требуется синхронизация данных, то необходимая синхропосылка вставляется в начало поля значимых данных.

Существующие спецификации требуют, чтобы любая реализация поддерживала использование алгоритма DES в режиме со сцеплением блоков (CBC), однако могут использоваться и другие алгоритмы шифрования, например: 3DES, RC5, CAST, GOST, Blowfish и др. При обеспечении аутентификации сообщений в протоколе ESP используются механизмы, рассмотренные в п. 3.1. Область действия сервисов конфиденциальности и аутентификации при их совместном использовании в протоколе ESP приведена на ри.6.

Рис. 6. Область действия шифрования и аутентификации ESP

2.3. Протоколы управления ключами

Поскольку основным механизмом обеспечения безопасности данных в VPN являются криптографические методы, участники защищённого соединения должны наладить обмен соответствующими криптографическими ключами. Обеспечить настройку процесса такого обмена можно вручную и автоматически. Первый способ допустим для небольшого количества достаточно статичных систем, а в общем случае это производится автоматически.

Для автоматического обмена ключами по умолчанию используется *Протокол управления ключами в Интернете (IKMP – Internet Key Management Protocol)*. Дополнительно или альтернативно могут быть применены другие протоколы, такие, как SKIP или Kerberos.

3.3.1. Протокол IKMP

IKMP совмещает в себе три отдельных протокола:

• *Протокол защищённой связи и управления ключами в Интернете (ISAKMP – Internet* Security *Association and Key Management Protocol)*;

• *Протокол определения ключей Окли (Oakley – Oakley key determination protocol)*;

• *Механизм безопасного обмена ключами в Интернете (SKEMI – Secure Key Exchange Mechanism for Internet)*.

ISAKMP – обеспечивает каркас схемы управления ключами в Интернет и необходимые форматы процедуры согласования атрибутов защиты. Он не регламентирует использование конкретного алгоритма обмена ключами, а предлагает набор типов сообщений, позволяющих задействовать любой подобный алгоритм.

Oakley – является конкретным алгоритмом обмена ключами, основанным на усовершенствованной схеме обмена ключами Диффи – Хеллмана.

SKEMI – описывает многофункциональные технологии, предоставляющие такие услуги защиты, как анонимность, защита от отказа передачи или получения сообщений и быстрое обновление ключей.

В ходе установления защищённой связи IKMP согласовывает следующие атрибуты: алгоритм шифрования, алгоритм хеширования, метод аутентификации и данные о группе преобразования алгоритма Диффи – Хеллмана.

Аутентификация может быть произведена с помощью следующих методов:

• шифрование с симметричным ключом (аутентификация осуществляется путём шифрования параметров обмена с использованием секретного ключа, известного обеим сторонам соединения до начала установления соединения);

• шифрование с открытым ключом (аутентификация обмена данными осуществляется с помощью шифрования некоторых параметров обмена с использованием открытого ключа получателя);

• цифровая подпись (аутентификация обмена данными осуществляется с помощью подписи доступного обеим сторонам хеш-кода с использованием личного ключа).

Алгоритм Диффи – Хеллмана предполагает предварительное соглашение о двух глобальных параметрах: q – большом простом числе, являющимся модулем конечного поля; a – основании степени – и определяет следующее взаимодействие между сторонами A и B.

Сторона A выбирает случайное число X_A, которое будет личным ключом A, и передаёт стороне B открытый ключ $Y_A = a^{X_A}$. Точно так же сторона B выбирает случайное число X_B, которое будет личным ключом B, и передаёт стороне A открытый ключ $Y_B = a^{X_B}$. Каждая из сторон теперь может вычислить секретный сеансовый ключ по формуле

$$K = (Y_B)^{X_A} \bmod q = (Y_A)^{X_B} \bmod q = a^{X_A X_B} \bmod q.$$

Имеющиеся сегодня спецификации протокола определяют следующие группы для обмена ключами Диффи – Хеллмана:

1) возведение в степень в арифметике классов вычетов с 768-битным модулем:

$$q = 2^{768} - 2^{704} + (\lfloor 2^{638} \times \pi \rfloor + 149686)2^{64} - 1,$$

$$a = 2;$$

2) возведение в степень в арифметике классов вычетов с 1024-битным модулем:

$$q = 2^{1024} - 2^{960} + (\lfloor 2^{894} \times \pi \rfloor + 129093)2^{64} - 1,$$

$$a = 2.$$

ISAKMP содержит две фазы согласования ключей. В первой фазе происходит создание защищённого канала, во второй – согласование и обмен ключами, установление защищённой связи. Сообщение ISAKMP состоит из заголовка и следующих за ним значимых данных и передаётся с помощью транспортного протокола UDP.

В ISAKMP определены следующие типы сообщений (табл. 2).

Таблица 2

№ п/п	Тип сообщения	Описание типа сообщения
1	2	3
1	Защищённая связь (SA)	Используется для согласования атрибутов защиты, указания области интерпретации и ситуаций, в рамках которых выполняется такое согласование
2	Предложение (P)	Используется в ходе согласования параметров создаваемой защищённой связи, указывает применяемый протокол и число преобразований
3	Преобразование (T)	Применяется в ходе согласования параметров защищённой связи, указывает преобразование и соответствующие атрибуты защищённой связи
4	Обмен ключами (KE)	Поддерживает ряд методов обмена ключами
5	Идентификация (ID)	Предназначено для обмена информацией идентификации
6	Сертификат (CERT)	Служит для пересылки сертификатов и другой связанной с сертификатами информации
7	Запрос сертификата (CR)	Используется для запросов сертификатов, указывает типы запрашиваемых сертификатов и приемлемые центры сертификации

Окончание табл. 2

1	2	3
8	Хеширование (HASH)	Содержит данные, генерируемые функцией хеширования
9	Подпись (SIG)	Содержит данные, генерируемые функцией цифровой подписи
10	Код соответствия (NONCE)	Случайные данные, используемые для защиты от подмены сообщения в реальном масштабе времени
11	Уведомление (N)	Используется для передачи данных уведомления, например признака возникновения ошибки
12	Удаление (D)	Указывает защищённую связь, которая больше не действует

3.3.2. Протокол SKIP

Отличительной особенностью протокола SKIP (Простой протокол управления ключами в Интернете) является исключительное использование в качестве криптографического алгоритма метода Диффи – Хеллмана (см. подразд. 3.1). Однако в данном протоколе совместно используемый ключ

$$K = a^{X_A X_B} \bmod q$$

является долговременным и его не требуется менять для каждого сеанса передачи данных.

Поскольку К – долговременный ключ, его использование для защиты самих данных небезопасно, так как создаёт возможность накопления материала для криптоанализа. Поэтому для шифрования самих данных используется отдельный сеансовый ключ $К_С$, а долговременный ключ К используется только для шифрования сеансового ключа. Тогда зашифрование IP пакета В выглядит следующим образом:

$$E_K (К_С) \,||\, Ек_С (В),$$

где || – операция конкатенации.

Аутентификация в данном случае обеспечивается предположением, что если пакет, показанный на рис.7, успешно расшифрован, значит, он был зашифрован именно тем, кто знает секретный ключ отправителя, т.е. самим отправителем.

Открыт	Зашифрован К	Зашифрован $К_С$
Заголовок IP	Сеансовый ключ $К_С$	Исходный IP пакет

Рис. 7. Зашифрованный SKIP-пакет

В качестве дополнительной меры обеспечения защиты используется механизм учёта количества использований долговременного ключа, который можно определить в виде

$$К_n = h(К, n),$$

где h – хеш-функция;

n – постоянно увеличивающийся счётчик.

Таким образом, обеспечивается дополнительная защита от возможного повторения посылки пакета, скопированного нарушителем в предыдущем сеансе.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

1. В чём сущность технологии VPN и в каких случаях она применяется?
2. Описать наиболее важные спецификации IPSec.
3. Разработать алгоритм реализации протокола ESP.
4. Пояснить сущность метода открытого распределения ключей Диффи – Хеллмана.
5. В чём отличие протоколов управления ключами ISAKMP и SKIP?

ЛИТЕРАТУРА

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ–ОБРАЗ, 2001. – 368 с.

2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. 2-е изд. – М.: Радио и связь, 2002. –328 с.

3. Столлингс В. Основы защиты сетей. Приложения и стандарты: Пер. с англ. – М.: Изд. дом «Вильямс», 2002. – 432 с.

4. Кульгин М. Технологии корпоративных сетей. Энциклопедия. – СПб.: Питер, 2000. – 704 с.

5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – СПб.: Питер, 2001. – 672 с.

Св. план 2005, поз.96

Учебное издание

Бобов Михаил Никитич

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ VPN

УЧЕБНОЕ ПОСОБИЕ
по курсам «Защита информации в банковских технологиях»,
«Защита программного обеспечения и баз данных в сетях телекоммуникаций»,
«Криптографическая защита информации в телекоммуникациях»
для студентов специальности 45 01 03 «Сети телекоммуникаций»
дневной и заочной форм обучения

Редактор Т.А.Лейко
Корректор Н.В. Гриневич

Подписано в печать 18.01.2005. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л. 1,51.
Уч.-изд. л. 0,9. Тираж 100 экз. Заказ 644.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия на осуществление издательской деятельности №02330/0056964 от 01.04.2004.
Лицензия на осуществление полиграфической деятельности №02330/0133108 от 30.04.2004.
220013, Минск, П. Бровки, 6