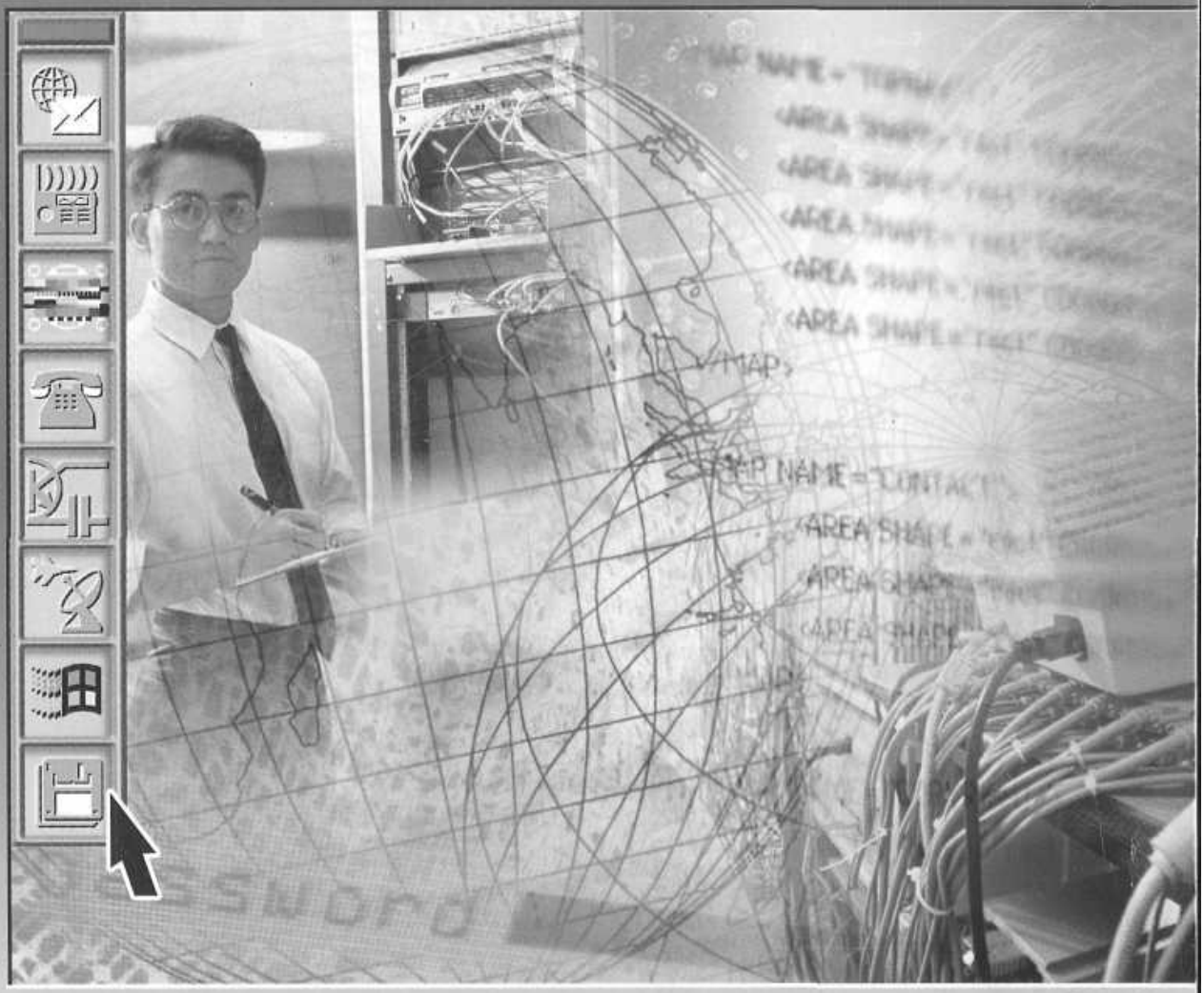
УЧЕБНОЕ ПОСОБИЕ

ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

СПЕЦИАЛЬНОСТЬ



ОСНОВЫ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Горячая линия–Телеком

С.В.Запечников
Н.Г.Милославская
А.И.Толстой

С.В.Запечников
Н.Г.Милославская
А.И.Толстой

ОСНОВЫ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Допущено УМО по образованию в области информационной безопасности в качестве учебного пособия для студентов, обучающихся по специальностям 075200 — компьютерная безопасность и 075500 — комплексное обеспечение информационной безопасности автоматизированных систем

ББК 32.973.2-018.2я73
З 31
УДК 004.732.056(075.8)

Рецензенты:
кафедра "Защита информации" МИФИ (заведующий кафедрой канд. техн. наук, доцент А.А. Малюк), член-корреспондент АК РФ А.П .Коваленко, доктор воен. наук, профессор В.П. Лось, доктор техн. наук, профессор А.Д. Иванников, канд. техн. наук, доцент С.Н. Смирнов, канд. физ-мат. наук, профессор В.М. Немчинов, канд.физ.-мат. наук, доцент И.В. Прокофьев, доцент А.М. Никитин

Запечинков С.В., Милославская Н.Г., Толстой А.И.
331 Основы построения виртуальных частных сетей: Учеб. пособие для вузов. М.: Горячая линия–Телеком, 2003. – 249 с.

ISBN 5-93517-139-2.

Рассматриваются основы построения виртуальных частных сетей (VPN). Даются основные определения. Описывается технология туннелирования в сетях. Подробно анализируются стандартные протоколы построения VPN и управление криптографическими ключами в VPN. Выделяются особенности различных вариантов и схем создания VPN. В качестве примеров реализации VPN приводятся различные российские продукты.

Для студентов высших учебных заведений, обучающихся по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем", и слушателей курсов повышения квалификации по специальности "Комплексное обеспечение информационной безопасности автоматизированных систем".

ББК 32.973.2-018.2я73

Учебное издание

Запечинков С.В., Милославская Н.Г., Толстой А.И.

ОСНОВЫ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Учебное пособие

Обложка художника В.Г. Ситникова

ЛР № 071825 от 16 марта 1999 г.
Подписано в печать 23.05.03. Печать офсетная. Формат 60×88/16
Уч.-изд. л. 15,75. Тираж 3000 экз. Изд. № 139

ISBN 5-93517-139-2

ОГЛАВЛЕНИЕ

Предисловие

Основой для учебного пособия послужил опыт преподавания технологий защиты в открытых сетях лично авторов и их коллег, подробные описания, сделанные разработчиками данных технологий и средств защиты, а также многочисленные отечественные и зарубежные публикации по рассматриваемой тематике.

В настоящее время специалистов-профессионалов по различным аспектам защиты информации готовит ряд вузов России. Обучение происходит на специализированных факультетах, ознакомительных курсах или курсах повышения квалификации. Но все эти учебные заведения испытывают острую нехватку узкопрофильной учебно-методической литературы, что, в первую очередь, сказывается на качестве обучения. Данное учебное пособие предлагается для обучающихся (студентов, аспирантов и повышающих квалификацию специалистов) по группе специальностей "Информационная безопасность".

Поскольку число атак на сети неизменно растет, а создать полностью защищенную информационную среду очень сложно, нужны специализированные средства, предназначенные для осуществления защиты информации, передаваемой по открытым каналам связи сетей передачи данных, и воплощения в жизнь выработанной организацией политики безопасности ее информационных и сетевых ресурсов. Специалист в области информационной безопасности должен владеть определенными теоретическими знаниями и практическими навыками в данной, очень важной области обеспечения информационной безопасности. На сегодняшний день учебной литературы по вопросам построения виртуальных частных сетей, к сожалению, пока не имеется.

Основная задача, которую призвано решить учебное пособие, — это представить обучающимся систематизированный подход к проблеме виртуальных частных сетей (VPN), ознакомить их с характерными признаками различных вариантов их построения, а также научить квалифицировано выбирать, применять и самостоятельно разрабатывать реализующие такие возможности средства. В пособии показано, что при условии грамотного использования VPN (совме-

стно с другими средствами обеспечения информационной безопасности, такими как средства аутентификации, средства обнаружения вторжений и т.п.) может быть реализована достаточно надежная защита информации от несанкционированного перехвата с различными целями во время ее передачи по открытым каналам связи. Такие знания особенно важны для специалистов-практиков по защите информации в современных сетях.

Важно подчеркнуть, что для приступающих к ознакомлению с учебным пособием есть определенные требования по предварительной подготовке. Например, следует знать протоколы и сервисы Internet, сетевые операционные системы, основные принципы безопасности сетей и технологий их защиты, иметь базовые знания по криптографии.

Учебное пособие состоит из введения, пяти разделов, заключения и приложений с полезной информацией.

Во введении отмечается своевременность рассмотрения заявленной в названии учебного пособия темы и решаемые на основе технологии виртуальных сетей задачи.

Первый раздел содержит основные определения, цели и задачи, а также описание специфики построения VPN и основного применяемого подхода — туннелирования. Выделены особенности построения VPN в различных типах сетей и рассмотрены разные схемы VPN. Вводится понятие политики безопасности для VPN и называются другие средства защиты информации, дополняющие VPN и реализующие комплексный подход к защите информации в корпоративных сетях.

Во втором разделе детально рассматриваются стандартные протоколы создания виртуальных частных сетей, реализующие функции VPN на различных уровнях модели взаимодействия открытых систем OSI/ISO (с указанием соотнесения их с уровнями стека протоколов TCP/IP) - канальном, сетевом и сеансовом.

Третий раздел посвящен управлению криптографическими ключами в VPN. Последовательно изучаются жизненный цикл криптографических ключей, особенности управления ключевой системой асимметричных криптосистем, концепция инфрастуктуры открытых

ключей, метод сертификации открытых ключей и модель инфраструктуры открытых ключей PKIX.

В четвертом разделе даются основы практического построения VPN, перечисляются и поясняются требования к VPN-продуктам, которые подразделяются на шлюзы и клиенты, рассматриваются варианты реализации VPN и решения для организации VPN на базе сетевой операционной системы, маршрутизаторов, межсетевых экранов, специализированного программного обеспечения и аппаратных средств. Также анализируются четыре основных вида VPN: Intranet VPN, Client/server VPN, Extranet VPN и Remote Access VPN и приводятся полезные рекомендации специалистов по выбору VPN-продуктов.

Пятый раздел описывает некоторые реализации VPN на основе таких российских разработок, как аппаратно-программный комплекс защиты информации "Континент-К", программные продукты компании "ЭЛВИС+", VPN-решения компании "Инфотекс", семейство продуктов "Net-PRO" компании "Сигнал-КОМ", продукты МО ПНИЭИ "ШИП" и "Игла-2" и аппаратно-программный комплекс "ФПСУ-IP" компании "Амикон". С целью определения лучших условий применения рассмотренных продуктов приводится их сравнение.

В заключение выделены основные проблемы, возникающие при использовании VPN-продуктов, и указаны возможные варианты их усовершенствования.

В приложениях представлена полезная информация справочного характера: сравнение зарубежных продуктов для создания VPN и документы, в которых содержится полное описание основных протоколов для VPN.

После каждого раздела приведены вопросы для самоконтроля.

Авторы признательны коллегам по факультету "Информационная безопасность" МИФИ, а также всем рецензентам.

Авторы, естественно, не претендуют на исчерпывающее изложение всех названных в работе аспектов проблемы построения VPN, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебным пособием.

Принятые сокращения

ИОК	инфраструктура открытых ключей
ИТ	информационная технология
КС	корпоративная сеть
ЛВС	локальная вычислительная сеть
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОС	операционная система
ПБ	политика безопасности
ПО	программное обеспечение
УЦ	удостоверяющий центр
ЭЦП	электронная цифровая подпись
AH	Authentication Header, протокол аутентифицирующего заголовка
CA	Certificate Authority, удостоверяющий центр
CHAP	Challenge Handshake Authentication, протокол аутентификации
ESP	Encapsulation Security Payload, протокол
IKE	Internet Key Exchange, протокол обмена ключами Internet
IPSec	Internet Security Protocol
ISP	Internet Service Provider, сервис-провайдер Internet
FR	Frame Relay
GRE	Generic Routing Encapsulation, общая маршрутная инкапсуляция
L2F	Layer-2 Forwarding, протокол эстафетной передачи на втором уровне
L2TP	Layer-2 Tunneling Protocol, протокол туннелирования на втором уровне
LDAP	Lightweight Directory Access Protocol, упрощенный протокол доступа к каталогу
MAC	Message Authentication Code, код аутентификации сообщения
NAT	Network Address Translation, трансляция сетевых IP-адресов
PAP	Assword Authentication Protocol, протокол аутентификации по паролю
PKI	Public Key Infrastructure, инфраструктура открытых ключей
PPTP	Point-to-Point Tunneling Protocol, протокол туннелирования "точка-точка"
RADIUS	Remote Authentication Dial-In User Service, сервис аутентификации удаленных пользователей
RAS	Remote Access Server, сервер удаленного доступа
SNMP	Simple Network Management Protocol, простой протокол управления сетями
SA	Security Association, безопасная ассоциация (защищенное соединение, контекст безопасности)
SSL	Secure Socket Layer
TLS	Transport Layer Security
VLAN	Virtual Local Area Network, виртуальная локальная сеть
VPN	Virtual Private Network, виртуальная частная сеть

Введение

Безопасность информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети, например, через глобальную сеть Internet, требует качественного решения двух базовых задач (рис. 1) [3]:

- защиты подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;
- защиты информации в процессе передачи по открытым каналам связи.

Рис. 1. Задачи по обеспечению безопасности информационного взаимодействия

Решение первой задачи основано на использовании межсетевых экранов (МЭ), поддерживающих безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене ин-

формацией. Для защиты локальных сетей МЭ располагают на стыке между локальной и открытой сетью. Для защиты отдельного удаленного компьютера, подключенного к открытой сети, программное обеспечение МЭ устанавливается на этом же компьютере, а сам МЭ в этом случае называют персональным.

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

- аутентификации (установление подлинности) взаимодействующих сторон;
- шифровании передаваемых данных;
- подтверждении подлинности и целостности доставленной информации;
- защите от повтора, задержки и удаления сообщений;
- защите от отрицания фактов отправления и приема сообщений.

Перечисленные функции во многом связаны друг с другом, и их реализация основана на криптографической защите передаваемых данных. Высокая эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем.

Многие организации имеют несколько локальных вычислительных сетей (ЛВС) и информационных серверов, находящихся в физически удаленных друг от друга местах. Если требуется обеспечить доступ к информации для всех сотрудников организации, то часто используются выделенные линии для соединения ЛВС с глобальными сетями. Этот способ имеет ряд существенных недостатков — не гарантирует надежной защиты коммуникаций, значительно ограничен в применении и требует больших затрат средств и времени. К примеру, как протянуть линию за сотрудником, если он периодически меняет место дислокации или постоянно разъезжает по всей стране?

Конечно, существует большое количество открытых коммуникационных каналов, которые можно арендовать у провайдеров связи или Internet.

Первый случай – провайдеры связи (рис. 2). Каналы, связывающие центральную сеть предприятия с сетями филиалов, проходят через мультиплексор, объединяющий каналы всех абонентов в маги-

стральный канал. Несмотря на то, что территориальные каналы в этом случае не относятся к собственности предприятия, корпоративные сети (КС), построенные на арендованных каналах, также называются частными, по крайней мере, по двум причинам.

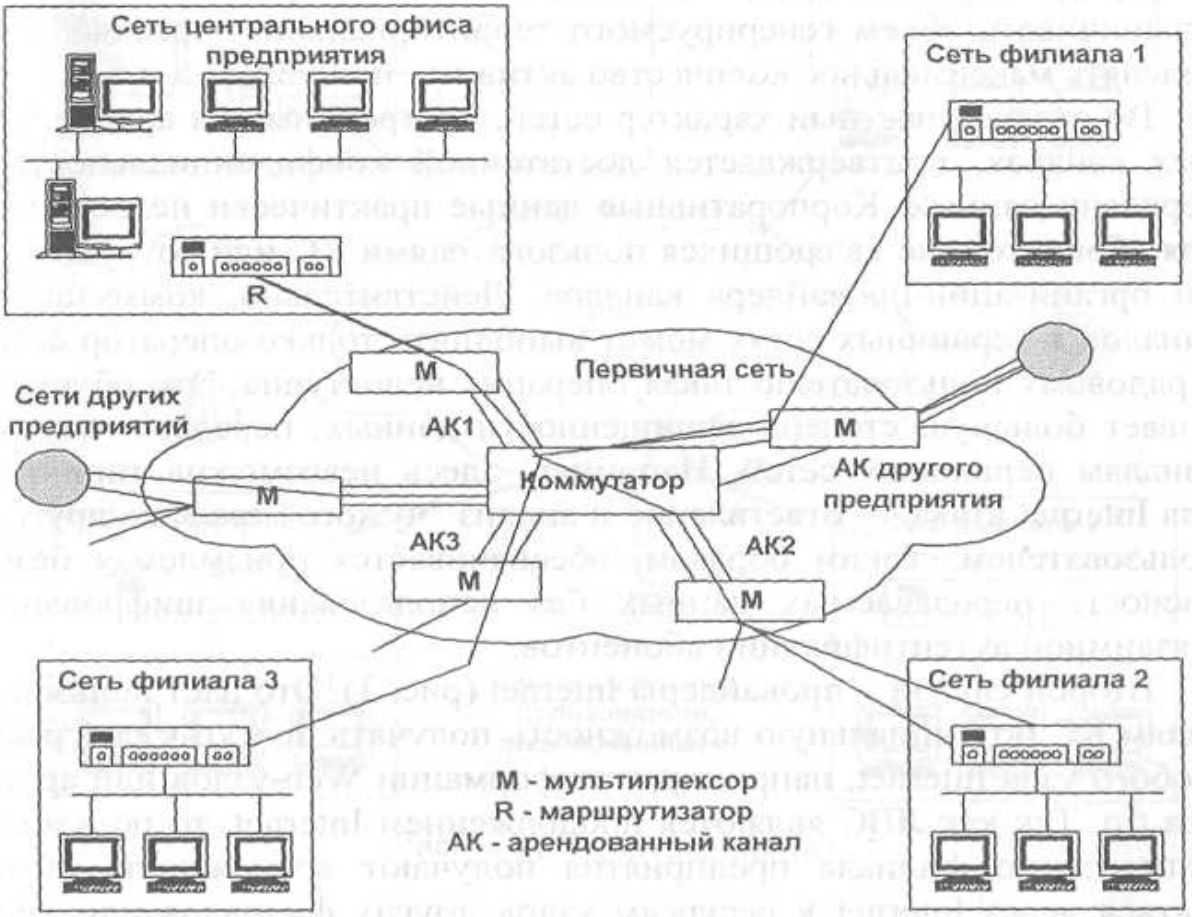


Рис. 2. Провайдеры связи

Во-первых, полоса пропускания арендованного канала полностью выделяется предприятию и поэтому является в некотором смысле его "частной собственностью". Это в полной мере относится к арендуемым цифровым каналам, которые поддерживаются провайдером на базе первичной цифровой сети с техникой мультиплексирования TDM. Арендатор такого канала получает в свое полное распоряжение всю его пропускную способность — 64, 128 кбит/с, 2 Мбит/с или выше. В любом случае, пропускную способность канала предприятие-арендатор не делит ни с кем, и это очень важно

для создания КС со стабильными характеристиками. Наличие гарантированной пропускной способности дает возможность администратору сети планировать работу приложений через глобальные каналы связи: распределять имеющуюся пропускную способность канала между приложениями, оценивать возможные задержки сообщений, ограничивать объем генерируемого территориального трафика, определять максимальное количество активных приложений и т.д.

Во-вторых, частный характер сетей, построенных на арендованных каналах, подтверждается достаточной конфиденциальностью передачи данных. Корпоративные данные практически недоступны для абонентов, не являющихся пользователями КС или сотрудниками организации-провайдера каналов. Действительно, коммутацию каналов в первичных сетях может выполнить только оператор сети, а рядовому пользователю такая операция недоступна. Это обуславливает большую степень защищенности данных, передаваемых по каналам первичных сетей. Например, здесь невозможна типичная для Internet атака — ответвление и анализ "чужого" трафика другим пользователем. Таким образом, обеспечивается приемлемая безопасность передаваемых данных без использования шифрования и взаимной аутентификации абонентов.

Второй случай – провайдеры Internet (рис. 3). Это дает пользователям КС потенциальную возможность получать доступ к ресурсам любого узла Internet, например, к информации Web-узлов или архивов ftp. Так как ЛВС являются продолжением Internet, то пользователи одного филиала предприятия получают возможность обращаться через Internet к ресурсам узлов других филиалов или центрального офиса.

Открытую внешнюю среду передачи информации можно разделить на среду скоростной передачи данных, в качестве которой может использоваться Internet, а также более медленные общедоступные каналы связи, в качестве которых чаще всего применяются каналы телефонной сети. Наиболее эффективным способом объединения ЛВС и удаленных компьютеров является объединение на основе Internet (рис. 4). В случае отсутствия непосредственного подключения доступ к Internet может осуществляться и через телефонную сеть.

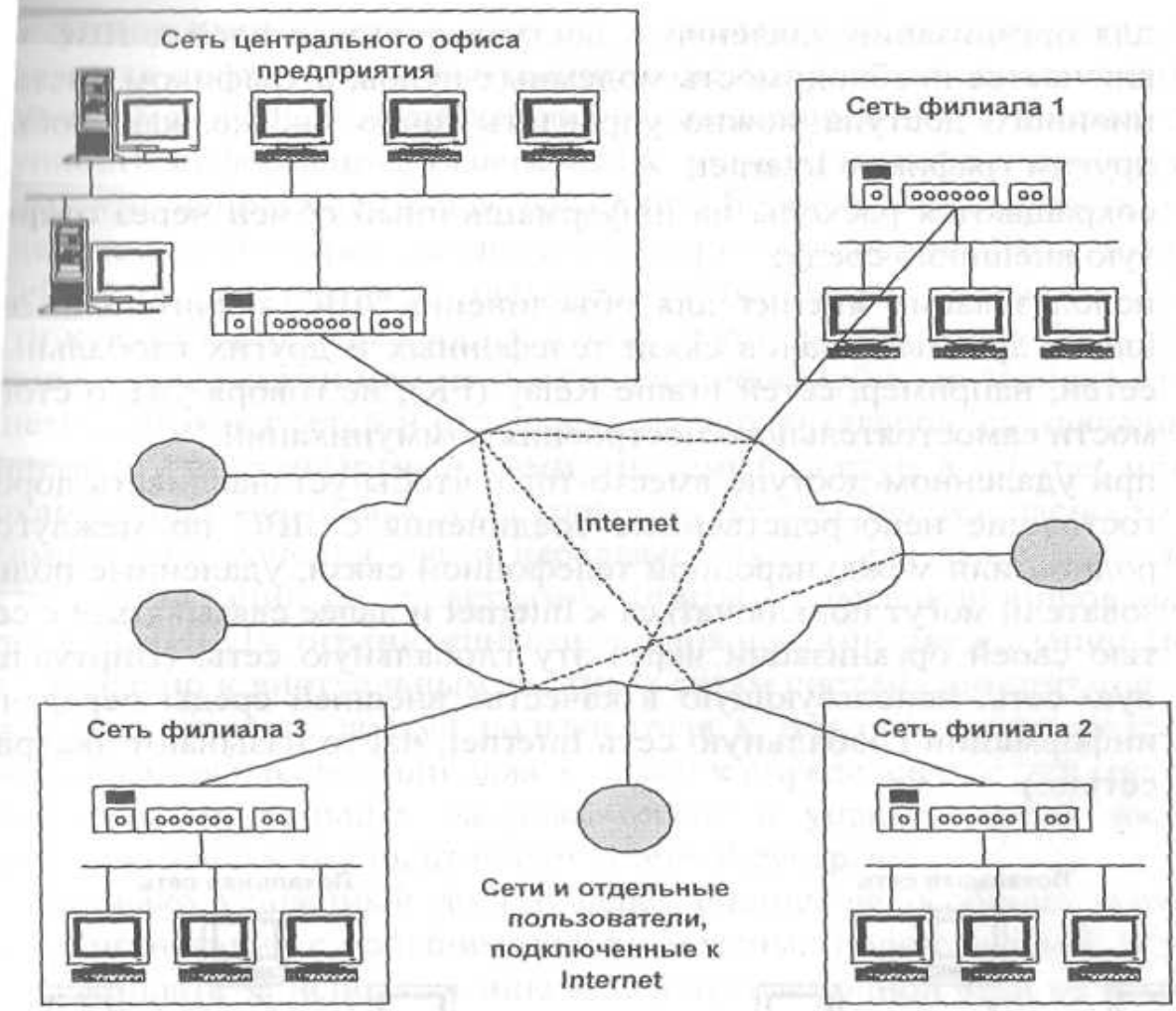


Рис. 3. Провайдеры Internet

Организация виртуальных сетей на основе Internet обладает рядом преимуществ:

- гарантирует высокое качество информационного обмена, так как магистральные каналы и маршрутизаторы Internet имеют большую пропускную способность и характеризуются надежностью передачи информации;
- обеспечивает масштабируемую поддержку удаленного доступа к ресурсам ЛВС, позволяя мобильным пользователям связываться по местным телефонным линиям с поставщиками услуг Internet и через них входить в свою КС;

- для организации удаленного доступа пользователей к ЛВС исключается необходимость модемных пулов, а трафиком дистанционного доступа можно управлять точно так же, как любым другим трафиком Internet;
- сокращаются расходы на информационный обмен через открытую внешнюю среду;
- использование Internet для объединения ЛВС значительно дешевле аренды каналов связи телефонных и других глобальных сетей, например, сетей Frame Relay (FR), не говоря уже о стоимости самостоятельного построения коммуникаций;
- при удаленном доступе вместо того, чтобы устанавливать дорогостоящие непосредственные соединения с ЛВС по междугородной или международной телефонной связи, удаленные пользователи могут подключаться к Internet и далее связываться с сетью своей организации через эту глобальную сеть. (Виртуальную сеть, использующую в качестве внешней среды передачи информации глобальную сеть Internet, часто называют экстрасетью.)

Рис. 4. Построение виртуальной сети на основе Internet

Основными недостатками использования Internet для этой цели являются отсутствие конфиденциальности данных, передаваемых по Internet между ЛВС, а также отсутствие защиты целостности и доступности информации, уязвимость к подмене пакетов и другим атакам, что неприемлемо для реального бизнеса. Безопасность – не единственный вопрос, возникающий при соединении ЛВС с Internet. Сейчас Internet не предоставляет гарантий в пропускной способности канала и его надежности. Файлы и сообщения могут быть переданы с задержками или не доставлены вообще, и это зависит от общего состояния сетей и отдельных маршрутизаторов, составляющих Internet. Т.е. стандартный коммутируемый доступ в Internet можно охарактеризовать невысоким уровнем обеспечения безопасности как самого подключения, так и передаваемых по сети данных, сложностью интеграции со средствами защиты от несанкционированного доступа (НСД), ограниченными возможностями авторизации (применительно к виртуальным частным сетям система авторизации может регулировать доступ пользователя к тем или иным средствам шифрования пакетов или даже в целом к определенным устройствам создания виртуальных частных сетей) и управляемости доступа пользователей к корпоративным сетевым ресурсам.

Однако удаленный доступ через Internet не особенно выгоден для организаций с большим числом местных пользователей. В этом случае плата за использование местной телефонной сети не изменяется от перехода с прямых звонков на RAS (Remote Access Server) предприятия к звонкам на RAS провайдера, а дополнительная плата за использование Internet может свести на нет выгоду от обслуживания немногочисленных пользователей из других городов и стран через Internet. Поэтому многие из тех компаний, что собираются реализовать VPN для удаленного доступа, предпочитают сочетать оба подхода: пользователи из других городов должны обращаться в КС через Internet, в то время как местные пользователи будут продолжать звонить напрямую на RAS предприятия по местной телефонной сети.

1. ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ

1.1. Определение, цели и задачи

Благодаря развитию криптографических технологий появился способ решить задачи защиты информации в современной сетевой среде за счет использования технологии защищенных виртуальных частных сетей (Virtual Private Network — VPN), надежно шифрующих информацию, передаваемую по дешевым открытым сетям, включая Internet. Открытая сеть может служить основой для одновременного сосуществования множества виртуальных сетей, количество которых определяется пропускной способностью открытых каналов связи.

Компания Check Point Software Technologies, которая не без основания считается законодателем моды в области VPN и МЭ (например, по данным независимых консалтинговых и аналитических агентств Dataquest и IDC компания Check Point захватила 52 % мирового рынка VPN-решений и 41 % МЭ), дает следующее определение: "VPN — это технология, которая объединяет доверенные сети, узлы и пользователей через открытые сети, которым нет доверия".

Можно встретить и такие общие подходы к определению VPN:

- VPN — это защита трафика, основанная на криптографии;
- VPN — это средство коммуникации, так как гарантия защиты доступа к внутренним ресурсам из любой точки мира инициирует применение информационных систем для удаленного доступа;
- VPN — это средство влияния на стратегию развития коммуникационных систем корпорации: вместо того, чтобы вкладывать

огромные средства в строительство собственных выделенных линий, вы практически сегодня же можете получить надежно защищенные каналы связи от коммуникационных провайдеров.

Под VPN понимают потоки данных одного предприятия, которые существуют в публичной сети с коммутацией пакетов и в достаточной степени защищены от влияния потоков данных других пользователей этой публичной сети [12]. Другими словами, VPN — это некоторая имитация сети, построенной на выделенных каналах. Если публичная сеть предоставляет такой сервис, то в ней одновременно сосуществуют несколько VPN, разделяющих общие коммутаторы и физические каналы связи.

Сети VPN решают задачи подключения корпоративного пользователя к удаленной сети и соединения нескольких ЛВС (рис. 5).

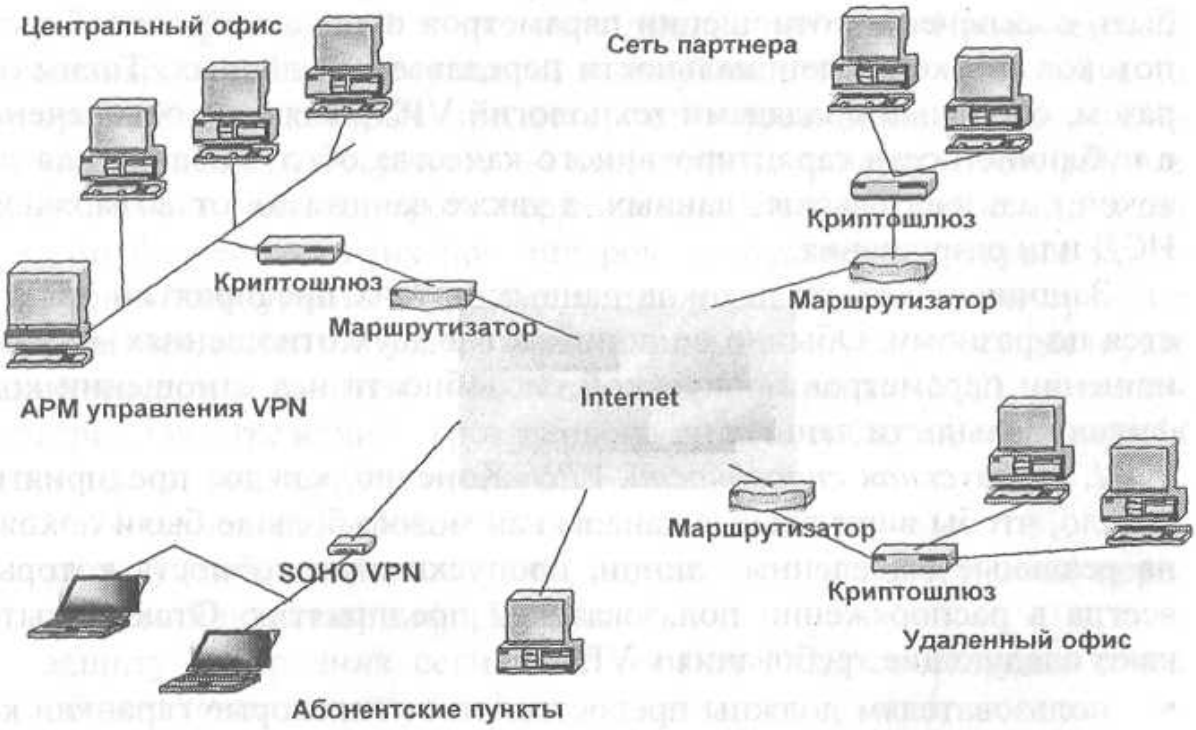


Рис. 5. Пример VPN

Маркетинговая трактовка товара подразумевает, как минимум, две его сущности: потребительскую и физическую. Потребительская сущность VPN — "виртуальный защищенный туннель, или путь",

с помощью которого можно организовать удаленный защищенный доступ через открытые каналы Internet к серверам баз данных, Web-, FTP- и почтовым серверам. Физическая сущность технологии VPN определяется тем, что она может защитить трафик любых информационных интранет- и экстранет-систем, аудио- и видеоконференций, систем электронной коммерции и т.п. (Но VPN, как любая распределенная система, в ее "физической сущности" является сложным комплексом, который требует целого ряда взаимодополняющих средств и систем защиты. Ее способность шифровать данные является необходимым, но далеко не достаточным условием для построения действительно надежной защиты.)

Цель VPN-технологий состоит в максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей публичной сети. Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и в конфиденциальности передаваемых данных. Таким образом, основными задачами технологий VPN являются обеспечение в публичной сети гарантированного качества обслуживания для потоков пользовательских данных, а также защита их от возможного НСД или разрушения.

Защищенность от потоков данных других предприятий трактуется по-разному. Обычно ее понимают в двух отношениях — в отношении параметров пропускной способности и в отношении конфиденциальности данных.

1. Пропускная способность VPN. Конечно, каждое предприятие хотело, чтобы виртуальные каналы как можно больше были похожи на реальные выделенные линии, пропускная способность которых всегда в распоряжении пользователей предприятия. Отсюда вытекают следующие требования к VPN:

- пользователям должны предоставляться некоторые гарантии качества обслуживания в виртуальных каналах VPN — средняя пропускная способность, максимально допустимый уровень пульсации, уровни задержек кадров;
- пользователи должны иметь инструменты для контроля действительных параметров пропускной способности виртуальных каналов.

Сегодня для различных типов сетей с коммутацией пакетов существуют различные возможности получения гарантий качества обслуживания.

2. *Конфиденциальность.* Возможность НСД к данным, передающимся по публичной сети, очень волнует сетевых администраторов, привыкших к использованию выделенных каналов или телефонных сетей для передачи корпоративных данных. Наличие злоумышленников в Internet представляет постоянную угрозу для корпоративных серверов, к данным которых можно попробовать подключиться с любого домашнего компьютера.

В то же время угрозы перехвата пакетов по пути следования по публичной сети передачи данных многие специалисты считают преувеличенными. Действительно, пакеты идут только через коммутаторы и маршрутизаторы провайдеров публичных сетей, а в сети посторонних организаций и частных лиц не заходят. Провайдерами публичных сетей с коммутацией пакетов выступают чаще всего те же организации, которые предоставляют традиционные виды телекоммуникационных сервисов — выделенные каналы и телефонные сети. Таким образом, угроза перехвата пакетов по пути следования исходит скорее от самих провайдеров, сотрудников которых могут подкупить конкуренты. От двух типов угроз: входа во внутренние серверы предприятия и перехвата данных по пути — существуют такие средства защиты, как межсетевые экраны (МЭ) и proxy-серверы для отражения угроз первого вида и средства образования защищенного канала для второго.

VPN-технологии обеспечивают:

- защиту (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;
- защиту внутренних сегментов сети от НСД со стороны сетей общего пользования;
- контроль доступа в защищаемый периметр сети;
- сокрытие внутренней структуры защищаемых сегментов сети;
- идентификацию и аутентификацию пользователей сетевых объектов;
- централизованное управление политикой корпоративной сетевой безопасности и настройками VPN-сети;

- криптографическую защиту данных, передаваемых по каналам связи сетей общего пользования между защищаемыми сегментами сети;
- безопасный доступ пользователей VPN к ресурсам сетей общего пользования.

Потоки данных отдельного предприятия образуют виртуальные каналы частной сети (рис. 6).

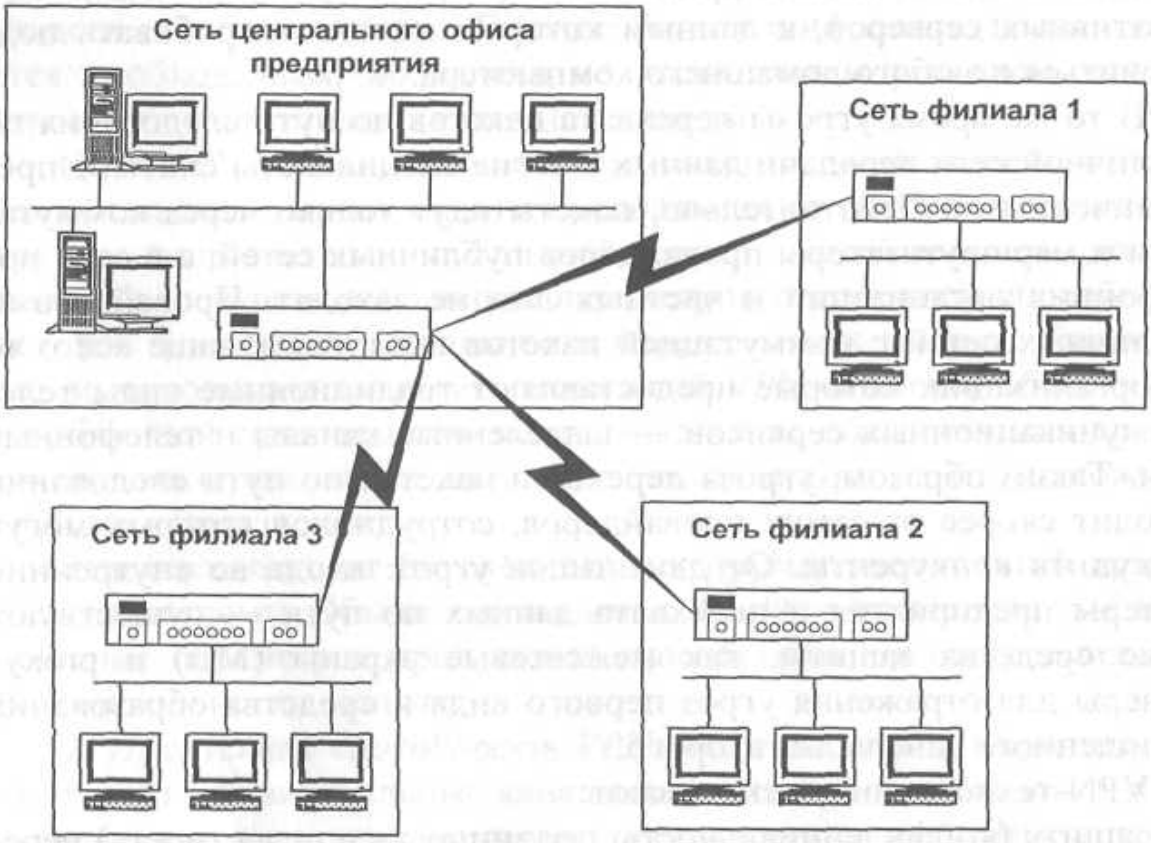


Рис. 6. Частная сеть с собственными территориальными каналами

Термин "private" имеет два основных значения: частный (собственный) и конфиденциальный (закрытый). Если делать акцент на первом значении, то частная сеть — это такая сеть, в которой все оборудование (включая территориальные кабельные системы, коммутирующие устройства, средства управления и т.п.) являются собственностью предприятия. На рис. 6 приведен пример КС, в которой связи между филиалами построены на основе собственного обору-

дования данного предприятия. Три территориальных канала связывают центральную ЛВС предприятия с тремя ЛВС удаленных филиалов. Каждый территориальный канал образован отрезками кабеля, проложенного между устройствами регенерации, необходимыми для усиления сигналов и восстановления их формы после прохождения определенного расстояния по пассивному кабелю. Вся пропускная способность территориальных каналов находится в полном распоряжении предприятия.

Следует заметить, что КС, являющихся абсолютно частными, в мире не так уж много. Использовать собственные территориальные каналы связи могут только те предприятия, для которых такие каналы являются органической частью собственной инфраструктуры, обусловленной основной производственной деятельностью. Например, для передачи технологической информации железнодорожные компании прокладывают линии связи вдоль полотна, а нефтяные — вдоль трубопроводов, поэтому они могут использовать свободную часть своих линий для построения КС.

Понятно, что сеть, построенная целиком на собственном оборудовании предприятия, соответствует и второму определению термина "private" — в собственной сети легче соблюдать конфиденциальность, поскольку все ресурсы сети используются только сотрудниками предприятия-владельца.

Интерес пользователей к данной технологии обусловлен следующими факторами:

- низкой стоимостью эксплуатации за счет использования сетей общего пользования вместо собственных или арендуемых линий связи;
- практически не ограниченной масштабируемостью;
- простотой изменения конфигурации и наращивания КС;
- "прозрачностью" для пользователей и приложений.

Для руководителя, принимающего решение об установке тех или иных средств или систем, важна и финансовая сущность применения VPN. При правильном выборе VPN:

- обеспечиваются защищенные каналы связи и защищенный трафик для отдельных приложений по цене доступа в Internet, что в несколько раз дешевле собственных линий;

- не требуется изменять топологию сетей при установке VPN, переписывать приложения, обучать пользователей, т.е. тратить дополнительные средства;
- обеспечивается масштабирование: VPN не создаст проблем роста, что сохранит уже сделанные раньше инвестиции в инфраструктуру безопасности.

Помимо обеспечения защиты от посторонних передаваемых данных, VPN несет с собой и ряд других преимуществ, в том числе и экономических. Например, исследовательская компания Forrester Research опубликовала следующие данные, характеризующие преимущество применения VPN поверх Internet (из расчета 1000 пользователей) по сравнению с созданием сервера удаленного доступа (Remote Access Service).

Из табл. 1 можно видеть, что использование VPN позволяет снизить многие статьи затрат, включая закупку коммуникационного оборудования, оплату услуг Internet-провайдера и т.д. Эти и другие исследования позволили Международной ассоциации компьютерной безопасности (International Computer Security Association, ICSA) причислить технологию VPN к десятке самых известных технологий, которые будут применяться многими компаниями в первую очередь. Это подтверждает и компания Gartner Group, которая в одном из своих отчетов предсказала, что средства построения VPN будут применяться в 2002 г. в 90 % компаний. Именно с этим связан прогноз рынка средств VPN, который исчисляется 11,94 млрд долл. в 2002 г. и 18,77 млрд в 2004 г. (по данным Frost & Sullivan).

Таблица 1. **Сравнительные характеристики использования VPN и удаленного доступа**

Статья затрат	Удаленный доступ, млн долл.	VPN, млн долл.
Оплата услуг провайдера связи	1,08	0,54
Расходы на эксплуатацию	0,3	0,3
Капиталовложения	0,1	0,02
Прочие расходы	0,02	0,03
Всего	1,5	0,89

С точки зрения конечных пользователей их обычно интересуют ответы на следующие вопросы о VPN.

1. Как мне защитить удаленный филиал своей организации или подключиться к КС из дома или с переносного компьютера?
2. Если я использую МЭ, то нужна ли мне VPN?
3. Защищает ли VPN от внешних и внутренних атак?
4. Насколько медленнее будет работать моя сеть после установки VPN?
5. Чем отличаются сертифицированное и несертифицированное VPN-устройства?
6. Почему VPN-устройства сертифицируются по классу МЭ?

1.2. Специфика построения

Как правило, построение VPN для распределенных компаний даже с небольшим количеством (5-10) удаленных подразделений (филиалов) является достаточно трудоемкой задачей, сложность которой обуславливается следующими основными причинами:

- гетерогенностью используемых аппаратно-программных платформ;
- разнообразием задач (защищенный обмен между головным офисом и филиалами, офисом и мобильными или удаленными сотрудниками, сегментами внутренней сети компании);
- необходимостью построения централизованной системы управления всей корпоративной VPN;
- наличием узкой полосы пропускания и откровенно плохим качеством существующих каналов связи, особенно с региональными подразделениями и т.д.

Сложность построения корпоративных VPN усугубляется еще и тем, что, как правило, корпоративные заказчики предъявляют к VPN достаточно жесткие требования по следующим критериям:

- *масштабируемости* применяемых технических решений;
- *интегрируемости* с уже существующими средствами;
- *легальности используемых алгоритмов и решений;*
- *пропускной способности* защищаемой сети;
- *стойкости* применяемых криптоалгоритмов;

- *унифицируемости* VPN-решения;
- *общей совокупной стоимости* построения корпоративной VPN.

Одним из требований является обеспечение масштабируемости конкретной VPN. Многолетний опыт показывает, что наиболее успешно для этого применяются программные VPN-агенты, которые:

- могут обеспечить защиту трафика на всех типах компьютеров — рабочих станциях, серверах и шлюзах (на выходе из ЛВС в открытые сети);
- работают на всех популярных ОС.

Вторая составляющая масштабируемости — централизованное, целостное и оперативное управление VPN. Значения этих понятий в данном контексте таковы:

- централизованное — конфигурирование VPN происходит в одном месте на одной рабочей станции;
- целостное — вся VPN создается как единое целое, поскольку совершенно недопустима ситуация, когда разные узлы имеют несовместимую политику безопасности или включаются в VPN не одновременно;
- оперативное — созданная в центре "конфигурация VPN" должна автоматически за считанные секунды быть разослана на все узлы VPN. Для больших систем неприемлемо, чтобы оператор последовательно, пусть и удаленно, конфигурировал все 300 VPN-узлов или передавал им конфигурации на дискетах.

1.3. Виртуальные частные сети в публичных сетях Frame Relay, ATM, X.25, TCP/IP

В основе технологии VPN лежит идея использования сетей общего пользования для защищенной передачи трафика территориально удаленных сетей заказчика, с использованием идеологии построения частных сетей. VPN можно организовывать в сетях с коммутацией пакетов любого типа X.25, FR, ATM и TCP/IP (Internet). В качестве сетей общего пользования могут выступать сети и магистральные сети сервис-провайдера.

Наличие в сетях X.25 техники виртуальных каналов создает предпосылки для образования в них VPN. Однако в технологии X.25

отсутствует важный элемент, который необходим для образования VPN — поддержка качества обслуживания. Пропускная способность виртуального канала VPN неизвестна. В настоящее время работы по совершенствованию технологии X.25 в этом направлении не ведутся, поэтому виртуальные каналы в сетях X.25 трудно отнести к полноценным VPN.

Сети FR часто упоминаются при описании сервиса VPN. Действительно, техника заказа качества обслуживания виртуального канала встроена в технологию FR. Кроме того, сети FR обычно мало доступны для индивидуальных пользователей из-за своих цен и отсутствия в них информационных сервисов типа службы Web, поэтому хакерские атаки в них маловероятны. Многие провайдеры сетей FR рекламируют свои сервисы как сервисы VPN.

Сети ATM — идеальное средство для образования VPN, так как они предлагают самые тонкие процедуры поддержания параметров качества обслуживания. Однако их небольшая распространенность как публичных сетей пока не позволяет широко использовать их для построения VPN.

Сети TCP/IP и Internet до недавнего времени не фигурировали в качестве возможной среды для образования в них VPN. Основная причина — та же, что и в случае сетей X.25 — в протоколах TCP/IP нет гарантий качества обслуживания. Однако в последнее время ситуация изменилась. Сам термин VPN многие стали употреблять исключительно в связи с созданием частной сети предприятия в Internet. Безусловно, это связано со стремительно возросшей популярностью Internet, его быстро растущей доступностью и дешевизной. Из-за этого многие администраторы мирятся с неизвестной пропускной способностью каналов, проложенных через Internet.

Тем не менее VPN в сетях TCP/IP начинают приобретать свойства "настоящих" VPN. Этому способствует ряд обстоятельств.

Во-первых, провайдеры, сети которых образуют магистрали Internet, много работают над улучшением качества обслуживания. Магистрали строятся на основе ATM и SDH. Также быстро растет производительность магистральных маршрутизаторов. Это уменьшает задержки в Internet и повышает качество обслуживания.

Во-вторых, стек протоколов TCP/IP модернизируется и в нем появляются протоколы, с помощью которых можно управлять качеством обслуживания — протоколы RSVP, RTP и ряд других.

В-третьих, многие крупные провайдеры предоставляют услуги магистралей TCP/IP, не связанных непосредственно с Internet. На этих магистралях передается трафик только крупных корпоративных пользователей, поэтому защищенность данных и пропускная способность таких сервисов существенно выше.

Ряд провайдеров оказывает услуги по построению VPN. Основная часть предложений по созданию корпоративных VPN относится к провайдерам сетей FR, поэтому ограничимся рассмотрением этих сетей.

Основой для создания VPN является договор с провайдером, в котором оговариваются основные параметры VPN — количество точек подключения, скорости портов, а также параметры качества обслуживания (например, CIR и CBR) [10]. В отношении этих пунктов договора все провайдеры похожи друг на друга, так как качество обслуживания поддерживается самой технологией.

Защиту данных своими средствами провайдеры FR не обеспечивают, так как нет и особого спроса на такие услуги — администраторы не видят высокого уровня угроз и считают каналы FR достаточно защищенными. Поэтому наиболее осторожные пользователи должны защищать свои данные самостоятельно.

Основные различия между провайдерами наблюдаются в средствах контроля за реальной пропускной способностью виртуальных каналов, которые они предоставляют корпоративным пользователям. Большинство провайдеров обеспечивает пользователей еженедельными или ежемесячными отчетами о реально используемой пропускной способности виртуальных каналов, а также более детальной информацией о трафике. Иногда информация отчета посылается по электронной почте или доступна на BBS провайдера. Многие операторы берут ежемесячную плату 200 долл. за предоставление отчета. AT&T берет по 5 долл. за каждый порт. Compuserve, Sprint, ICI и некоторые другие предоставляют отчеты бесплатно.

Если по сети FR передается трафик реального времени, то администратора интересуют данные о его передаче с периодом в минуты, а не дни. Для этих целей некоторые сервис-провайдеры могут периодически посылать администратору сети SNMP-сообщения. Эти сообщения обычно непосредственно загружаются с интервалом в 15—60 мин с консоли управления типа OpenView или Netview от TivoliSysytems. Интервал доставки оговаривается в договоре с провайдером.

Только два провайдера поставляют также программное обеспечение (ПО) для отображения данных SNMP в виде графиков — Compuserve и ICI. Compuserve берет ежемесячную плату 575 долл. за FrameNetManager. ICI берет 125 долл. за свой продукт EnhancedCustomerView.

Остальные провайдеры поставляют только файлы сырых данных. Только один провайдер, LDDSWorldcom, предлагает доступ к статистике с помощью Web-сервиса. Данные обновляются каждый час, но в будущем интервал будет уменьшен до 15 мин.

В своих отчетах провайдеры дают следующую статистику: коэффициент использования на порт/PVC и процент кадров с пометкой DE (подлежит отбрасыванию). Гораздо более полезной информацией были бы данные о том, сколько кадров были отброшены сетью на самом деле, но провайдеры такой статистики не дают. Однако есть смысл попытаться получить такую статистику, оговорив ее в договоре.

Что действительно интересует администратора, так это коэффициент загрузки сети FR в целом. Пока только Ameritech, Cable & Wireless и StentorAlliance дают эти данные.

Статистика, поставляемая с периодом в 15 мин, не может дать правильного представления о кратковременных пульсациях трафика. Только Cable & Wireless соглашается поставлять данные с периодом 5 мин. SprintCompuserve рассчитывают на возможности системы VisualUptime от VisualNetworks. Эта система собирает данные через каждую минуту от агентов, внедренных в CSU/DSU пользователей. Система дает рекомендации по корректировке скорости порта и CIR. Агенты собирают также данные на уровнях 1, 2 и 3.

Sprint и Compuserve уже применяют систему VisualUptime в своих сетях. Стоимость ПО составляет от 7000 до 30000 долл., а аппаратных агентов от 1195 до 6700 долл.

1.4. Туннелирование в виртуальных частных сетях

VPN состоит из каналов глобальной сети, защищенных протоколов и маршрутизаторов (рис. 7). Для объединения удаленных ЛВС в VPN используются так называемые виртуальные выделенные каналы. Для организации подобных соединений применяется механизм *туннелирования*, или *инкапсуляции*.

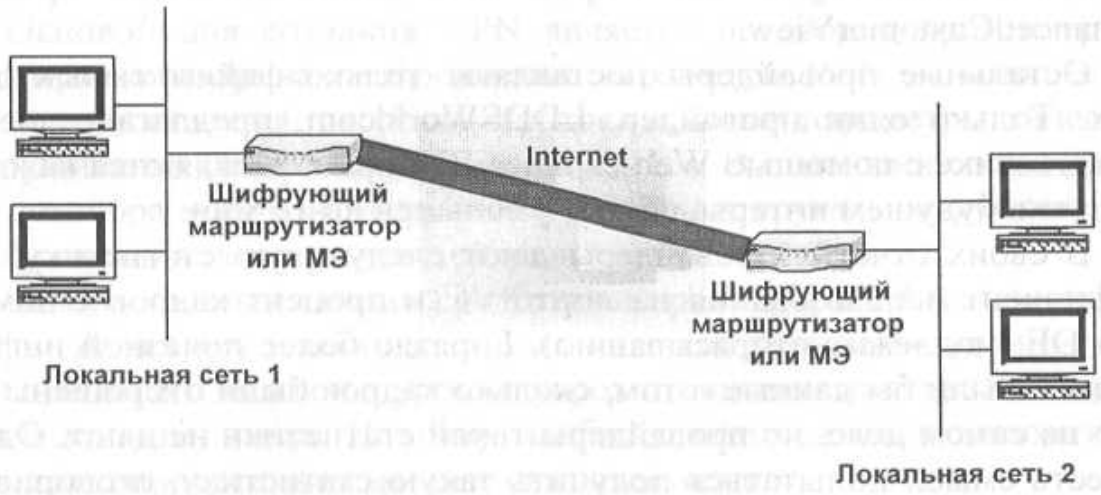


Рис. 7. Структура VPN

При туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Например, при туннелировании кадр Ethernet может быть размещен в пакете IP, а пакет IPX — в пакете IP. Возможен и такой вариант: пакет IP размещается в пакете IP.

Туннель создается двумя пограничными устройствами, которые размещаются в точках входа в публичную сеть. Инициатор туннеля инкапсулирует пакеты ЛВС (в том числе пакеты немаршрутизируемых протоколов) в IP-пакеты, содержащие в заголовке адреса инициатора и терминатора туннеля. Терминатор туннеля извлекает исходный пакет. Естественно, при подобной передаче требуется решать проблему конфиденциальности и целостности данных, что

не обеспечивается простым туннелированием. Конфиденциальность передаваемой корпоративной информации достигается шифрованием (алгоритм одинаков на обоих концах туннеля).

Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных. Исходный пакет зашифровывают полностью, вместе с заголовком, и этот зашифрованный пакет помещают в другой, внешний пакет с открытым заголовком. Для транспортировки данных по "опасной" сети используются открытые поля заголовка внешнего пакета, а при прибытии внешнего пакета в конечную точку защищенного канала из него извлекают внутренний пакет, расшифровывают и используют его заголовок для дальнейшей передачи уже в открытом виде по сети, не требующей защиты. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних пакетах в защищенном виде (рис. 8).

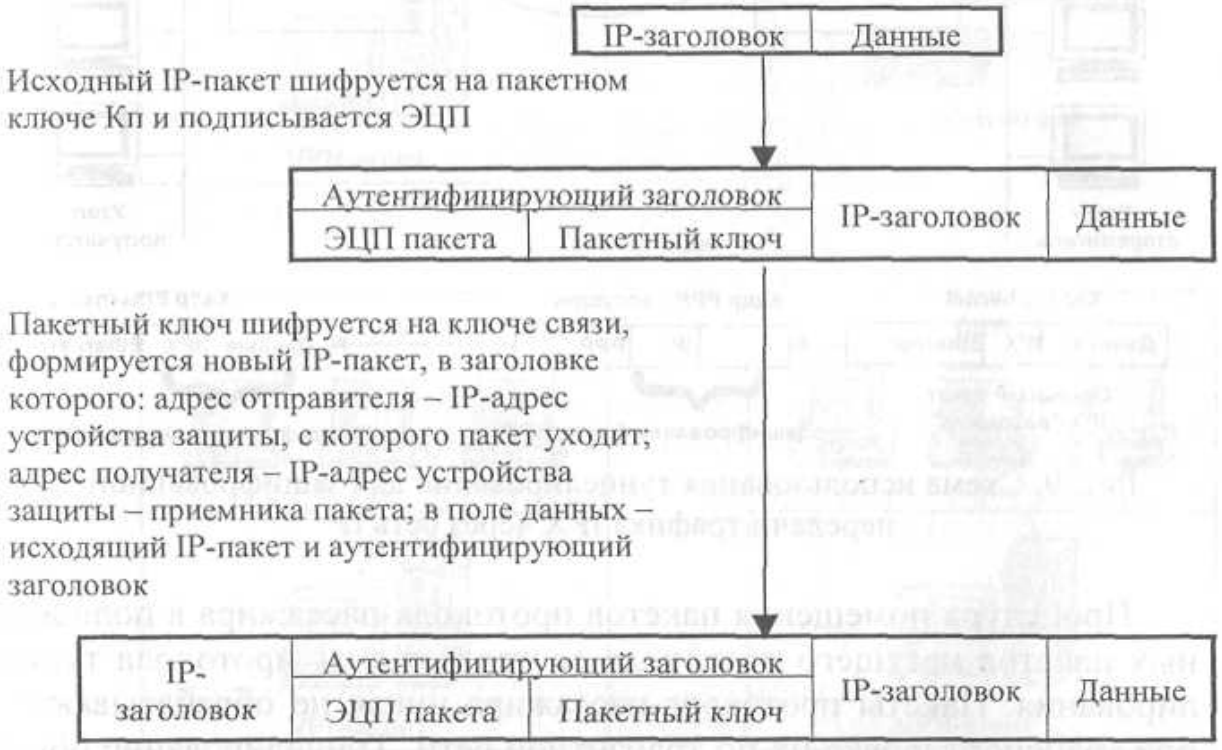


Рис. 8. Туннелирование пакетов

Механизм туннелирования можно представить как результат работы протоколов трех типов:

- протокола-пассажира;
- несущего протокола;
- протокола туннелирования.

Транспортный протокол объединяемых сетей (например, протокол IPX, переносящий данные в ЛВС филиалов одного предприятия) является протоколом-пассажиром, а протокол транзитной сети (например, протокол IP сети Internet) — несущим протоколом (рис. 9).

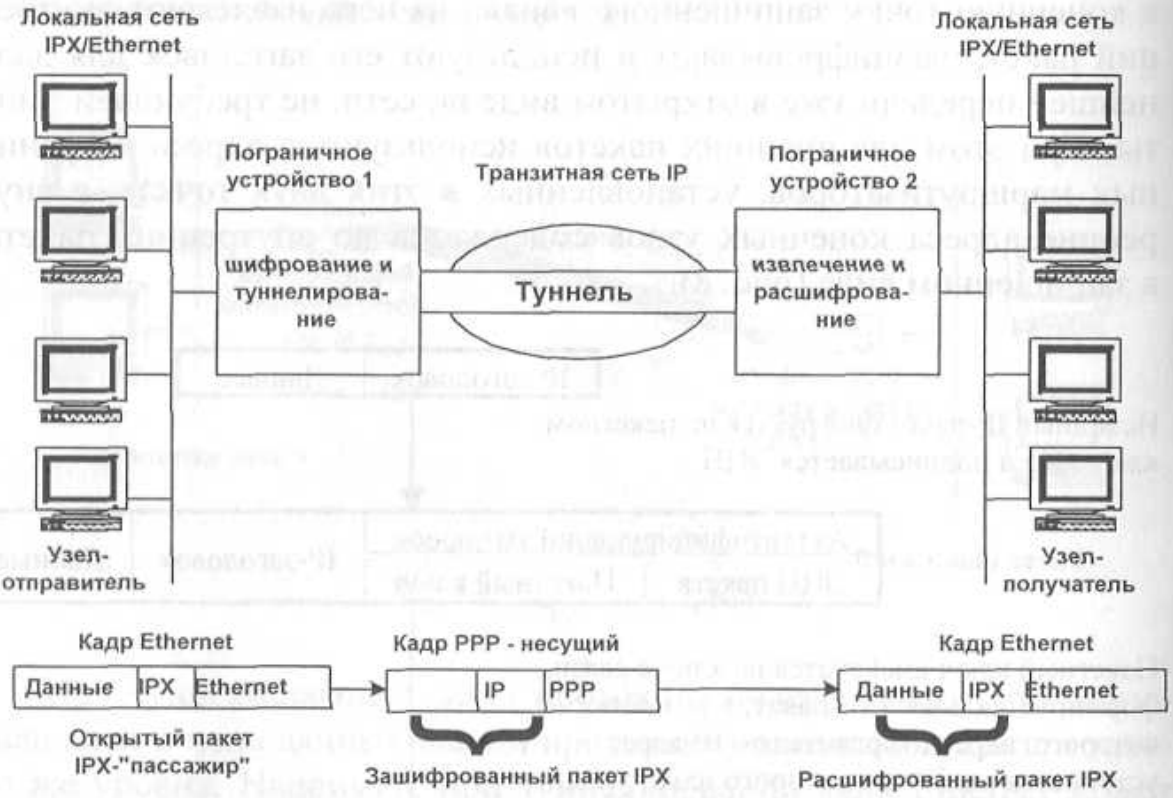


Рис. 9. Схема использования туннелирования для зашифрованной передачи трафика IPX через сеть IP

Процедура помещения пакетов протокола-пассажира в поле данных пакетов несущего протокола составляет суть протокола туннелирования. Пакеты протокола-пассажира никак не обрабатываются при транспортировке их по транзитной сети. Туннелирование обычно выполняет пограничное устройство (маршрутизатор или шлюз), которое располагается на границе между исходной и транзитной се-

тями, но этой работой может заниматься и узел-отправитель. Извлечение пакетов-пассажиров из несущих пакетов выполняет второе пограничное устройство, которое находится на границе между транзитной сетью и сетью назначения, либо узел-получатель.

1.5. Схема виртуальной частной сети

Суть VPN состоит в следующем (рис. 10) [6] — на все компьютеры, имеющие выход в Internet, устанавливается средство, реализующее VPN (VPN-агент). (Не должно остаться ни одного незащищенного!)

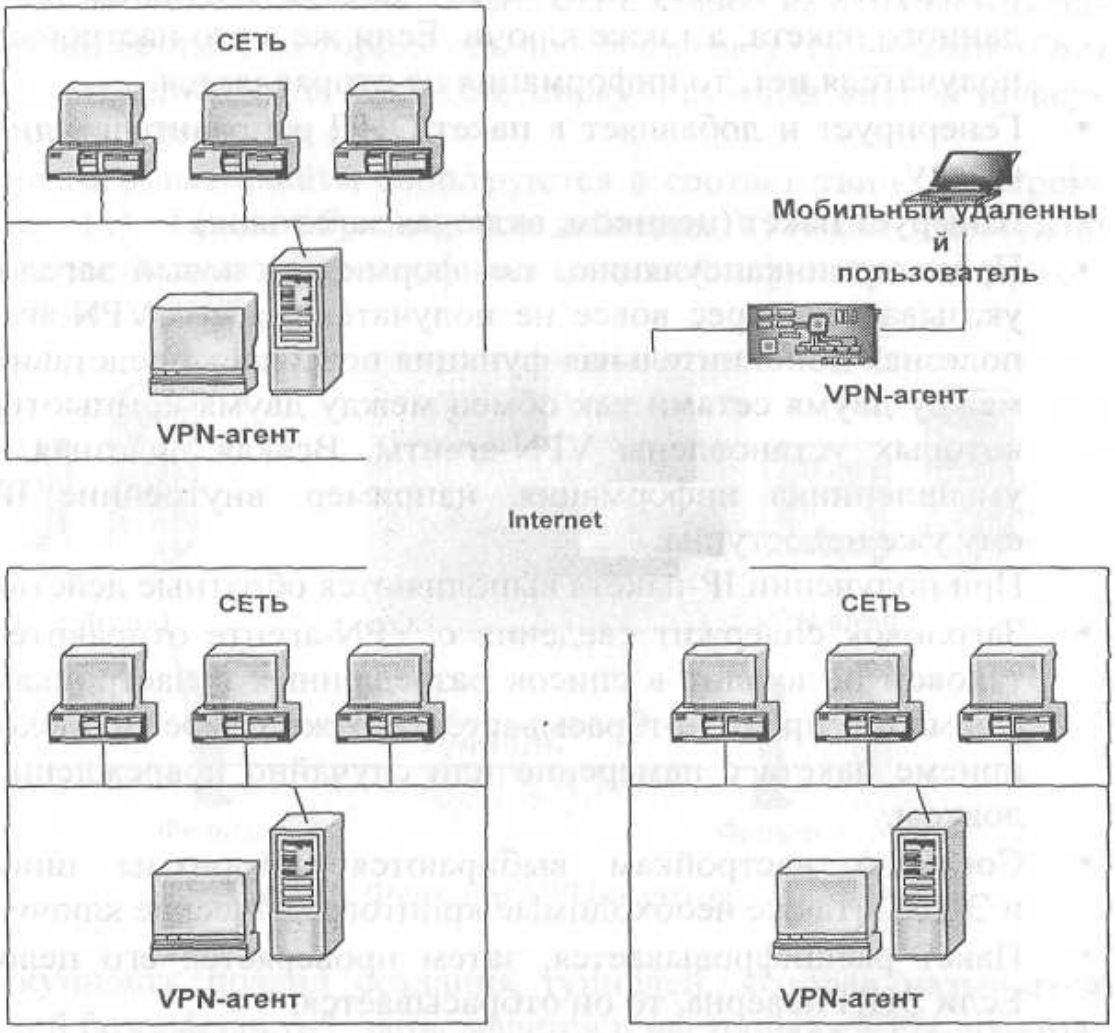


Рис. 10. Схема VPN

VPN-агенты автоматически шифруют всю исходящую информацию (и соответственно расшифровывают всю входящую). Они также следят за ее целостностью с помощью электронной цифровой подписи (ЭЦП) или имитовставок (криптографическая контрольная сумма, рассчитанная с использованием ключа шифрования). Поскольку информация, циркулирующая в Internet, представляет собой множество пакетов протокола IP, VPN-агенты работают именно с ними.

Перед отправкой IP-пакета VPN-агент действует следующим образом.

- Из нескольких поддерживаемых им алгоритмов шифрования и ЭЦП по IP-адресу получателя выбирает нужный для защиты данного пакета, а также ключи. Если же в его настройках такого получателя нет, то информация не отправляется.
- Генерирует и добавляет в пакет ЭЦП отправителя или имитовставку.
- Шифрует пакет (целиком, включая заголовок).
- Проводит инкапсуляцию, т.е. формирует новый заголовок, где указывается адрес вовсе не получателя, а его VPN-агента. Эта полезная дополнительная функция позволяет представить обмен между двумя сетями как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для злоумышленника информация, например, внутренние IP-адреса, ему уже недоступна.

  При получении IP-пакета выполняются обратные действия.
- Заголовок содержит сведения о VPN-агенте отправителя. Если таковой не входит в список разрешенных в настройках, то информация просто отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.
- Согласно настройкам выбираются алгоритмы шифрования и ЭЦП, а также необходимые криптографические ключи.
- Пакет расшифровывается, затем проверяется его целостность. Если ЭЦП неверна, то он отбрасывается.
- Пакет в его исходном виде отправляется настоящему адресату по внутренней сети.

Все операции выполняются автоматически. Сложной в технологии VPN является только настройка VPN-агентов.

VPN-агент может находиться непосредственно на защищаемом ПК, что полезно для мобильных пользователей, подключающихся к Internet из разных мест. В этом случае он обезопасит обмен данными только того компьютера, на котором установлен.

Возможно совмещение VPN-агента с маршрутизатором (в этом случае его называют криптографическим) IP-пакетов. Ведущие мировые производители в последнее время выпускают маршрутизаторы со встроенной поддержкой VPN, например Express VPN от Intel, который шифрует все проходящие пакеты по алгоритму Triple DES.

Как видно из описания, VPN-агенты создают каналы между защищаемыми сетями, которые обычно называют туннелями. Они "прорыты" от одной сети к другой; циркулирующая внутри информация спрятана от чужих глаз.

Кроме того, все пакеты фильтруются в соответствии с настройками (рис. 11). Таким образом, все действия VPN-агентов можно свести к двум механизмам: созданию туннелей и фильтрации проходящих пакетов.

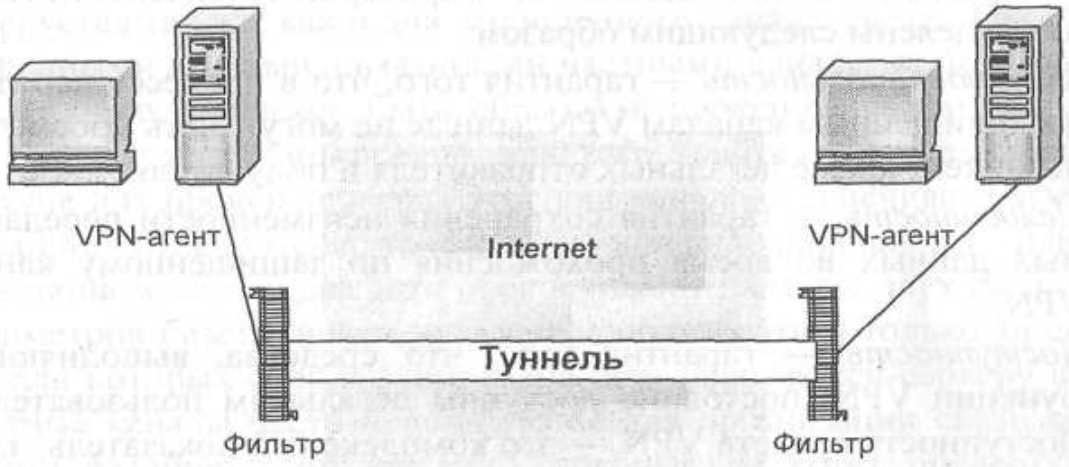


Рис. 11. Функции VPN-агентов

Совокупность правил создания туннелей, которая называется "политикой безопасности", записывается в настройках VPN-агентов. IP-пакеты направляются в тот или иной туннель или отбрасываются после того, как будут проверены:

- IP-адрес источника (для исходящего пакета — адрес конкретного компьютера защищаемой сети);
- IP-адрес назначения;
- протокол более высокого уровня, которому принадлежит данный пакет (например, TCP или UDP);
- номер порта, с которого или на который отправлена информация (например, 1080).

1.6. Политики безопасности в виртуальных частных сетях

Важным вопросом при создании VPN является то, что в каждой ЛВС должны использоваться эквивалентные политики безопасности. VPN по существу создает одну большую сеть из группы независимых ранее сетей. Поэтому безопасность VPN будет равна безопасности наименее защищенной ЛВС – если хотя бы одна ЛВС позволяет осуществить незащищенный доступ по коммутируемым линиям, то под угрозой окажутся все ресурсы VPN.

В соответствии с общепринятым определением, безопасность данных означает их конфиденциальность, целостность и доступность. Применительно к задачам VPN критерии безопасности могут быть определены следующим образом.

- *Конфиденциальность* — гарантия того, что в процессе передачи по защищенным каналам VPN данные не могут быть просмотрены никем, кроме легальных отправителя и получателя.
- *Целостность* — гарантия сохранения неизменности передаваемых данных во время прохождения по защищенному каналу VPN.
- *Доступность* — гарантия того, что средства, выполняющие функции VPN, постоянно доступны легальным пользователям. Доступность средств VPN — это комплексный показатель, зависящий от нескольких факторов: надежности реализации, качества обслуживания, а также степени защищенности самого средства от внешних атак. Если средство VPN поддерживается провайдером, то доступность является одной из характеристик, обычно включаемых в соглашение об уровне сервиса.

  Существует три основных варианта создания VPN.

1. *Защищенные каналы.* МЭ шифрует весь трафик, передаваемый удаленному хосту (хост — это компьютер, имеющий уникальный IP-адрес) или сети, и расшифровывает весь трафик, принятый от них. Трафик между хостами в VPN, связанными защищенными каналами, передается свободно, как будто между ними нет МЭ. На самом деле трафик маршрутизируется МЭ VPN. Его обработка прокси-серверами (proxy-сервер, или сервер полномочий, или сервер-посредник [к сожалению, на сегодня нет единого термина этого средства] ждет директив из сети, пересылает запрос к удаленному серверу, расположенному за пределами защитной системы, получает от него ответное сообщение и передает его по назначению) и аутентификация не требуются. Любые два хоста внутри VPN, связанные защищенными каналами, могут свободно обмениваться данными между собой, и предоставлять все сервисы TCP/IP, которые у них имеются. Защищенные каналы часто используются для соединения географически разделенных сетей, принадлежащих одной организации, каждая из которых имеет свое собственное подключение к Internet через провайдера, в одну виртуальную сеть безопасным способом.

2. *Частные каналы.* Трафик между МЭ и удаленным хостом шифруется так же, как и для защищенного канала. Но трафик между удаленными хостами, связанными частными каналами, не передается свободно, а должен быть обработан прокси-сервером МЭ и соединение аутентифицировано, как того требует обычная политика доступа для прокси-сервера. Этот вид канала обеспечивает аутентификацию отправителя трафика и конфиденциальность данных, но в данном случае две сети обеспечивают наличие двух различных периметров безопасности, и могут использоваться только те сервисы, для которых сконфигурирована передача прокси-серверу в МЭ. Частные каналы часто используются для организации связи между сетями различных организаций, которые не хотят предоставлять полного доступа к их сетям, и требуют конфиденциальности трафика между ними.

3. *Промежуточные каналы.* Эти каналы используются для промежуточной передачи зашифрованного трафика между хостами, расположенными за МЭ и входящими в состав другой VPN. Это по-

зволяет МЭ, находящемуся между двух других VPN, быть сконфигурированным так, что он только передает зашифрованные данные. Он не расшифровывает трафик и даже не знает ключа шифрования. Ему надо лишь знать адреса хостов по обе стороны МЭ, участвующих в организации этого канала, чтобы определить, какие зашифрованные пакеты пропускать. Такая архитектура позволяет использовать промежуточный МЭ как маршрутизатор.

Используя только что введенные понятия каналов VPN, приведем примеры некоторых политик безопасности (ПБ) при использовании каналов Internet для построения VPN.

1. *Высокая ПБ.* Для VPN, использующих Internet, МЭ организации должны работать в режиме частного канала, шифровать трафик VPN и требовать использования прокси-серверов МЭ для ограничения доступа к сервисам со стороны удаленных хостов VPN. Также должны иметься средства, обеспечивающие быстрое создание резервного канала для передачи в случае временной невозможности передачи через Internet.

2. *Низкая-средняя ПБ.* Для VPN, использующих Internet, МЭ организации должны работать в режиме защищенного канала, шифровать трафик VPN и не требовать использования прокси-серверов для его обработки.

3. *Средняя-высокая ПБ.* VPN между ЛВС не должны использовать Internet для передачи критичного к оперативности передачи трафика. Если уровень надежности, предоставляемый Internet, недостаточен для обеспечения требуемого уровня сервиса, для передачи данных должны использоваться другие способы.

1.7. Средства защиты информации, дополняющие виртуальные частные сети

Современные VPN-сети строятся на основе международных стандартов протокола IPSec и достижений в области инфрастуктуры открытых ключей (Public Key Infrastructure, PKI или ИОК).

Основная задача VPN — защита трафика. Эта задача исключительно сложна уже на криптографическом уровне, поскольку VPN должна удовлетворять большому числу требований. В первую оче-

редь обладать надежной криптографией, гарантирующей от прослушивания, изменения, отказа от авторства (это определяется протоколом IPSec), иметь надежную систему управления ключами, защищать от атак методом повтора сеанса протокола (replay attack) и проверять, "жив" ли абонент в данный момент (это обеспечивается принятым в 1998 г. протоколом IKE). Применение стандартных протоколов IPSec/IKE в VPN-системах сегодня практически обязательно. В противном случае ни один заказчик не сможет быть уверенным, что поставщик VPN создал криптографически целостную и надежную систему. Кроме того, в будущем она окажется несовместима с VPN, применяемыми контрагентами корпорации, что в конце концов приведет к проблеме "вавилонской башни".

Ни одна криптозащита, построенная на открытой криптографии, не может существовать без ИОК, в задачу которой входит:

- создание и подпись сертификатов, что требует наличия иерархической системы нотариусов, так как пользователь VPN должен получать свой сертификат по месту работы, а не ездить за ним, например, в центральный офис или в какую-то иную организацию;
- передача сертификатов на электронный носитель пользователя (смарт-карта, e-token, дискета) и публикация их на сервере сертификатов с тем, чтобы любой участник VPN мог легко получить сертификат своего партнера;
- регистрация фактов компрометации и публикация "черных" списков отозванных сертификатов.

VPN должна взаимодействовать с системой ИОК в целом ряде точек (передача сертификата на подпись, получение сертификата и "черного" списка при установлении взаимодействия и т.п.). Очевидно, что это взаимодействие с чуждой по отношению к VPN системой может осуществляться только при условии полной поддержки международных стандартов, которым удовлетворяет большинство современных архитектур ИОК. (Более подробно вопросы применения ИОК для поддержки протоколов VPN будут рассмотрены в третьем разделе пособия.)

Следующим важным элементом интеграции систем является наличие криптоинтерфейса. Любая система, использующая крипто-

операции (VPN, защищенная почта, программы шифрования дисков и файлов, ИОК), должна получать криптосервис из сертифицированных соответствующими органами модулей, созданных специализирующимися в этом компаниями. Опасно доверяться поставщику VPN, создавшему свой собственный, никому не известный, но, как он утверждает, надежный алгоритм.

Обеспечение безопасности — задача построения множества линий обороны и наблюдения за ними. Как бы ни осуществлялось это наблюдение — ручной разборкой регистрационной информации или с помощью систем обнаружения вторжений (Intrusion Detection Systems, IDS), нужно сначала получить эту информацию. VPN должна создавать на всех своих агентах:

- LOG-файлы с регистрационной информацией;
- SNMP-сообщения о текущих атаках, сбоях и проблемах (SNMP, Simple Network Management Protocol — простой протокол управления сетями).

Вся эта информация должна собираться и обрабатываться в том же центре управления или в одной из специализированных систем наблюдения (типа HP-OV).

Обычно VPN различает только отдельные компьютеры, но не их пользователей. Корпоративный заказчик требует, чтобы VPN отличала отдельных пользователей и отдельные приложения. Пользователь должен получить одну и ту же конфигурацию VPN независимо от того, за каким компьютером он сидит. Все необходимые для этого данные (ключи, сертификаты, конфигурация) находятся на его смарт-карте, электронном ключе или дискете. Если корпорация использует так называемые серверы доступа (технология single-sign-on), то VPN должна работать совместно с такой системой, не подключая VPN тем пользователям, которые не прошли авторизацию в системе аутентификации.

VPN образует "непроницаемые" каналы связи поверх открытых сетей. В реальной жизни организации всегда требуется, чтобы сотрудники имели доступ из VPN в открытые сети и Internet. Контроль в критичной точке контакта с открытой сетью должен осуществляться МЭ. Более правильная ситуация — VPN обеспечивает функции МЭ в каждой точке, где есть ее агент. Такой "распределенный"

МЭ контролируется из того же центра безопасности. МЭ и VPN являются взаимодополняющими системами, решая две связанные задачи:

- использование открытых сетей в качестве канала недорогой связи (VPN);
- обеспечение защиты от атак из открытых сетей при работе с открытой информацией, содержащейся в этих сетях (МЭ).

Гарантируя защиту передаваемой информации, VPN не обеспечивает ее защиту во время хранения на конечных компьютерах. Эта задача решается целым рядом специальных средств:

- систем криптозащиты файлов и дисков (а также почты);
- систем защиты от НСД к компьютерам;
- антивирусных систем и т.п.

Необходимо обратить внимание на сложную взаимосвязь продуктов защиты информации. Например, система защиты компьютера от НСД должна работать с теми же смарт-картами, что и VPN, а это требует реализации в обеих системах единого интерфейса доступа к смарт-карте (например, PKCS#11 фирмы RSA).

Средства защиты информации должны обладать следующим набором характеристик:

- соответствие открытым международным стандартам;
- открытые интерфейсы к другим средствам защиты информации;
- способность взаимодействовать с одними и теми же "интегрирующими" элементами системы;
- способность к масштабированию.

Продукты, создаваемые для защиты информации, должны быть совместимы с системами ИОК, известными на российском рынке. И, прежде всего, с сервером сертификатов — программным средством управления VPN. Сервер сертификатов предназначен для хранения в виде базы данных открытых сертификатов всех пользователей VPN. Он осуществляет автоматическую раздачу сертификатов VPN-устройствам и взаимодействие с внешними системами ИОК.

Итак, начав с отдельного средства, обеспечивающего оперативное решение проблемы защиты информации (VPN), мы рассмотрели процесс наращивания системы, добавив некоторые самые необходимые компоненты (ИОК, МЭ и т.д.).

Вопрос о том, нужно ли использовать VPN, если уже есть МЭ (и наоборот), даже не стоит на повестке дня, так как эти решения выполняют абсолютно разные задачи. МЭ — это "ограда" вокруг сети, которая препятствует проникновению сквозь нее злоумышленников, в то время как VPN — это "бронированный автомобиль", который защищает ценности при вывозе их за пределы ограды. Поэтому надо использовать оба решения для обеспечения необходимого уровня защищенности информационных ресурсов. Вопрос совместного применения МЭ и VPN возникает в случае защиты КС по всем указанным вариантам, кроме VPN на базе МЭ. Существует две крайности — устанавливать МЭ перед VPN-устройством и после него. В первом случае, возникает ситуация, когда на МЭ из Internet попадает еще нерасшифрованный трафик, что приводит к невозможности контроля передаваемого содержимого (вирусы, апплеты Java, команды протоколов и т.д.). Во втором случае ситуация несколько лучше, но само устройство VPN становится уязвимым к внешним атакам. Кроме того, оно уже не может осуществлять обработку трафика в зависимости от его содержания или пользователя, являющегося получателем данных. Идеальным решением, к которому пришло большинство зарубежных производителей (Check Point, Cisco Systems и т.д.), а также приходят отечественные разработчики — совместить в одном устройстве функции МЭ и VPN. В этом случае указанные проблемы исчезают.

Контрольные вопросы по разделу 1

1. Дайте различные определения виртуальной частной сети и поясните их.
2. Какие задачи решает построение VPN, а какие — установка МЭ?
3. Каковы значения термина "частный" применительно к VPN?
4. В чем различие использования провайдеров связи и провайдеров Internet для создания VPN?
5. Возможно ли использование только каналов связи предприятия для создания его VPN?
6. Каковы преимущества и недостатки использования Internet для создания VPN?
7. В чем заключаются маркетинговая и потребительная сущность VPN?
8. Как понимается защищенность от потоков данных в VPN?

9. Какие услуги по защите данных обеспечивают VPN?
10. Что важно для конечных пользователей при использовании VPN?
11. Каковы особенности современных сетей, на основе которых приходится создавать VPN?
12. Какие требования предъявляются к создаваемой VPN?
13. Каковы особенности построения VPN в различных сетях передачи данных (FR, ATM, X.25, TCP/IP)?
14. Какие услуги предлагают провайдеры по построению VPN?
15. В чем заключается механизм туннелирования в сетях? Каковы его особенности и схемы использования?
16. Что такое VPN-агенты и каковы их функции?
17. Дайте определение политики безопасности VPN и приведите несколько примеров.
18. Поясните определения критериев безопасности применительно к задачам VPN.
19. Какими средствами защиты информации нужно дополнить VPN, чтобы реализовать комплексную защиту?

2. СТАНДАРТНЫЕ ПРОТОКОЛЫ СОЗДАНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

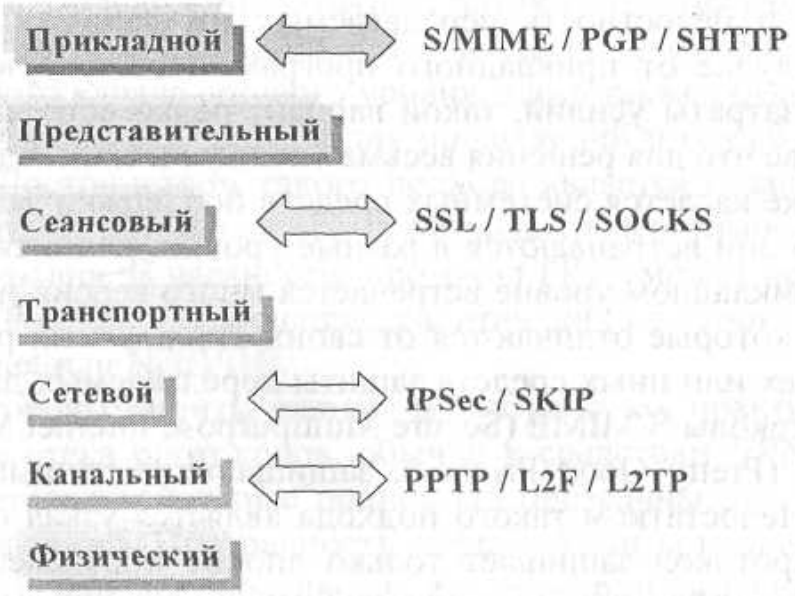
2.1. Уровни защищенных каналов

При построении VPN одной из наиболее острых является проблема совместимости. Конечные точки туннеля VPN должны использовать одни и те же методы взаимной аутентификации, шифрования данных и генерации секретных ключей. Естественное решение этой проблемы — поддержка каждым VPN-устройством некоторого набора стандартных технологий и протоколов защиты данных, чтобы при установлении защищенного соединения два узла сети в результате переговорного процесса смогли найти общую технологию и общий протокол. Особенно это важно при организации экстрасетей, когда недостаточно принять некий стандарт защиты данных в рамках одного предприятия.

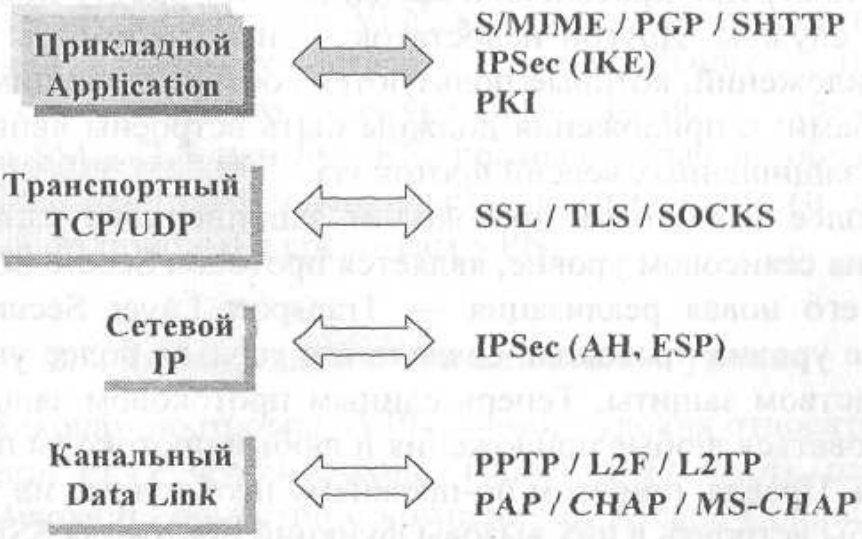
В настоящее время процесс стандартизации технологий VPN еще не достиг того уровня, при котором пользователи спокойно могут приобретать VPN-продукты разных производителей, не заботясь об их совместимости. Но значительная часть работы в этом направлении уже проделана. В конце 1998 г. была принята новая версия системы стандартов IPSec, которые, скорее всего, будут доминировать в Internet и частных IP-сетях при организации VPN. В приложении 2 приведен полный список документов (стандартов и проектов стандартов) по протоколам для создания VPN.

Важной характеристикой стандартов защищенного канала является уровень модели взаимодействия открытых систем OSI, на котором работают протоколы данного стандарта (рис. 12). Модель OSI,

разработанная Международной организацией по стандартизации (International Standards Organization – ISO), определяет семь уровней, на которых компьютерные системы взаимодействуют друг с другом, начиная с уровня физической среды передачи данных и заканчивая уровнем прикладных программ, используемых для коммуникаций.



а)



б)

Рис. 12. Уровни защищенных каналов

Защищенный канал можно построить на основе системных средств, реализованных на разных уровнях стека коммуникационных протоколов (рис. 12, а). Для сравнения (рис. 12, б) приведено соответствие этих же протоколов стеку протоколов TCP/IP. Конечно, возможен и такой вариант, когда приложение самостоятельно, без обращения к системным средствам, обеспечивает конфиденциальность и целостность передаваемых им данных. Но поскольку в этом случае от прикладного программиста требуются дополнительные затраты усилий, такой вариант редко встречается на практике, разве что для решения весьма специфических задач.

Что же касается системных средств поддержки защищенных каналов, то они встраиваются в разные уровни, начиная с прикладного. На прикладном уровне встречается много версий известных протоколов, которые отличаются от своих стандартных реализаций наличием тех или иных средств защиты передаваемых данных (например, протоколы S/MIME (Secure Multipurpose Internet Mail Extension) или PGP (Pretty Good Privacy), защищающие данные электронной почты). Недостатком такого подхода является узкая область действия — протокол защищает только вполне определенную сетевую службу — файловую, гипертекстовую или почтовую. Поэтому для каждой службы необходимо разрабатывать соответствующую защищенную версию протокола и выполнять эту работу при разработке новой службы. Другой недостаток — необходимость переписывания приложений, которые пользуются соответствующими сетевыми службами: в приложения должны быть встроены явные вызовы функций защищенных версий протокола.

Наиболее известным протоколом защищенного канала, работающим на сеансовом уровне, является протокол Secure Socket Layer (SSL) и его новая реализация — Transport Layer Security (TLS). Снижение уровня протокола сделало его гораздо более универсальным средством защиты. Теперь единым протоколом защиты могут воспользоваться любые приложения и любые протоколы прикладного уровня. Правда, при этом по-прежнему необходимо их переписывать, чтобы встроить в них вызовы функций протокола SSL.

Чем ниже по стеку расположены средства защищенного канала, тем проще их сделать прозрачными для приложений и прикладных

протоколов. Наиболее известным стандартным средством защиты сетевого уровня является протокол IPSec. Однако в этом случае приложения ограничены использованием вполне определенного протокола сетевого уровня, например, протокол IPSec применим только в IP-сетях.

Протокол защищенного канала может работать также и на канальном уровне модели OSI. К таким протоколам относится, например, протокол PPTP (Point-to-Point Tunneling Protocol). Как и в случае защищенного канала сетевого уровня, здесь также обеспечивается прозрачность средств защиты для приложений и служб прикладного уровня. Достоинством такого подхода является независимость средств защиты от применяемого протокола транспортировки пакетов сетевого уровня. В частности, протокол PPTP может переносить пакеты как в IP-сетях, так и в сетях, работающих на основе протоколов IPX, DECnet или NetBEUI.

Хотя протоколы зашиты данных могут работать практически на любом уровне стека протоколов, обычно к средствам VPN относят только те протоколы, которые полностью прозрачны для приложений и сетевых служб. Прозрачность средств защиты позволяет провайдерам услуг или корпоративным администраторам унифицированным способом обеспечивать защиту данных любых приложений, как применяемых сегодня, так и тех, которые будут применяться завтра. Поэтому к средствам VPN, как правило, относят протоколы трех уровней: канального, сетевого и транспортного, и эти уровни называют соответственно VPN-уровнями. Такие же средства, как протоколы SSL, TLS или SOCKS, прозрачностью не обладают. По этой причине некоторые специалисты не относят их (и другие непрозрачные протоколы) к средствам VPN.

2.2. Защита данных на канальном уровне

К протоколам построения VPN данного уровня относятся:

- протокол PPTP (Point-to-Point Tunneling Protocol), разработанный Microsoft совместно с компаниями Ascend Communications, 3Com/Primary Access, Ecl-Telematics и US Robotics,
- протокол L2F (Layer-2 Forwarding) компании Cisco Systems,

- протокол L2TP (Layer-2 Tunneling Protocol), объединивший оба вышеназванных протокола.

Однако эти протоколы, в отличие от IPSec, нельзя назвать полнофункциональными (например, PPTP не определяет метод шифрования).

Протоколы PPTP, L2F и L2TP объединяет то, что они представляют собой протоколы туннелирования канального уровня, которые инкапсулируют кадры канального протокола в протокол сетевого уровня. С помощью последнего данные затем передаются по составной сети. Кроме того, эти протоколы близки также и тем, что их главная область применения — решение задачи защищенного многопротокольного удаленного доступа к ресурсам КС через публичную сеть, в первую очередь через Internet. Так как практически любое клиентское ПО использует сегодня для удаленного доступа стандартный протокол канального уровня PPP, то и протоколы PPTP, L2F и L2TP основаны на инкапсуляции кадров PPP в пакеты сетевого уровня. В таком качестве используется прежде всего IP, но возможно применение и других сетевых протоколов, таких как IPX или DECnet.

Хотя все три протокола часто относят к протоколам образования защищенного канала, строго говоря, этому определению соответствует только PPTP, обеспечивающий как туннелирование, так и шифрование данных. Протоколы L2F и L2TP являются только протоколами туннелирования, а функции защиты данных (шифрование, аутентификация, целостность) в них не поддерживаются. Предполагается, что при их применении защита туннелируемых данных будет выполняться с помощью некоторого третьего протокола, например, IPSec.

Протокол PPTP. Сквозной туннельный протокол PPTP был представлен в рабочую группу PPP Extentions IETF в качестве претендента на стандартный протокол создания защищенного канала, однако в качестве стандарта так и не был утвержден. Это было связано с тем, что компания Cisco Systems примерно в то же время представила IETF свой протокол L2F, поэтому было решено не отдавать предпочтение ни одному из этих протоколов, а создать некий объединенный вариант, который получил название L2TP. Несмотря

на отсутствие статуса стандарта Internet, протокол PPTP получил практическое распространение, в основном благодаря усилиям компании Microsoft, реализовавшей его в своих операционных системах (ОС) Windows NT. Некоторые производители МЭ и шлюзов VPN также поддерживают PPTP.

PPTP никак не меняет протокол PPP, но предоставляет для него новое транспортное средство. В рамках этого протокола определяется архитектура клиент/сервер, предназначенная для разделения функций, которые существуют в текущих серверах сетевого доступа (NAS, Network Access Server) и для поддержки VPN. Сервер сети PPTP (PNS) должен работать под управлением операционной системы (ОС) общего назначения, а клиент, называемый концентратором доступа к PPTP (PAC), работает на платформе удаленного доступа. PPTP определяет протокол управления вызовами, который позволяет серверу управлять удаленным коммутируемым доступом через телефонные сети общего пользования (PSTN) или цифровые каналы ISDN или инициализировать исходящие коммутируемые соединения. PPTP использует механизм общей маршрутной инкапсуляции (Generic Routing Encapsulation, GRE) для передачи пакетов PPP, обеспечивая при этом контроль потоков и сетевых заторов. Безопасность данных в PPTP может обеспечиваться при помощи протокола IPSec.

Протокол PPTP позволяет создавать защищенные каналы для обмена данными по различным протоколам — IP, IPX или NetBEUI. Данные этих протоколов, поступающие в глобальную сеть упакованными в кадры PPP, инкапсулируются затем с помощью протокола PPTP в пакеты протокола IP, посредством которого переносятся в зашифрованном виде через любую сеть TCP/IP. Принимающий узел извлекает из пакетов IP кадры PPP, а затем обрабатывает их стандартным способом, т.е. извлекает из кадра PPP исходный пакет IP, IPX или NetBEUI и отправляет его по ЛВС.

Многопротокольность — основное преимущество инкапсулирующих протоколов канального уровня перед протоколами защищенного канала более высоких уровней. Например, протоколы IPSec или SSL ориентируются только на один протокол сетевого уровня — IP, поэтому они не могут применяться, если в КС используется IPX

или NetBEUI. Защита данных на канальном уровне является прозрачной для протоколов как прикладного, так и сетевого уровня.

В протоколе PPTP определены две схемы его применения.

Первая схема рассчитана на то, что протокол PPTP поддерживается сервером удаленного доступа ISP (Internet Service Provider — провайдера Internet) и пограничным корпоративным маршрутизатором. Защищенный канал образуется между RAS ISP и пограничным маршрутизатором (рис. 13). Это вариант защищенного канала типа "шлюз-шлюз", поэтому компьютер удаленного пользователя не должен поддерживать протокол PPTP. Пользователь связывается с сервером удаленного доступа RAS, установленного у ISP, с помощью стандартного протокола PPP, и проходит аутентификацию у провайдера. По имени пользователя RAS ISP должен найти в базе учетных данных пользователей IP-адрес пограничного маршрутизатора КС данного пользователя, поддерживающего протокол PPTP. С этим маршрутизатором RAS ISP устанавливает сессию через Internet уже по протоколу PPTP.

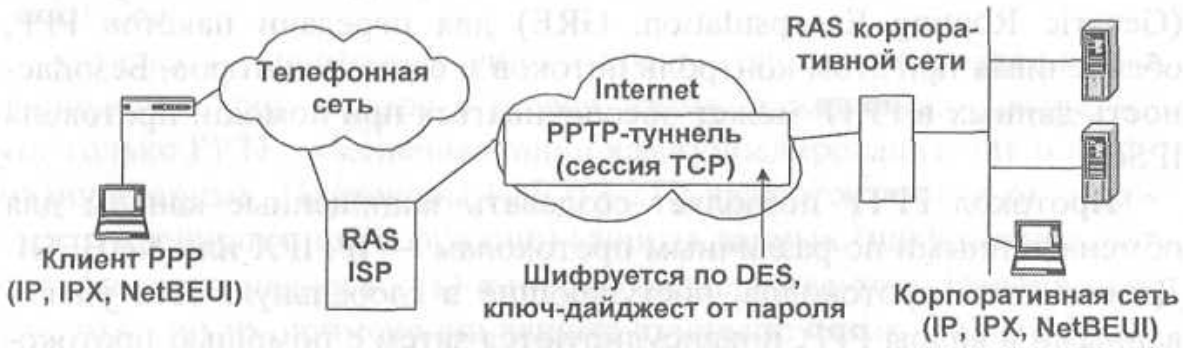


Рис. 13. Защищенный канал "провайдер — маршрутизатор КС" на основе протокола PPTP

Протокол PPTP определяет служебные сообщения, которыми обмениваются взаимодействующие стороны, причем служебные сообщения передаются по протоколу TCP. RAS ISP передает маршрутизатору КС идентификатор пользователя, по которому маршрутизатор аутентифицирует пользователя по протоколам PAP (Password Authentication Protocol) или CHAP (Challenge Handshake Authentication) — стандартным протоколам аутентификации протокола PPP.

Если пользователь прошел вторичную аутентификацию (она для него прозрачна), то RAS ISP посылает ему сообщение об этом по протоколу PPP и пользователь начинает отправлять свои данные в RAS ISP по протоколу IP, IPX или NetBIOS, упаковывая их в кадры PPP. RAS ISP осуществляет инкапсуляцию кадров PPP в пакеты IP, указывая в качестве адреса назначения адрес пограничного маршрутизатора, а в качестве адреса источника — свой собственный IP-адрес. Пакеты PPP шифруются с помощью симметричного секретного ключа, в качестве которого используется хэш-код от пароля пользователя, хранящийся в базе учетных данных RAS ISP для аутентификации по протоколу CHAP. В качестве алгоритмов шифрования используются алгоритмы RC-4 или DES.

Пакеты, переносящие пользовательские данные в рамках сессии PPTP, инкапсулируются непосредственно в пакеты IP с помощью заголовка общей маршрутной инкапсуляции GRE, определенного в RFC 1701 и 1702. Результирующий пакет представлен на рис. 14.

Заголовок канального уровня, используемого внутри Internet (PPP, SLIP, Ethernet)
Заголовок IP
Заголовок GRE
Исходный пакет PPP, включающий пакет IP, IPX, NetBEUI

Рис. 14. Структура пакета PPTP

Внутренние серверы КС также не должны поддерживать протокол PPTP, так как пограничный маршрутизатор извлекает кадры PPP из пакетов IP и посылает их по сети в необходимом формате — IP, IPX или NetBIOS.

Описанная схема не нашла широкого применения, поскольку протокол PPTP далеко не всегда поддерживается маршрутизаторами и RAS провайдеров Internet. Поэтому компания Microsoft предложила также и другую схему использования протокола PPTP, которая не требует поддержки протокола PPTP RAS провайдера. Защищенный канал во второй схеме (рис. 15) образуется между компьютером удаленного пользователя и пограничным маршрутизатором КС, который, как и в первой схеме, должен поддерживать PPTP.

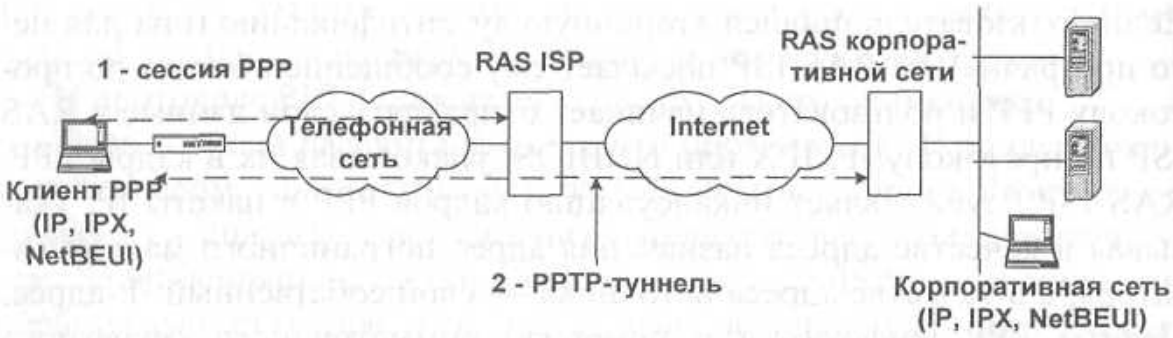


Рис. 15. Защищенный канал "пользователь — маршрутизатор КС" на основе протокола PPTP

В качестве такого маршрутизатора сегодня может выступать программный маршрутизатор Windows NT 4.0 с установленной службой RAS (без службы RAS протокол PPTP работать не будет), либо другой маршрутизатор с поддержкой PPTP. Если предприятие хочет использовать в качестве пограничного маршрутизатора аппаратный маршрутизатор, который не поддерживает PPTP, то туннель можно создать между удаленным клиентом и любым внутренним компьютером КС, на котором работа.т служба RAS и протокол PPTP. Пользователь дважды устанавливает удаленное соединение с помощью утилиты Dial-Up Networking, представляющей собой клиентскую часть сервиса удаленного доступа RAS Windows NT. В первый раз он звонит на сервер RAS ISP и устанавливает с ним связь по протоколу PPP, проходя аутентификацию одним из способов, поддерживаемых провайдером — по протоколам PAP, CHAP или с помощью терминального диалога.

После аутентификации у провайдера пользователь вторично "звонит", на этот раз на компьютер КС, где работает протокол PPTP (на рисунке этот компьютер выполняет роль пограничного маршрутизатора КС). Этот "звонок" отличается от обычного тем, что вместо телефонного номера указывается IP-адрес RAS Windows NT, подключенного к Internet со стороны КС. При этом устанавливается сессия по протоколу PPTP между клиентским компьютером и компьютером КС. Клиент еще раз аутентифицируется, теперь уже на сервере RAS его КС, а затем начинается передача данных, как

и в первом варианте. Для сокращения ручного труда Microsoft предлагает пользоваться возможностями скриптов в RAS Windows NT.

Протокол L2F. Протокол эстафетной передачи на втором уровне был разработан компанией Cisco Systems. Он обеспечивает туннелирование протоколов канального уровня (т.е. фреймов High-Level Data Link Control [HDLC], async HDLC или Serial Line Internet Protocol [SLIP]) с использованием протоколов более высокого уровня, например IP. С помощью таких туннелей можно разделить местоположение RAS, к которому подключается пользователь, используя местные коммутируемые линии связи, и точки, где происходит непосредственная обработка протокола удаленного доступа (SLIP, PPP) и пользователь получает доступ в сеть. Эти туннели дают возможность использовать приложения, требующие удаленного доступа с частными адресами IP, IPX и AppleTalk через протокол SLIP/PPP по существующей инфраструктуре Internet. Поддержка таких многопротокольных приложений виртуального удаленного доступа очень выгодна конечным пользователям и независимым поставщикам услуг, поскольку позволяет разделить на всех расходы на средства доступа и базовую инфраструктуру и дает возможность осуществлять доступ через местные линии связи. Кроме того, такой подход защищает инвестиции, сделанные в существующие приложения, работающие не по протоколу IP, предоставляя защищенный доступ к ним и в то же время поддерживая инфраструктуру доступа к Internet. Видно, что протоколы L2F и PPTP имеют сходную функциональность.

Протокол L2TP. Компании Cisco и Microsoft согласились вместе (в рамках IETF) разработать единый стандартный протокол, который получил название туннельного протокола второго уровня. Протокол L2TP обладает следующими свойствами.

- Он прозрачен для конечных систем: ни удаленной конечной системе, ни корпоративному серверу не требуется дополнительное специальное ПО, чтобы пользоваться этим сервисом.
- Аутентификация обеспечивается с помощью PPP CHAP/PAP или посредством других протоколов перед стартом сессии PPP. Могут также использоваться такие системы, как TACACS+, RADIUS (Remote Authentication Dial-In User Service), токены

доступа и одноразовые пароли. Аутентификация выполняется в КС независимо от провайдера Internet.

- Адресация конечного узла осуществляется по той же схеме, что и при прямом звонке на RAS КС. Адрес назначается не провайдером, а из КС.
- Авторизация, как и при прямом звонке, также управляется из КС.
- Учет выполняется как провайдером (в целях оплаты), так и пользователем (в целях аудита и возврата оплаты).

Протокол L2TP предполагает использование схемы, в которой туннель образуется между RAS провайдера и маршрутизатором КС (рис. 16). В терминах L2TP сервер удаленного доступа провайдера, оснащенный протоколом L2TP, называется концентратором доступа LAC (L2TP Access Concentrator), а корпоративный маршрутизатор, поддерживающий L2TP, — сетевым сервером LNS (L2TP Network Server). Удаленный пользователь инициирует PPP-соединение с провайдером через ТфОП (телефонные сети общего пользования) или ISDN (Integrated Services Digital Network — цифровая сеть интегрального обслуживания). Концентратор LAC принимает соединение и устанавливает канал PPP. Протокол L2TP позволяет концентратору свериться с LNS после приема уведомления о звонке, но до приема этого звонка — такая техника полезна в том случае, когда уведомление о звонке содержит информацию о номере вызывающей стороны.

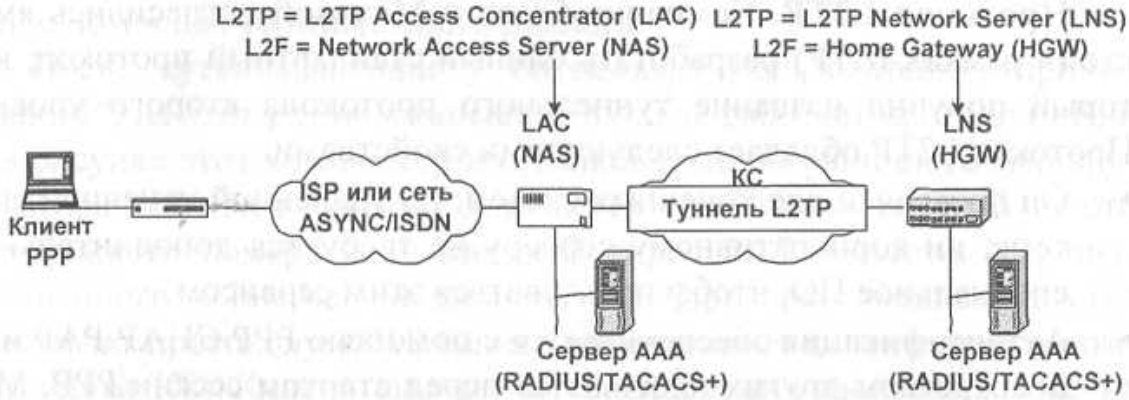


Рис. 16. Применение L2TP

После этого провайдер выполняет частичную аутентификацию конечного узла и его пользователя. Для этого используется только имя пользователя, с помощью которого провайдер решает, нужен ли пользователю сервис туннелирования L2TP. Если такой сервис нужен, то следующим шагом для LAC будет выяснение адреса сетевого сервера LNS, с которым нужно установить туннельное соединение. Желательно, чтобы имя пользователя указывалось в структурированном виде, например, user@company.com. Это дает возможность простого определения имени сетевого сервера LNS, обслуживающего сеть пользователя, к которой он должен получить доступ. Другим способом определения соответствия между пользователем и его сервером LNS может быть база данных, поддерживаемая провайдером для своих клиентов. Кроме того, провайдер может определить LNS по номеру вызывающего сервис пользователя, если его предоставит телефонная сеть.

После выяснения адреса сервера LNS проверяется, не существует ли уже туннель L2TP с этим сервером, и если нет, то он устанавливается. Протокол L2TP разработан с максимально возможной степенью изоляции его от деталей транспорта публичной сети, через которую прокладывается туннель. Единственное требование, предъявляемое к транспорту, состоит в том, чтобы он поддерживал пакетный режим взаимодействия "точка-точка". Таким транспортом может быть, например, протокол UDP, постоянные виртуальные соединения FR или коммутируемые виртуальные соединения X.25.

При существовании туннеля между LAC и LNS новому соединению в рамках этого туннеля присваивается идентификатор, называемый идентификатором вызова (Call ID). LAC посылает LNS пакет с уведомлением о вызове с данным Call ID. Сервер LNS может принять вызов или отклонить его.

Уведомление о вызове может включать информацию для аутентификации пользователя LSN, которую собрал LAC в процессе общения с пользователем. В случае применения CHAP пакет уведомления включает слово-вызов, имя пользователя и его ответ. Для протокола PAP или текстового диалога эта информация состоит из имени пользователя и незашифрованного пароля. Сервер LNS может использовать эту информацию для выполнения аутентификации,

чтобы не прибегать к дополнительному циклу аутентификации и не заставлять удаленного пользователя повторно вводить свои данные.

При отправке результата аутентификации сервер LNS может также передать концентратору LAC данные об адресе узла пользователя (например, о его IP-адресе), которые LAC передаст по протоколу PPP этому узлу. В сущности, концентратор LAC работает как посредник между узлом удаленного пользователя и сервером LNS КС. Выделение адреса для удаленного узла из пула адресов КС позволяет избежать многих неудобств, с которыми удаленный пользователь сталкивается при традиционном получении адреса из пула провайдера. В последнем случае пользователь часто не может получить доступ к ресурсам КС, так как они защищены МЭ или фильтрующим маршрутизатором, настроенными на пропуск внутрь сети только пакетов со "своими" адресами. Кроме того, сервер LNS может снабдить удаленный узел IP-адресами из частных диапазонов, или же IPX-адресами — главное, чтобы эти адреса имели корректное значение для КС, а при передаче через публичную сеть они не используются.

После приема вызова сервер LNS создает "виртуальный интерфейс" PPP в том же стиле, что и при поддержании обычного PPP-соединения. Теперь по туннелю между LAC и LNS инкапсулированные кадры PPP могут передаваться в обоих направлениях. При поступлении кадра PPP от удаленного пользователя LAC удаляет из него байты обрамления кадра, байты контрольной суммы, инкапсулирует его с помощью L2TP в сетевой протокол и отправляет по туннелю серверу LNS. Сервер LNS после извлечения из прибывшего пакета с помощью протокола L2TP кадра PPP обрабатывает его стандартным образом.

Так как L2TP может работать поверх любого транспорта с коммутацией пакетов, то в общем случае этот транспорт (например, UDP) не обеспечивает гарантированной доставки пакетов. Поэтому протокол L2TP самостоятельно занимается этими вопросами за счет процедуры установления соединения внутри туннеля для каждого удаленного пользователя, а также для нумерации передаваемых пакетов по каждому соединению и восстановления потерянных и искаженных пакетов.

Хотя протокол L2TP имеет пока только статус Internet Draft, список производителей, поддерживающих этот протокол, очень обширен и постоянно пополняется.

Для наибольшей наглядности приведенных описаний сравним возможности трех протоколов защиты данных на канальном уровне (табл. 2).

Таблица 2. **Сравнение протоколов защиты данных на канальном уровне**

Свойства	PPTP	L2F	L2TP
Задание частных адресов	+	+	+
Многопротокольность	+	+	+
Типы звонков	Входящие и исходящие	Входящие	Входящие и исходящие
Протокол управления	TCP порт 1723	UDP порт 1701	UDP порт 1701
Шифрование	Microsoft PPP (MPPE)	MPPE, IPSec опционально	MPPE/ECP, IPSec опционально
Аутентификация	PPP (пользователь)	PPP (пользователь), IPSec опционально (пакет)	PPP (пользователь), IPSec опционально (пакет)
Туннельный режим	Использование по желанию	Обязательное использование	Возможны оба подхода
Много звонков на один туннель	-	+	+
Многоканальная поддержка PPP	-	+	+

2.3. Защита данных на сетевом уровне

Протокол IPSec. Возможность построения VPN на оборудовании и ПО различных производителей достигается внедрением некоторого стандартного механизма. Таким механизмом выступает протокол Internet Protocol Security (IPSec). Он описывает все стандартные методы VPN и определяет методы идентификации при инициализации туннеля, методы шифрования в конечных точках туннеля и механизмы обмена и управления ключами шифрования между этими точками. Правда, этот протокол ориентирован исключительно на IP-протокол.

IPSec называют в стандартах Internet системой, что соответствует действительности. Это система открытых стандартов, которая имеет на сегодня четко очерченное ядро и в то же время позволяет достаточно просто дополнять ее новыми протоколами, алгоритмами и функциями. Этому способствует ее открытое построение, включающее все новые достижения в области криптографии. Осенью 1998 г. были приняты пересмотренные спецификации RFC на все основные компоненты IPSec, а совместная работа этих компонентов описана в стандарте RFC 2401 "Security Architecture for the Internet Protocol". По сравнению с первыми версиями стандартов IPSec, принятых в 1996 г., пересмотренные в 1998 г. спецификации стали более конкретными. Например, применение IKE снимает большую степень неопределенности при управлении ключами, отличавшую первую версию стандартов IPSec.

IPSec решает следующие основные задачи установления и поддержания защищенного соединения:

- аутентификацию пользователей или компьютеров при инициации защищенного соединения;
- шифрование и аутентификацию передаваемых данных между конечными точками соединения;
- автоматическое снабжение конечных точек секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Для решения поставленных задач система IPSec использует протоколы трех типов:

- протокол обмена ключами Internet IKE (Internet Key Exchange), предназначенный для первоначального этапа установки соединения и определяющий способ инициализации защищенного канала, а также процедуры обмена и управления секретными ключами в рамках защищенного соединения, методы шифрования и др.;
- протокол AH (Authentication Header), который обеспечивает целостность и аутентификацию источника данных в передаваемых пакетах, а также опционально — защиту от ложного воспроизведения пакетов (в заголовке AH данные пакета не шифруются);

- протокол ESP (Encapsulation Security Payload), обеспечивающий шифрование, аутентификацию и целостность передаваемых данных, и опционально — защиту от ложного воспроизведения пакетов (данные и заголовок шифруются в соответствии с этим протоколом).

Для шифрования данных в IPSec может быть применен любой симметричный алгоритм шифрования, использующий секретные ключи. Проверка целостности и аутентификация данных выполняются с помощью вычисления хэш-кода данных.

Для решения задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами используется протокол IKE (тогда как IPSec кодирует и подписывает пакеты). Протокол IKE автоматизирует обмен ключами и устанавливает безопасное соединение. Кроме того, IKE позволяет изменять ключ для уже установленного соединения, что повышает конфиденциальность передаваемой информации.

IKE является комбинацией нескольких протоколов — ISAKMP, Oakley и SKEME. Дело в том, что общие правила управления безопасными соединениями (в стандартах IPSec "безопасная ассоциация" или "контекст безопасности" — Security Association, SA) в IP-сетях определяет протокол ISAKMP. Однако он задает только последовательность этапов установления безопасной ассоциации, форматы пакетов, с помощью которых ассоциация устанавливается и разрывается, формулирует требования к процедурам аутентификации сторон и обмена секретными ключами, но сами протоколы аутентификации сторон и обмена ключами в нем детально не определены. Поэтому разработчики протокола IKE дополнили общие правила и процедуры протокола ISAKMP процедурами аутентификации и обмена ключами, взятыми из протоколов Oakley и SKEME. Из-за того, что протокол IKE использует для управления ассоциациями алгоритмы и форматы протокола ISAKMP, эти названия иногда используют как синонимы.

Аутентичность сторон в IKE устанавливается одним из двух способов. Первый способ предполагает выполнение протокола аутентификации типа "запрос-ответ" с использованием хэш-функции с общим секретным ключом (например, MD5). Во втором способе

используются сертификаты открытых ключей стандарта X.509. Каждая из сторон подписывает свой сертификат своим секретным ключом и передает эти данные противоположной стороне. Если проверка подписанного сертификата другой стороной дает положительный результат, то это удостоверяет тот факт, что сторона, предоставившая данные, действительно обладает соответствующим секретным ключом. Правда, для удостоверения аутентичности стороны нужно еще удостовериться в аутентичности самого сертификата, и для этого сертификат должен быть подписан не только его владельцем, но и некоторой третьей стороной, выдавшей сертификат и вызывающей доверие. Эта сторона называется удостоверяющим центром (УЦ) (перевод с английского Certificate Authority, CA), и ее открытый ключ должен быть известен всем узлам, использующим ее сертификаты для удостоверения личностей друг друга. В пределах одной организации эта проблема не вызывает больших сложностей. Достаточно во все узлы предварительно ввести открытый ключ единственного на предприятии сервера сертификатов, который выполняет роль УЦ для всех узлов и пользователей КС данного предприятия. Однако при взаимодействии узлов различных организаций, которые в общем случае используют сертификаты, выданные разными УЦ, проблема становится достаточно сложной. Должна существовать иерархия УЦ, во главе которой находятся несколько УЦ, открытые ключи которых всем известны. Кроме того, необходим автоматический протокол проверки подлинности сертификата. С его помощью последовательно проверяется подлинность подписей УЦ вплоть до того УЦ, публичный ключ которого известен стороне, выполняющей аутентификацию. В целом такую иерархическую систему выдачи и удостоверения сертификатов в публичных сетях называют ИОК. Для Internet разработано несколько подобных стандартов, например, PKIX.

После проверки аутентичности сторон протокол IKE использует алгоритм Диффи—Хеллмана, с помощью которого стороны определяют разделяемый секретный ключ, который будет использоваться в безопасной ассоциации протоколами AH или ESP. У этого ключа есть время жизни — если оно истекает, то данная ассоциация принудительно разрывается и устанавливается новая, для которой зано-

во определяется другой секретный ключ. Кроме разделяемого секретного ключа, на этой стадии стороны могут согласовать и другие параметры ассоциации.

Взаимодействуют протоколы IKE, AH и ESP следующим образом. Сначала с помощью протокола IKE между двумя точками устанавливается SA. При установлении канала выполняется аутентификация его конечных точек, а также выбираются параметры защиты данных, например, алгоритм шифрования, сеансовый секретный ключ и т.п. Затем в рамках установленного канала SA начинает работать протокол AH или ESP (но не оба сразу), с помощью которого и выполняется требуемая защита передаваемых данных с использованием выбранных параметров. Возможности протоколов AH и ESP частично перекрываются: протокол AH занимается только обеспечением целостности и аутентификации данных, а протокол ESP, как более мощный, может шифровать данные и выполнять функции протокола AH. Протокол ESP может поддерживать функции шифрования и аутентификации/целостности в любых комбинациях, т.е. либо и ту и другую группу функций, либо только аутентификацию/целостность, либо только шифрование.

В рамках одной ассоциации SA может работать только один из протоколов защиты данных — либо AH, либо ESP, но не оба вместе. Если же администратор хочет применить к пакетам одновременно оба эти протокола, то он должен создать две ассоциации между конечными точками. Такой подход дает администратору большую свободу выбора способа защиты данных.

Разделение функций защиты на два протокола — AH и ESP — вызвано практикой, применяемой во многих странах на ограничение экспорта и/или импорта средств, обеспечивающих конфиденциальность данных путем шифрования. Каждый из этих двух протоколов может использоваться как самостоятельно, так и одновременно с другим. Так что в тех случаях, когда шифрование из-за действующих ограничений применять нельзя, можно поставлять систему только с протоколом AH. Естественно, защита данных с помощью протокола AH во многих случаях будет недостаточной. В этом случае принимающая сторона уверена только в том, что данные были отправлены именно тем узлом, от которого они ожидаются, и дошли

в том виде, в котором были отправлены. От несанкционированного просмотра по пути следования данных протокол AH защитить не может, так как не шифрует их. Для шифрования данных необходимо применять протокол ESP, который может также и проверить их целостность и аутентичность. В некоторых случаях имеет смысл совместное применение протоколов ESP и AH, так как это обеспечивает более надежную защиту, чем использование только ESP.

Для работы протоколов AH и ESP по защите передаваемых данных между двумя конечными точками должна существовать безопасная ассоциация SA. Параметры SA определяют, какой из двух протоколов, AH или SPE, применяется для защиты данных; если конечный узел представляет собой хост, то в каком режиме — транспортном или туннельном — работает протокол защиты; какие функции выполняет протокол защиты, например, только аутентификации и целостности, или же еще и защиты от ложного воспроизведения. Очень важным параметром безопасной ассоциации является секретный ключ (или ключи), используемый в работе протоколов AH и ESP для защиты данных.

Параметры SA должны устраивать обе стороны, поддерживающие защищенный канал. Кроме того, при установлении ассоциации необходима взаимная аутентификация сторон. Без аутентификации данные могут передаваться защищенным образом, но не тому лицу, а значит, все меры защиты будут работать вхолостую.

Система IPSec разрешает применять два способа установления SA: ручной и автоматический. При ручном способе администратор или администраторы конфигурируют каждый конечный узел таким образом, чтобы они поддерживали согласованные параметры SA, включая и секретный ключ. Для автоматического установления SA необходим соответствующий протокол, в качестве которого в стандартах IPSec определен протокол IKE.

Хотя базовые протоколы в IPSec определены жестко, тем не менее эта система обеспечивает высокую степень гибкости за счет возможности использования различных алгоритмов аутентификации и шифрования. Гибкость IPSec состоит в том, что для каждой задачи предлагается несколько способов ее решения. При установлении соединения две конечные точки защищенного канала согласуют

способ решения данной задачи с помощью переговорного процесса. Выбранные методы для одной задачи обычно не зависят от методов реализации других задач. Так выбор в качестве алгоритма шифрования DES не влияет на выбор функции для вычисления хэш-кода, используемого для аутентификации данных. Одновременно для обеспечения совместимости продуктов разных производителей рабочая группа IETF определила базовый набор поддерживаемых функций и алгоритмов, который должен быть однотипно реализован во всех продуктах, поддерживающих IPSec. Механизмы AH и ESP могут использоваться с различными схемами аутентификации и шифрования, некоторые из них являются обязательными. Например, в IPSec определено, что пакеты аутентифицируются либо с использованием хэш-функции MD5, разработанной RSA Data Security Inc., либо с помощью хэш-функции SHA-1, разработанной U.S. *National* Security Agency (NSA), а шифруются с помощью алгоритма DES. Производители продуктов, в которых работает IPSec, вольны добавлять другие алгоритмы аутентификации и шифрования. Например, многие реализации IPSec поддерживают алгоритм Triple DES, который выполняет три операции шифрования по стандарту DES для каждого пакета. Некоторые реализации поддерживают также алгоритмы Blowfish, Cast, CDMF, Idea, RC5.

Принципиальным ограничением IPSec является то, что он поддерживает только те приложения, которые используют для передачи данных на сетевом уровне протокол IP. Это значит, что приложения IPX или NetBEUI не могут непосредственно воспользоваться функциями защиты, обеспечиваемыми IPSec. Такое ограничение, правда, будет все меньше и меньше затруднять работу по защите передаваемых данных, так как в настоящее время в мире только 1 % компьютеров вообще не поддерживает IP. Остальные 99 % используют его либо как единственный протокол, либо в качестве одного из нескольких протоколов.

Но и для случая, когда через Internet необходимо передать трафик протокола, отличного от IP, существует стандартное решение. IPSec может работать совместно с протоколами L2TP или L2F, которые выполняют только туннелирование (без шифрования и аутентификации данных). Эти протоколы создают туннель для пакетов лю-

бых протоколов, упаковывая их в пакеты IP. Трафик с помощью L2F или L2TP упаковывается в пакеты IP, а дальше можно использовать IPSec для его защиты. Таким образом, комбинирование IPSec с универсальными протоколами туннелирования типа L2F/L2TP решает задачу защиты данных и для протоколов, отличных от IP.

Протокол IPSec может защищать как трафик текущей версии протокола IPv4, применяемой сегодня в Internet, так и трафик новой версии IPv6. Последняя постепенно внедряется в Internet, образуя там островки будущей магистрали.

Протоколы AH и ESP могут защищать данные в двух режимах: транспортном и туннельном. В транспортном режиме передача IP-пакета через сеть выполняется с помощью оригинального заголовка этого пакета. В туннельном режиме исходный пакет помещается в новый IP-пакет и передача данных по сети выполняется на основании заголовка нового IP-пакета. SA представляет собой в IPSec однонаправленное (симплексное) логическое соединение, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA. При этом режим работы каждой из них (транспортный или туннельный) не зависит от режима работы другой ассоциации.

Применение того или иного режима зависит от требований, предъявляемых к защите данных, а также от роли узла, в котором работает IPSec. Существует две основные схемы применения IPSec, отличающиеся ролью узлов, завершающих защищенный канал.

В первой схеме защищенный канал SA устанавливается между узлами H1* и H2*, представляющими собой конечные узлы сети, т.е. хосты (рис. 17, а). Звездочки при именах узлов отмечают тот факт, что в данном узле работает протокол IPSec. В этой схеме протоколы IPSec защищают тот узел, на котором выполняются. Во второй схеме (рис. 17, б) защищенный канал устанавливается между двумя узлами, являющимися шлюзами безопасности — SG1* и SG2* (SG — Security Gateway). Эти шлюзы принимают данные от конечных узлов H1 и H2, подключенных к сетям, которые расположены позади шлюзов безопасности. Хосты H1 и H2 не поддерживают протокол IPSec. Они передают свой трафик в незащищенном виде через сети предприятий, которые считаются заслуживающими доверия. Трафик, направляемый в публичную сеть, проходит через шлюз безо-

пасности, который и выполняет его защиту с помощью IPSec, действуя от своего имени.

Для хостов, поддерживающих IPSec, разрешается использовать как транспортный режим, так и туннельный. Шлюзы же могут использовать только туннельный режим работы.

Если хост использует транспортный режим IPSec, то он защищает не все поля исходного IP-пакета. Протокол ESP в этом режиме аутентифицирует, проверяет целостность и шифрует только поле данных пакета IP. Другими словами, он защищает пакеты протоколов, расположенных в стеке выше протокола IP — протоколов TCP, UDP, FTP, HTTP и т.п. Шифровать заголовок IP-пакета в этом режиме ESP не может — иначе маршрутизатор не сумеет прочитать поля заголовка и корректно выполнить продвижение пакета между сетями.

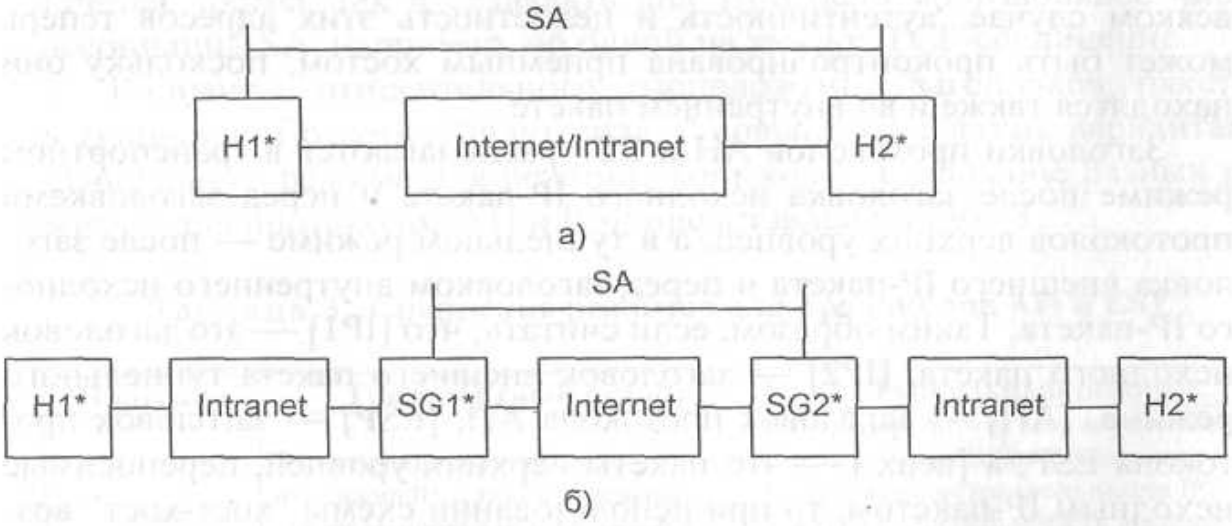


Рис. 17. Схемы применения защищенного канала SA

Протокол AH в транспортном режиме защищает больше полей, чем ESP, но все-таки не все. AH аутентифицирует и проверяет целостность поля данных пакета IP и большинства полей его заголовка, за исключением полей, которые изменяются непредсказуемым образом в процессе передачи пакета по IP-сети. Например, целостность значения поля TTL, которое уменьшается на единицу каждым промежуточным маршрутизатором, в приемной точке канала оценить нельзя. При вычислении дайджеста в момент отправления пакета

учитывается исходное значение поля TTL, а при получении пакета это значение никак не может совпадать с исходным. Поэтому традиционные методы контроля целостности, основанные на проверке хэш-кода, здесь применяться не могут.

Скрыть IP-адреса источника и назначения от возможного просмотра посторонними лицами в транспортном режиме не удается, так как эти поля всегда присутствуют в незашифрованном виде и соответствуют действительным адресам хостов.

В туннельном режиме ПО стека TCP/IP хоста сначала генерирует традиционный IP-пакет, а затем протоколы AH или ESP системы IPSec упаковывают его в новый, внешний пакет. Вся передача данных по составной IP-сети выполняется на основании заголовка внешнего пакета. Внутренний пакет становится при этом полем данных внешнего. Во внешнем пакете указываются те же IP-адреса, что и во внутреннем, поэтому скрыть их хостам опять не удается. Но, во всяком случае, аутентичность и целостность этих адресов теперь может быть проконтролирована приемным хостом, поскольку они находятся также и во внутреннем пакете.

Заголовки протоколов AH и ESP располагаются в транспортном режиме после заголовка исходного IP-пакета и перед заголовками протоколов верхних уровней, а в туннельном режиме — после заголовка внешнего IP-пакета и перед заголовком внутреннего исходного IP-пакета. Таким образом, если считать, что [IP1] — это заголовок исходного пакета, [IP2] — заголовок внешнего пакета туннельного режима, [AH] — заголовок протокола AH, [ESP] — заголовок протокола ESP, а [верх.] — это пакеты верхних уровней, переносимые исходным IP-пакетом, то при использовании схемы "хост-хост" возможны следующие варианты относительного расположения заголовков и пакетов.

Транспортный режим:	Туннельный режим:
1. [IP1] [AH] [верх.]	1. [IP2] [AH] [IP1] [верх.]
2. [IP1] [ESP] [верх.]	2. [IP2] [ESP] [IP1] [верх.]
3. [IP1] [AH] [ESP] [верх.]	

Шлюзам разрешается работать только в туннельном режиме (хотя они могли бы поддерживать и транспортный режим, но разработ-

чики стандарта решили, что он в этом случае малоэффективен). В соответствии со схемой, изображенной на рис. 17, б, шлюз принимает проходящий через него транзитом исходящий пакет и создает для него внешний IP-пакет. В этом пакете в качестве адреса источника шлюз указывает IP-адрес своего интерфейса, связывающего его с публичной сетью. В качестве адреса назначения внешнего пакета указывается IP-адрес принимающего шлюза. Затем шлюз помещает в поле данных внешнего пакета исходный пакет и выполняет необходимые действия в соответствии с протоколом AH или ESP. Другими словами, он либо вычисляет дайджест от данных внутреннего пакета, либо шифрует внутренний пакет (либо делает и то, и другое, если применяется протокол ESP, выполняющий одновременно функции аутентификации и шифрования).

Стандарты IPSec позволяют шлюзам использовать как одну ассоциацию SA для передачи трафика всех взаимодействующих через Internet хостов, так и создавать для этой цели произвольное число ассоциаций SA, например, по одной на каждое TCP-соединение.

Варианты относительного расположения заголовков пакетов в туннельном режиме "шлюз-шлюз" совпадают с двумя вариантами туннельного режима для режима "хост-хост". Сравнение разных режимов для протоколов AH и ESP представлено в табл.3.

Таблица 3. **Сравнение режимов для протоколов AH и ESP**

Протокол	Транспортный режим	Туннельный режим
AH	Идентифицирует протокол-пассажир IP, а также отдельные части заголовка IP и заголовков расширений IPv6.	Идентифицирует весь внутренний пакет IP (заголовок и протокол-пассажир внутреннего пакета IP), а также отдельные части внешнего заголовка IP и внешних заголовков расширений IPv6.
ESP	Шифрует протокол-пассажир IP и все заголовки расширений IPv6, следующие за заголовком ESP.	Шифрует внутренний пакет IP
ESP с аутентификацией	Шифрует протокол-пассажир IP и все заголовки расширений IPv6, следующие за заголовком ESP. Идентифицирует протокол-пассажир IP и заголовок IP.	Шифрует внутренний пакет IP. Идентифицирует внутренний пакет IP

Кроме описанных двух схем работы протокола IPSec, существует еще несколько схем, представляющих практический интерес. Например, при защищенном удаленном доступе применяется схема, в которой защищенный канал образуется между удаленным хостом H1* с установленным программным обеспечением IPSec, и шлюзом SG2*, защищающий трафик для хостов интрасети предприятия. Удаленный хост может использовать при отправке пакетов шлюзу как транспортный, так и туннельный режим. Шлюз же отправляет пакет хосту только в туннельном режиме. Эту схему можно усложнить, создав параллельно еще один защищенный канал — между хостом H1* и каким-либо хостом H2*, принадлежащим внутренней сети, защищаемой шлюзом SG2*. Такое комбинированное использование двух каналов SA позволяет надежно защитить трафик и во внутренней сети.

Как видно из описания, IPSec предлагает различные способы защиты трафика. Кто же решает, какой способ должна применить к трафику реализация IPSec, работающая в хосте или шлюзе? В стандартах IPSec разработан весьма гибкий способ, основанный на использовании в каждом узле, поддерживающем IPSec, базы данных политики безопасности — Security Policy Database, SPD.

База SPD создается и управляется либо пользователем (этот вариант больше подходит для хоста), либо системным администратором (вариант для шлюза), либо приложением. Записи базы SPD содержат два типа полей — поле селектора пакета и поле политики защиты пакета с данным значением селектора. Селектор имеет признаки, на основании которых можно с большой степенью детализации выделить тип трафика, который нужно защищать определенным образом. Политика зашиты трафика на верхнем уровне разветвляется на три варианта: каждый IP-пакет, выходящий из IPSec-узла, может быть либо обработан в соответствии с алгоритмами IPSec, либо отброшен, либо пропущен без обработки IPSec.

Если пакет должен быть защищен с помощью IPSec, то поле политики безопасности определяет набор параметров SA для данного пакета.

Селектор состоит из следующего набора признаков (некоторые из них являются опциональными):

- IP-адрес назначения (IPv4 или IPv6). Этот адрес может быть отдельным (любого типа — индивидуальным, групповым или широковещательным), или же представлять диапазон адресов, заданный с помощью верхней и нижней границы, или с помощью адреса и маски. При задании диапазона адресов подразумевается, что все узлы с адресами этого диапазона будут защищаться шлюзом с помощью одной ассоциации SA;
- IP-адрес источника. Свойства адреса те же, что и адреса назначения;
- имя пользователя в формате DNS (например, petr@math.mgu.ru) или X.500;
- имя системы (хоста, шлюза безопасности и т.п.) в формате DNS или X.500;
- тип протокола транспортного уровня (*TCP*, *UDP*);
- порты источника и назначения (т.е. порты TCP/UDP).

Каждый IPSec-узел должен поддерживать две базы SPD: одну для исходящего трафика, другую — для входящего, так как защита в разных направлениях может требоваться разная (что и отражено в однонаправленном характере SA). Для каждого поступающего пакета ПО IPSec должно просмотреть все записи базы SPD и в случае совпадения значения селектора с признаками пакета отработать заданную политику защиты.

Рассмотрим применение баз SPD на примере работы двух шлюзов безопасности (рис. 18). Пусть на вход шлюза SG1* поступает поток пакетов от различных хостов сети Net1. Протокол IPSec рассчитан на обработку трафика протокола IP, работающего без установления соединений, поэтому IPSec рассматривает каждый поступающий пакет независимо от предыдущих. При поступлении нового IP-пакета шлюз просматривает все записи в базе SDP для исходящего трафика и сравнивает значение селекторов этих записей с соответствующими полями IP-пакета. Если значение полей совпадает с каким-либо селектором, то над пакетом выполняются действия, определенные в поле политики безопасности данной записи.

Если в поле политики определено, что к пакету должна быть применена защита IPSec, то просматривается еще одно поле записи, о котором раньше не упоминалось — указатель на уже существую-

щую ассоциацию SA, которая соответствует набору параметров защиты, определенных в данной записи SPD. В рассматриваемом примере признаки поступившего в шлюз пакета совпали с селектором, указатель которого соответствует уже существующей ассоциации SA1.

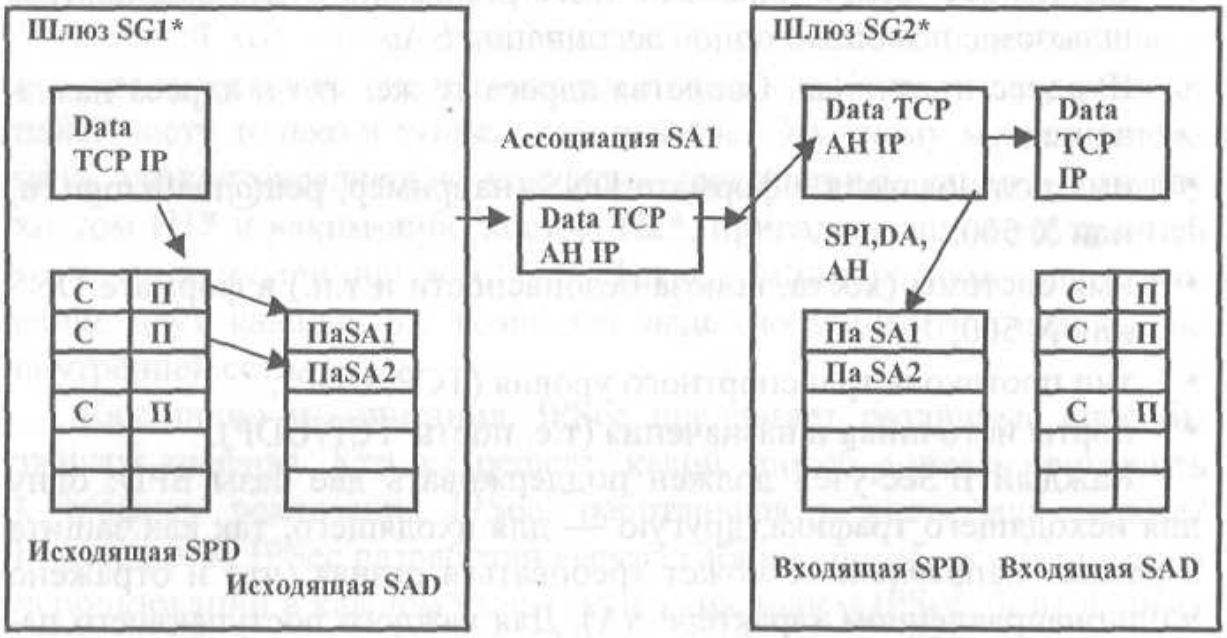


Рис. 18. Применение базы данных политики безопасности:
С – селектор, П – политика, Па — параметры

Для хранения данных о поддерживаемых в этот момент хостом или шлюзом ассоциациях существует база данных другого формата — база данных безопасных ассоциаций (Security Association Database, SAD). База SAD хранит текущие параметры каждой активной ассоциации — используемый протокол защиты AH или ESP, секретные ключи, значение текущего номера пакета в ассоциации и т.п. В процессе работы содержимое базы SPD остается неизменным длительное время (пока администратор не изменит политику защиты для какого-нибудь приложения или хоста), а содержимое базы SAD постоянно изменяется, соответствуя процессу обработки трафика протоколами AH или ESP.

Каждый IPSec-узел поддерживает две базы SAD — одну для исходящих ассоциаций, а другую — для входящих.

Если к исходящему пакету нужно применить некоторую политику защиты, но указатель записи SPD показывает, что в настоящее время нет активной SA с такой политикой, то IPSec действует следующим образом. Он создает новую ассоциацию с помощью протокола IKE, помещает ее параметры в базу SAD исходящих ассоциаций, а указатель на нее — в запись SDP исходящих ассоциаций. В том случае, когда указатель в SPD показывает, что нужная ассоциация существует, то пакет обрабатывается с помощью ее параметров — протокола AH или ESP, секретного ключа и т.п. В том случае, когда пакет нужно обработать с помощью и того и другого протокола, администратор должен завести в базе SPD две записи, соответствующие двум ассоциациям.

После конструирования и добавления заголовка AH или ESP (на рис. 17 — AH), шлюз SG1* конструирует также заголовок внешнего пакета IP, если задано в ассоциации, то выполняет шифрование внутреннего пакета, а затем отправляет внешний пакет шлюзу SG2*. Шлюз SG2* обрабатывает каждый входящий пакет с помощью базы SAD для входящих ассоциаций. Для распознавания принадлежности пакета определенной ассоциации используется специальная метка Security Parameters Index (SPI), помещаемая в заголовок AH или ESP. Эта метка представляет собой 32-разрядное число, которое должно быть уникально для всех ассоциаций определенного протокола защиты данных (т.е. AH или ESP), заканчивающихся в этом узле.

На основании тройки "протокол, адрес назначения, SPI" в базе SDP входящего трафика шлюза SG2* находится нужная ассоциация (в данном случае — SA1). Затем пакет подвергается обработке протоколом AH или ESP в соответствии с параметрами, хранящимися в записи SAD. Если соответствующая ассоциация отсутствует в SAD, то пакет отбрасывается. После извлечения и расшифрования внутреннего пакета приемный шлюз SG2* проверяет его признаки на предмет совпадения с селектором записи SPD для входящего трафика (чтобы убедиться, что проведенная обработка пакета соответствовала политике защиты, заданной администратором).

Использование баз SDP для управления процессом защиты трафика позволяет достаточно гибко сочетать механизм безопасных ассоциаций, работающий в режиме установления логического со-

единения, с дейтаграммным характером трафика протокола IP. Соответствующая настройка базы SDP позволяет выбирать нужную степень детализации защиты. Выбор достаточно широк — от применения одной ассоциации для трафика большого количества хостов до защиты каждого отдельного TCP или UDP порта (т.е. отдельного приложения отдельного хоста) с помощью индивидуально настроенной ассоциации.

Протокол AH. AH позволяет принимающей стороне убедиться в следующем:

- пакет был отправлен стороной, с которой установлена данная ассоциация;
- содержимое пакета не было искажено в процессе передачи его по сети;
- пакет не является дубликатом некоторого пакета, полученного ранее.

Две первые функции являются обязательными для протокола AH, а последняя — опциональной, выбираемой при установлении ассоциации. Для выполнения этих функций протокол AH использует заголовок, показанный на рис. 19. В поле Next Header (следующий заголовок) указывается тип протокола следующего уровня, как это принято в стеке TCP/IP. Скорее всего, это один из протоколов транспортного уровня TCP или UDP, или же протокол ICMP, но может встретиться и протокол ESP, если он используется в комбинации с AH. Поле Payload Len указывает длину заголовка AH в 32-битных словах. Поле SPI представляет собой 32-разрядную метку SA, на основании которой пакет должен быть правильно отнесен к одной из существующих ассоциаций в приемном шлюзе (или хосте). Если же активной ассоциации, на которую указывает метка SPI, не существует, то пакет просто отбрасывается.

0	8	16	31
Next Header	Payload Len	Зарезервировано	
Security Parameters Index (SPI)			
Sequence Number (SN)			
Authentication Data (переменная длина)			

Рис. 19. Структура заголовка протокола AH

Поле Sequence Number используется для защиты от ложного воспроизведения пакетов *(anti-replay service)*, когда третья сторона пытается повторно использовать перехваченные защищенные пакеты, отправленные аутентичным отправителем. Отправляющая пакеты сторона последовательно наращивает значение этого поля для каждого нового пакета, передаваемого в рамках данной ассоциации. Принимающая сторона заметит приход дубликата пакета только в том случае, если функция защиты от ложного воспроизведения была активирована в рамках ассоциации. Поле всегда заполняется отправителем новыми значениями. Однако получатель игнорирует это поле, если при установлении ассоциации не была выбрана функция защиты от ложного воспроизведения. Эта функция не занимается восстановлением утерянных пакетов и не упорядочивает прибывающие — она просто отбрасывает пакет в том случае, когда обнаруживает, что аналогичный уже был получен. Для сокращения требуемой для работы протокола буферной памяти используется механизм скользящего окна — на возможность дублирования проверяется только пакет, чей номер находится в пределах окна от наибольшего полученного на данный момент номера пакета. Окно обычно выбирается размером в 32 или 64 пакета.

Для аутентификации и проверки целостности пакета используется поле Authentication Data. В этом поле переносится контрольный код (Integrity Check Value, ICV), который вычисляется с помощью однонаправленной функции узлом-отправителем заголовка от содержимого пакета. Это значение, называемое также хэш-кодом, вычисляется с помощью одной из двух обязательно поддерживаемых протоколом AH функций MD5 или SHA-1. Оно может использоваться и любой опциональной функцией, о применении которой стороны договорились во время установления SA. Так как длина хэш-кода зависит от выбранной функции, то это поле имеет в общем случае переменный размер (наиболее часто используемая функция MD5 всегда порождает 16-байтный хэш-код). При вычислении хэш-кода в качестве аргумента однонаправленной функции используется общий секретный ключ, который был установлен вручную или протоколом IKE для данной ассоциации.

Протокол AH старается захватить при вычислении однонаправленной функции как можно большее число полей исходного IP-пакета. Но в транспортном режиме изменяемые в процессе передачи по сети поля включить в хэш-код принципиально невозможно, поэтому эти поля при его подсчете как узлом-отправителем, так и узлом-получателем считаются равными нулю.

Результирующий пакет в транспортном режиме может выглядеть, например, так, как показано на рис. 20.

Заголовок исходного IP-пакета (со всеми опциями)	Заголовок AH	Заголовок TCP	Данные
Аутентифицированная часть пакета (за исключением изменяющихся полей)			

Рис. 20. Результирующий пакет протокола AH в транспортном режиме

При использовании туннельного режима защищаются все поля исходного пакета, а также неизменяемые поля нового заголовка внешнего пакета (рис. 21).

Заголовок нового IP-пакета	Заголовок AH	Заголовок исходного IP-пакета	Заголовок TCP	Данные

Рис. 21. Результирующий пакет протокола AH в туннельном режиме

Протокол ESP. ESP использует для защиты данных заголовок следующего формата (рис. 22).

Протокол ESP поддерживает две группы функций: обеспечение целостности и конфиденциальности. Первую группу образуют те же функции, что и у протокола AH, а вторую — функция поддержания конфиденциальности данных и частичной конфиденциальности трафика. При установлении SA определяется конкретный набор функций, который будет применяться к пакетам. При этом должна быть выбрана хотя бы одна из групп функций защиты — иначе применение протокола ESP лишено смысла. В том случае, когда функции целостности не используются, поле контроля целостности (Authentication Data) также опускается.

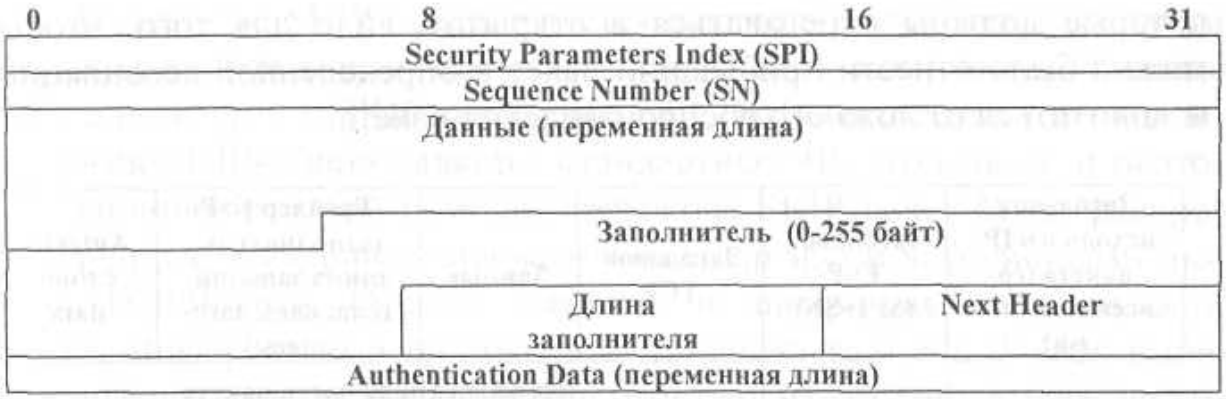


Рис. 22. Структура заголовка протокола ESP

Не все поля заголовка ESP располагаются перед данными протоколов верхних уровней, как это сделано у протокола AH. Перед полем данных помещаются только два поля: SPI и sequence Number, а остальные расположены позади данных. Непосредственно за полем данных размещается поле заполнителя (padding), а также поля длины заполнителя и указатель на протокол следующего уровня.

Заполнитель может понадобиться в трех случаях. Во-первых, для нормальной работы некоторых алгоритмов шифрования требуется, чтобы шифруемый текст содержал кратное число блоков определенного размера. Во-вторых, формат заголовка ESP требует, чтобы поле данных заканчивалось на границе 4-х байт. И, наконец, заполнитель можно использовать для некоторого искажения действительного размера пакета, что в стандартах IPSec названо частичной конфиденциальностью трафика. Правда, протокол ESP ограничивает возможности маскировки 255 байтами заполнителя. Это сделано для того, чтобы из-за большого объема избыточных данных не слишком уменьшалась полезная пропускная способность канала связи. В транспортном режиме заголовок ESP размещается после заголовка исходного IP-пакета, и его области защиты по двум группам функций показаны на рис. 23.

В отличие от протокола AH, контроль целостности и аутентичности данных в протоколе ESP не распространяется на заголовок исходного пакета и по этой причине имеет смысл применять совместно — протокол ESP для шифрования, а протокол AH для контроля целостности. В число шифруемых полей не попали поля SPI и SN,

которые должны передаваться в открытом виде для того, чтобы можно было отнести прибывший пакет к определенной ассоциации и защититься от ложного воспроизведения пакета.

Заголовок исходного IP-пакета (со всеми опциями)	Заголовок ESP (SPI+SN)	Заголовок TCP	Данные	Трейлер ESP (заполнитель, длина заполнителя, след. заголовок)	Autenti-cation data
	Зашифрованная часть пакета				
	Аутентифицированная часть пакета				

Рис. 23. Результирующий пакет ESP в транспортном режиме

В туннельном режиме схема защиты выглядит почти так же, с той разницей, что заголовок исходного IP-пакета помещается после заголовка ESP и полностью попадает в число защищаемых полей, а заголовок внешнего IP-пакета протоколом ESP не защищается (рис. 24).

Заголовок нового внешнего IP-пакета (со всеми опциями)	Заголовок ESP (SPI+SN)	Заголовок исходного IP-пакета (со всеми опциями)	Заголовок TCP	Данные	Трейлер ESP (заполнитель, длина заполнителя, след. заголовок)	Autenti-cation data

Рис. 24. Структура результирующего пакета протокола ESP в туннельном режиме

При совместном использовании протоколов AH и ESP заголовок AH предшествует заголовку ESP.

Для протокола ESP также определен перечень обязательных алгоритмов шифрования — это DES, MD5 и SHA-1.

Протокол SKIP. *Одной из технологий, предлагающей необходимые для применения в масштабах Internet универсальность и общность, является спецификация SKIP (Simple Key management for Internet Protocol – простое управления ключами для IP-протокола), разработанная компанией Sun в 1994 г.*

Почему же SKIP представляется решением, адекватным задачам защиты информации в масштабах такой сети, как Internet? Прежде всего потому, что SKIP совместим с IP. Это достигается тем, что заголовок SKIP-пакета является стандартным IP-заголовком, и поэтому защищенный при помощи протокола SKIP пакет будет распространяться и маршрутизироваться стандартными устройствами любой TCP/IP-сети. Отсюда вытекает и аппаратная независимость SKIP. Информация о протоколе SKIP записывается в IP-стек выше аппаратно-зависимой его части и работает на тех же каналах, на которых работает IP.

Принадлежность SKIP к IP-стеку обеспечивает универсальность и прозрачность этого протокола для приложений: SKIP шифрует IP-пакеты, ничего не зная о приложениях, пользователях или процессах, их формирующих; он обрабатывает весь трафик, не накладывая никаких ограничений на вышележащее программное обеспечение. В свою очередь, приложения никак не "чувствуют" SKIP.

SKIP сеансонезависим: для организации защищенного взаимодействия между парой абонентов не требуется никакого дополнительного информационного обмена и передачи по каналам связи какой-либо открытой информации.

Еще одной чертой SKIP является его независимость от системы шифрования. Пользователь может выбирать любой по конфигурации из предлагаемых поставщиком криптоалгоритмов или использовать свой алгоритм шифрования; могут использоваться различные по своей криптостойкости алгоритмы шифрования – различные системы шифрования могут подсоединяться к системе как внешние библиотечные модули.

В основе SKIP лежит криптографический протокол обмена ключами Диффи–Хеллмана. Система открытых ключей Диффи–Хеллмана представляет собой криптографическую систему с асимметричными ключами, в которой используются различные ключи для шифрования и расшифрования. Каждый узел сети снабжается секретным и открытым ключами. Открытые ключи могут свободно распространяться среди пользователей, заинтересованных в организации защищенного обмена информацией (рис. 25). Узел *i*, адресующий свой трафик к узлу *j*, на основе логики открытых ключей

вычисляет парный ключ *Kij*. Однако этот, требующий высокой степени защиты, разделяемый секрет не используется прямо для шифрования данных. Для шифрования конкретного пакета или их небольшой группы узел *i* вырабатывает специальный пакетный (сеансовый) ключ *Kp*, зашифровывает при помощи этого ключа данные, укладывает их в блок данных SKIP-пакета. Далее, собственно пакетный ключ *Kp* шифруется на основе другого ключа, вырабатываемого из общего секретного ключа *Kij*, и тоже записывается в пакет. Пакет снабжается SKIP-заголовком, по синтаксису совпадающим с заголовком IP-пакета, и отправляется в сеть. Поскольку SKIP-заголовок совпадает с заголовком IP-пакета, все промежуточное оборудование сети стандартным образом маршрутизирует этот пакет до его доставки узлу-получателю *j*. Узел *j*, получив пакет и вычислив разделяемый секрет *Kij*, расшифровывает ключ *Kp* и с его помощью расшифровывает весь пакет.

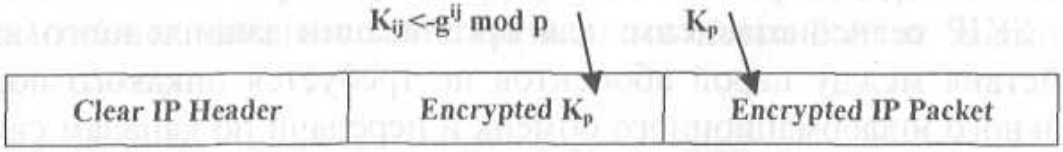


Рис. 25. Зашифрованный широковещательный SKIP-пакет

Описанный выше процесс называется инкапсуляцией, или туннелированием. Инкапсуляция обеспечивает шифрование (путем инкапсуляции пакетов, подлежащих защите, в SKIP-пакеты) и аутентификацию информации. Режимы инкапсуляции и шифрования могут применяться как совместно, так и раздельно. Структура пакета, получающегося в результате такой инкапсуляции, приведена на рис. 26.

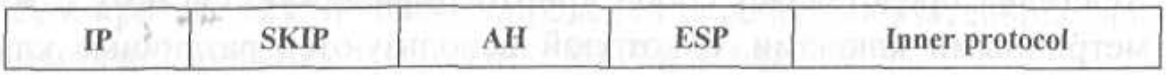


Рис. 26. Структура SKIP-пакета:
IP и SKIP – заголовки протоколов IP и SKIP;
AH – аутентификационный заголовок;
ESP – заголовок, включающий данные об инкапсулированном протоколе;
Inner protocol – пакет инкапсулируемого протокола.

Если применяется только режим аутентификации или инкапсуляции, то заголовки AH и ESP, ответственные за аутентификацию и инкапсуляцию, могут изыматься из пакета.

В первой версии SKIP для повышения криптостойкости вычисляемого парного ключа предлагалась следующая логика. При шифровании данных каждого пакета или их группы вырабатывался случайный пакетный или сеансовый ключ, *Kp*. Затем ключ *Kp* шифровался при помощи вычисляемого парного ключа – долговременного разделяемого секрета *Kij*. Такое решение обеспечивало два преимущества:

- в случае компрометации пакетного ключа риску подвергается только относительно малая часть трафика, зашифрованная при помощи этого ключа;
- обеспечивалась дополнительная защита разделяемого секрета, поскольку он использовался для шифрования относительно малой части передаваемого трафика, и накопить статистику, необходимую для проведения криптоатаки на этот ключ, представлялось затруднительным.

В последующих реализациях спецификации SKIP были приняты дополнительные меры для защиты разделяемого секрета. Повышение криптостойкости протокола при атаках на пакетный ключ *Kp* достигнуто за счет включения в заголовок пакета нового параметра (*n*), который используется для вычисления ключа (*Kijn*), применяемого при шифровании сеансового ключа. Основная идея заключается в том, что для получения ключа *Kp* используется не сам разделяемый секрет *Kij*, а результат применения хэш-функции к выражению, составленному из разделяемого ключа *Kij* и параметра *n*. При этом *n* никогда не уменьшается, а только увеличивается. Правила для работы с *n* отнесены на усмотрение разработчика, однако для обеспечения совместимости версий предлагается считать, что *n* – это время в часах, отсчитанное от 00 час. 00 мин. 01.01.95.

Проблема синхронизации часов на защищаемых системах решается достаточно просто – если параметр *n* отличается более, чем на единицу, что составляет расхождение во времени свыше одного часа, то пакет выбрасывается, поскольку потенциально может быть инструментом для выполнения атаки методом повтора протокола.

Далее наиболее существенной из эволюций спецификации SKIP является приведение протокола SKIP к единообразному виду с точки зрения архитектуры протоколов семейства IP. Это выразилось, в первую очередь, в некотором упорядочении инкапсуляции протоколов, выполненной в соответствии со стандартом RFC 1827.

В заголовке SKIP-пакета появилось поле NEXT HEADER, которое указывает протокол, содержащийся внутри данного SKIP-пакета. Таким образом достигается привычная картина последовательной инкапсуляции пакетов один в другой.

Аналогично привычной цепочке Ethernet packet -> IP packet -> TCP packet при работе по протоколу SKIP получаем IP packet -> SKIP packet -> ESP packet -> TCP packet. Еще один результат появления в заголовке информации о следующем протоколе заключается в том, что теперь протокол SKIP отвечает только за передачу сеансового ключа и номера алгоритма для использования внутри инкапсулируемого протокола ESP. В качестве протокола ESP может применяться любой протокол. SKIP не накладывает никаких ограничений на конкретную реализацию ESP.

Формат заголовков при использовании AH в SKIP представлен на рис. 27.

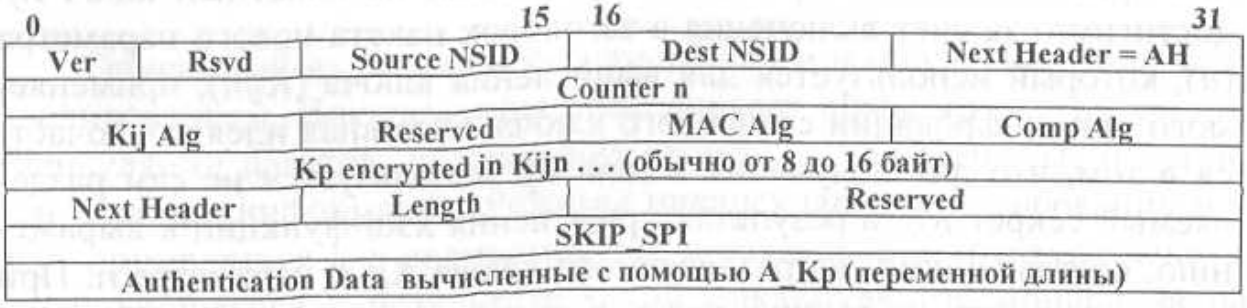


Рис. 27. Формат заголовков при использовании AH в SKIP

Более подробную информацию о технологии SKIP можно найти по следующим адресам: Web-сервер Internet Commerce Group – подразделения Sun Microsystems, занимающегося разработкой спецификации SKIP и SKIP-продуктов http://www.incog.com, http://skip.incog.com; WWW-сервер АО ЭЛВИС+ http://www.elvis.ru; FTP-сервер Swiss Federal Institute of Technology;

ftp://www.tik.ee.ethz.ch/pub/packages/skip; Web-сервер Internet Security Group IETF; http://www.ietf.cnri.reston.va.us.

2.4. Защита на сеансовом уровне

Наиболее известным протоколом защищенного канала, работающим на сеансовом уровне модели OSI, является протокол Secure Socket Layer (SSL), разработанный компанией Netscape Communications. Протокол SSL прошел проверку временем, работая в популярных браузерах Netscape Navigator и Internet Explorer, а также Web-серверах всех ведущих производителей. В январе 1999 г. на смену версии SSL 3.0 пришел протокол Transport Layer Security (TLS), который является стандартом Internet. TLS базируется на SSL, и различия между SSL 3.0 и TLS 1.0 не слишком существенны (хотя и достаточны для того, чтобы эти протоколы не были совместимыми). Основные свойства протокола SSL, описанные ниже, применимы и к TLS.

Протокол SSL. Протокол SSL спроектирован для обеспечения конфиденциальности обмена между двумя прикладными процессами клиента и сервера (http://www.netscape.com/eng/security/SSL_3.html). Он предоставляет возможность аутентификации сервера и, опционально, клиента. SSL требует применения надежного транспортного протокола (например, TCP).

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и т.д., могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и сеансовый ключ, а также аутентифицировать сервер до того, как приложение примет или передаст первый байт данных. Все протокольные прикладные данные передаются зашифрованными с гарантией конфиденциальности.

Несмотря на то, что протокол SSL может использоваться для создания защищенного канала между любыми приложениями, наиболее широко он используется протоколом HTTP (режим HTTPS). Когда используются SSL-совместимые браузеры (например, Internet Explorer или Netscape Navigator) и SSL-совместимые Web-серверы,

то вся передаваемая между браузером и сервером информация (например, номера кредитных карточек) недоступна злоумышленнику. При вызове защищенной страницы пользователь не видит процесс организации защищенного канала. Браузер вызывает сервер, а тот посылает свой общедоступный сертификат, и если он был выдан организацией, признаваемой браузером, то транзакция осуществляется.

Протокол SSL выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, передачу данных в зашифрованном виде и обеспечение целостности и аутентичности данных.

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена сертификатами при установлении SSL-сессии. SSL поддерживает сертификаты различных сертифицирующих организаций, основанные на стандарте X.509, а также стандарты ИОК, с помощью которой организуется выдача и проверка подлинности сертификатов.

Секретность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сеансовых ключей, которыми стороны обмениваются при установлении соединения. Сеансовые ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов зашифрования и расшифрования на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей.

Целостность передаваемых сообщений достигается за счет того, что к сообщению (еще до его зашифрования сеансовым ключом) добавляется хэш-код, полученный в результате применения однонаправленной функции к тексту сообщения.

Протокол SSL предоставляет защищенный канал, который имеет три основные свойства.

- Канал является частным. Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа.

- Канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, в то время как клиентская аутентифицируется опционально.
- Канал надежен. Транспортировка сообщений включает в себя проверку целостности (с привлечением MAC — Message Authentication Code) .

В SSL все данные пересылаются в виде записей — объектов, которые состоят из заголовка и некоторого количества данных. Каждый заголовок записи содержит два или три байта кода длины. Если старший бит в первом байте кода длины записи равен 1, тогда запись не имеет заполнителя и полная длина заголовка равна 2 байтам, в противном случае запись содержит заполнитель и полная длина заголовка равна 3 байтам. Передача всегда начинается с заголовка.

Заметим, что в случае длинного заголовка (3 байта), второй по старшинству бит первого байта имеет специальное значение. Когда он равен нулю, посылаемая запись является информационной. При равенстве 1, посылаемая запись является *security escape* (в настоящее время не определено ни одного значения *security escapes*; это зарезервировано для будущих версий протокола).

Код длины записи не включает в себя число байтов заголовка (2 или 3). Для 2-байтового заголовка его длина вычисляется следующим образом (используется Си-подобная нотация):

RECORLENGTH = ((byte[0] & 0x7F << 8)) | byte[1];

где byte[0] представляет собой первый полученный байт, а byte[1] – второй полученный байт. Когда используется 3-байтовый заголовок, длина записи вычисляется следующим образом:

RECORD-LENGTH = ((byte[0] & 0x3F) << 8)) | byte[1];

IS-ESCAPE = (byte[0] & 0x40) != 0;

PADDING = byte[2];

Заголовок записи определяет значение, называемое PADDING (*перевод с англ.* — "заполнитель"). Значение PADDING специфицирует число байтов, добавленных отправителем к исходной записи. Данные заполнителя используются для того, чтобы сделать длину записи кратной размеру блока шифра, если применен блочный шифр.

Отправитель "заполненной" записи добавляет заполнитель после имеющихся данных, а затем шифрует все это, благо длина этого массива кратна размеру блока используемого шифра. Содержимое заполнителя не играет роли. Так как объем передаваемых данных известен, заголовок сообщения может быть корректно сформирован с учетом объема субполя PADDING.

Получатель этой записи расшифровывает все поле данных и получает исходную информацию. После этого производится вычисление истинного значения RECORD-LENGTH (с учетом наличия опционального PADDING), при этом заполнитель из поля *данные* удаляется.

Часть данных записи протокола SSL состоит из трех компонентов (передаваемых и получаемых в приведенном ниже порядке):

MAC-DATA[MAC-SIZE]

ACTUAL-DATA[N]

PADDING-DATA[PADDING]

ACTUAL-DATA представляет собой реальные переданные данные (поле данных сообщения). PADDING-DATA – это данные заполнителя, посылаемые, когда используется блочный код шифрования. MAC-DATA является кодом аутентификации сообщения.

Когда записи SSL посылаются открытым текстом, никаких шифров не используется. Следовательно, длина PADDING-DATA будет равна нулю и объем MAC-DATA также будет нулевым. Когда используется шифрование, PADDING-DATA является функцией размера блока шифра. MAC-DATA зависит от CIPHER-CHOICE. MAC-DATA вычисляется следующим образом:

MAC-DATA = HASH [SECRET, ACTUAL-DATA, PADDING-DATA, SEQUENCE-NUMBER],

где SECRET передается хэш-функции первым, далее следует ACTUAL-DATA и PADDING-DATA, за которыми передается SEQUENCE-NUMBER. Порядковый номер (SEQUENCE-NUMBER) представляет собой 32-битовый код, который передается хэш-функции в виде 4 байт. Первым передается старший байт (т.е. используется сетевой порядок передачи — big endian).

MAC-SIZE является функцией используемого алгоритма вычисления хэш-кода. Для MD2 и MD5 MAC-SIZE равен 16 байтам (128 битам).

Значение SECRET зависит от того, кто из партнеров посылает сообщение. Если сообщение посылается клиентом, тогда SECRET равен CLIENT-WRITE-KEY (сервер будет использовать SERVER-READ-KEY для проверки MAC). Если клиент получает сообщение, SECRET равен CLIENT-READ-KEY (сервер будет использовать SERVER-WRITE-KEY для генерации MAC).

SEQUENCE-NUMBER является счетчиком, который инкрементируется как сервером, так и получателем. Для каждого направления передачи используется пара счетчиков: один для отправителя, другой для получателя. При отправлении сообщения счетчик инкрементируется. Порядковыми номерами являются 32-битовые целые числа без знака, которые при переполнении обнуляются.

Получатель сообщения использует ожидаемое значение порядкового номера для передачи хэш-функции MAC (тип хэш-функции определяется параметром CIPHER-CHOICE). Вычисленная MAC-DATA должна совпадать с переданной MAC-DATA. Если сравнение не прошло, запись считается поврежденной, такая ситуация рассматривается как случай I/O Error (т.е. как непоправимая ошибка, которая вызывает закрытие соединения).

Окончательная проверка соответствия выполняется, когда используется блочный шифр и соответствующий протокол шифрования. Объем данных в записи (RECORD-LENGTH) должен быть кратным размеру блока шифра. Если полученная запись не кратна размеру блока шифра, запись считается поврежденной, при этом считается, что имела место I/O Error (что вызовет разрыв соединения).

Уровень записей SSL используется для всех коммуникаций SSL, включая сообщения диалога и информационный обмен. Уровень записей SSL применяется как клиентом, так и сервером.

Для двухбайтового заголовка, максимальная длина записи равна 32767 байтов. Для трехбайтового заголовка, максимальная длина записи равна 16383 байтов. Сообщения протокола диалога SSL должны соответствовать одиночным записям протокола SSL (Record

Protocol). Сообщения прикладного протокола могут занимать несколько записей SSL.

Прежде чем послать первую запись SSL, все порядковые номера делаются равными нулю. При передаче сообщения порядковый номер инкрементируется, начиная с сообщений CLIENT-HELLO и SERVER-HELLO.

Протокол диалога SSL имеет две основные фазы. Первая фаза используется для установления конфиденциального канала коммуникаций. Вторая — служит для аутентификации клиента (рис. 28).

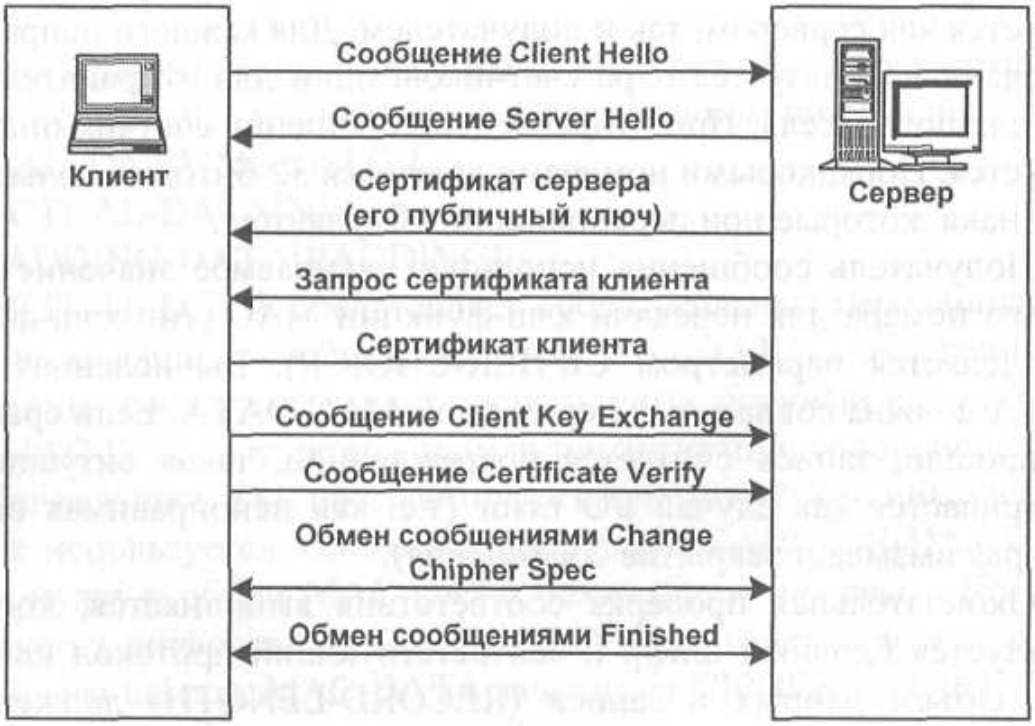


Рис. 28. Протокол диалога SSL

Первая фаза является фазой инициализации соединения, когда оба партнера посылают сообщения hello. Клиент инициирует диалог посылкой сообщения CLIENT-HELLO. Сервер получает сообщение CLIENT-HELLO, обрабатывает его и откликается сообщением SERVER-HELLO. К этому моменту как клиент, так и сервер имеют достаточно информации, чтобы знать, нужен ли новый мастер-ключ. Когда новый мастер-ключ не нужен, клиент и сервер немедленно переходят в фазу 2. Когда нужен новый мастер-ключ, сообщение

SERVER-HELLO будет содержать достаточно данных, чтобы клиент мог сформировать такой ключ. Сюда входит подписанный сертификат сервера, список базовых шифров и идентификатор соединения (представляет собой случайное число, сформированное сервером и используемое на протяжении сессии). Клиент генерирует мастер-ключ и посылает сообщение CLIENT-MASTER-KEY (или сообщение ERROR, если информация сервера указывает, что клиент и сервер не могут согласовать базовый шифр).

Здесь следует заметить, что каждая оконечная точка SSL использует пару шифров для каждого соединения (т.е. всего 4 шифра). На каждой конечной точке один шифр используется для исходящих коммуникаций и один — для входящих. Когда клиент или сервер генерирует ключ сессии, они в действительности формируют два ключа: SERVER-READ-KEY (известный так же, как CLIENT-WRITE-KEY) и SERVER-WRITE-KEY (известный так же, как CLIENT-READ-KEY). Мастер-ключ используется клиентом и сервером для генерации различных ключей сессий.

Наконец, после того как мастер-ключ определен, сервер посылает клиенту сообщение SERVER-VERIFY. Этот заключительный шаг аутентифицирует сервер, так как только сервер, который имеет соответствующий общедоступный ключ, может знать мастер-ключ.

Вторая фаза является фазой аутентификации. Сервер уже аутентифицирован клиентом на первой фазе, по этой причине здесь осуществляется аутентификация клиента. При типичном сценарии серверу необходимо получить что-то от клиента, и он посылает запрос. Клиент пришлет позитивный отклик, если располагает необходимой информацией, или пришлет сообщение об ошибке в противном случае. Эта спецификация протокола не определяет семантику сообщения ERROR, посылаемого в ответ на запрос сервера (например, конкретная реализация может игнорировать ошибку, закрыть соединение, и т.д. и, тем не менее, соответствовать данной спецификации). Когда один партнер выполнил аутентификацию другого партнера, он посылает сообщение finished. В случае клиента сообщение CLIENT-FINISHED содержит зашифрованную форму идентификатора CONNECTION-ID, которую должен верифицировать сервер.

Если верификация терпит неудачу, сервер посылает сообщение ERROR.

Раз партнер послал сообщение finished, он должен продолжить воспринимать сообщения до тех пор, пока не получит сообщение finished от партнера. Как только оба партнера послали и получили сообщения finished, протокол диалога SSL закончил свою работу. С этого момента начинает работать прикладной протокол.

Протокол TLS. Целью протокола TLS (Transport Layer Security) является обеспечение конфиденциальности и целостности данных при связи двух приложений.

TLS состоит из двух основных протоколов:

- TLS Handshake Protocol (протокол установления соединения, или протокол диалога) — выполняет двустороннюю аутентификацию и обмен ключевой информацией; предназначен для создания защищенной сессии;
- TLS Record Protocol (протокол записи) — обеспечивает шифрование и контроль целостности передаваемых данных.

На нижнем уровне, работающем поверх транспортного протокола (например, TCP), размещается протокол записей TLS. Этот протокол обеспечивает безопасность соединений, которые имеют два основных свойства.

- Соединение является конфиденциальным. Для шифрования данных используется симметричная криптография (например, DES, RC4 и т.д.). Ключи для шифрования генерируются независимо для каждого соединения и базируются на секретном коде, получаемом с помощью другого протокола (такого, как протокол диалога TLS). Протокол записей может использоваться и без шифрования.
- Соединение является надежным. Процедура передачи сообщения включает в себя проверку целостности с помощью вычисления MAC. Для расчета MAC используются хэш-функции (например, SHA, MD5 и т.д.). Протокол записей может работать и без MAC, но в этом режиме он применяется только в случае, когда другой протокол использует протокол записей в качестве транспортного при выяснении параметров безопасности.

Протокол записей TLS является послойным. На каждом уровне, сообщения могут включать поля длины, описания и содержимого. Протокол записей берет сообщения, подлежащие пересылке, разбивает их на блоки, опционально сжимает данные, применяет MAC, шифрует и передает результат. Полученные данные расшифровываются, верифицируются, декомпрессируются, восстанавливается их первоначальный вид, результат передается клиентам верхнего уровня.

Протокол записей TLS используется для инкапсуляции различных протоколов высокого уровня. Один из таких инкапсулируемых объектов, протокол диалога TLS, позволяет серверу и клиенту аутентифицировать друг друга и согласовать алгоритм шифрования и криптоключи до того, как приложение передаст или примет первый байт информации. Протокол диалога TLS обеспечивает безопасное соединение, которое имеет три базовых свойства.

- Идентичность партнеров может быть выяснена с использованием асимметричной криптографии (например, RSA, DSS и т.д.). Эта аутентификация может быть сделана опциональной, но она необходима, по крайней мере, для одного из партнеров.
- Выявление общего секретного кода является безопасным: этот секретный код недоступен злоумышленнику, даже если он ухитрится подключиться к соединению.
- Диалог надежен: атакующий не может модифицировать обсуждаемое соединение без того, чтобы быть обнаруженным партнерами обмена.

Любой протокол, предназначенный для использования поверх TLS, должен быть тщательно сконфигурирован, для того чтобы противостоять любым атакам. Заметим, из-за того, что тип и длина записи не защищены шифрованием, следует принимать меры, чтобы минимизировать трафик анализа этих величин.

Протокол диалога TLS содержит набор из трех субпротоколов (*протокол уведомления, протокол спецификации изменения шифра и прикладной информационный протокол*), которые используются, чтобы партнеры могли согласовать используемые параметры безопасности для уровня записи, аутентифицировать себя и уведомлять друг друга об ошибках.

Протокол диалога ответственен за согласования характеристик сессии, куда входят следующие объекты.

- Идентификатор сессии – произвольная последовательность байтов, выбранная сервером для идентификации состояния сессии (активная/ возобновляемая).
- Сертификат партнера – X509v3 сертификат партнера. Этот элемент состояния может быть равен нулю.
- Метод сжатия – алгоритм, используемый для сжатия информации перед шифрованием.
- Спецификация шифра – специфицирует алгоритм шифрования (такой, как DES, и т.д.) и алгоритм MAC (такой, как MD5 или SHA). Она определяет также криптографические атрибуты, такие, как hash_size.
- Секретный мастер-код — 48-байтовый секретный код, общий для сервера и клиента.
- "is resumable" – флаг, указывающий, может ли сессия использоваться для инициализации нового соединения.

Эти объекты используются затем для определения параметров безопасности для уровня записей при защите прикладных данных. Многие соединения могут реализоваться в рамках той же сессии с помощью процедуры возобновления (resumption) протокола диалога.

Одним из преимуществ TLS является то, что он не зависит от протокола приложения. Протоколы верхнего уровня могут размещаться поверх протокола TLS прозрачным образом. Стандарт TLS, однако, не специфицирует то, как протоколы увеличивают безопасность с помощью TLS. Решение о том, как инициализировать TLS-диалог и как интерпретировать сертификаты аутентификации, оставляется на усмотрение разработчиков протоколов и программ, которые работают поверх TLS.

Перечислим цели протокола TLS в порядке их приоритетности.

1. *Криптографическая безопасность*. TLS должен использоваться для установления безопасного соединения между двумя партнерами.
2. *Совместимость*. Независимые программисты должны быть способны разрабатывать приложения, использующие TLS, которые

будут способны успешно обмениваться криптографическими параметрами без знания особенностей программ друг друга.

3. *Расширяемость.* TLS ищет способ, как при необходимости встроить в систему новые ключи и методы шифрования. Здесь имеются две побочные цели: исключить необходимость создания нового протокола (что может быть сопряжено с введением новых слабых мест) и сделать ненужным внедрение новой библиотеки, обеспечивающей безопасность.
4. *Относительная эффективность.* Криптографические операции требуют больших вычислительных мощностей, особенно этим славятся операции с открытыми ключами. По этой причине TLS имеет опциональную схему хэширования сессии, что позволяет уменьшить число соединений, устанавливаемых с использованием новых временных буферов. Были приняты меры, чтобы уменьшить сетевую активность.

К недостаткам протоколов SSL и TLS можно отнести то, что для транспортировки своих сообщений они используют только один протокол сетевого уровня — IP, и, следовательно, могут работать лишь в IP-сетях. Кроме того, применение на практике защитных свойств SSL/TLS не в полной мере прозрачно для прикладных протоколов, так как для инициации защищенного канала они должны использовать явные вызовы типа STARTSSL.

Протокол SOCKS. Разработан в 1990 г. Дэвидом Кобласом для организации посредничества при взаимодействии между клиент-серверными приложениями на сеансовом уровне модели OSI [3]. Изначально данный протокол разрабатывался только для перенаправления запросов к серверам со стороны клиентских приложений, а также возврата этим приложениям полученных ответов. Однако даже лишь перенаправление запросов и ответов между клиент-серверными приложениями уже позволяет реализовать функцию трансляции сетевых IP-адресов (Network Address Translation — NAT). При замене для исходящих пакетов внутренних IP-адресов отправителей одним IP-адресом шлюза топология внутренней сети скрыта от внешних пользователей, что усложняет НСД. Трансляция сетевых адресов, помимо повышения безопасности, позволяет расширить внутреннее адресное пространство сети за счет возможно-

сти поддержки собственной системы адресации, не согласованной с адресацией во внешней сети.

На основе протокола SOCKS могут быть реализованы и любые другие функции посредничества по защите сетевого взаимодействия. Например, SOCKS может применяться для контроля над направлениями информационных потоков и разграничения доступа в зависимости от атрибутов пользователей и/или информации. Эффективность использования данного протокола для выполнения функций посредничества обеспечивается его ориентацией на сеансовый уровень модели OSI. По сравнению с посредниками прикладного уровня на сеансовом уровне достигаются более высокое быстродействие и независимость от высокоуровневых протоколов (HTTP, FTP, POP3, SMTP, NNTP и др.). Кроме того, протокол SOCKS не привязан к протоколу IP, а также не зависит от ОС. Например, для обмена информацией между клиентским приложением и посредником может использоваться протокол IPX.

VPN и МЭ благодаря протоколу SOCKS могут организовать безопасное взаимодействие и обмен информацией между разными сетями. Кроме того, SOCKS позволяет реализовать безопасное управление этими системами на основе унифицированной стратегии. Следует отметить, что если на основе протоколов канального и сетевого уровня защищенные виртуальные каналы формируются между разными парами взаимодействующих сторон, то на основе протокола SOCKS могут создаваться защищенные туннели для каждого приложения и сеанса в отдельности.

В соответствии с протоколом SOCKS различают SOCKS-сервер, который целесообразно устанавливать на шлюз (МЭ) сети, а также SOCKS-клиент, который устанавливается на каждый пользовательский компьютер. SOCKS-сервер обеспечивает взаимодействие с любым прикладным сервером от имени соответствующего этому серверу прикладного клиента. Для перехвата всех запросов к прикладному серверу со стороны клиента и передачи их SOCKS-серверу предназначен SOCKS-клиент. Поскольку SOCKS-серверу известно о трафике на уровне сеанса (сокета), он может осуществлять тщательный контроль, например, блокировать работу конкрет-

ных приложений пользователей, если они не имеют необходимых полномочий на информационный обмен.

С момента разработки широкое распространение получили 4 и 5 версии (v4 и v5) этого протокола. SOCKS v5 в настоящее время одобрен организацией IETF (Internet Engineering Task Force) в качестве стандарта Internet и включен в RFC 1928.

Обобщенная схема взаимодействия по протоколу SOCKS v4 сводится к следующему.

1. Запрос прикладного клиента, желающего установить соединение с каким-либо прикладным сервером в сети, перехватывает SOCKS-клиент, установленный на этом же компьютере.
2. SOCKS-клиент соединяется с SOCKS-сервером и передает ему запрос прикладного клиента.
3. SOCKS-сервер соединяется с запрошенным прикладным сервером.
4. Прикладной клиент и прикладной сервер взаимодействуют друг с другом по цепочке соединений, в которой SOCKS-сервер просто ретранслирует данные.

В реализации SOCKS-сервера v4, кроме трансляции IP-адресов, могут быть предусмотрены другие функции посредничества по защите сетевого взаимодействия. Однако в протоколе SOCKS v4 такие функции не специфицируются.

Протокол SOCKS v5 является значительным развитием четвертой версии, реализуя следующие дополнительные возможности [3].

1. SOCKS-клиент может передавать SOCKS-серверу не только IP-адрес компьютера, с которым необходимо установить соединение, но и его DNS-имя. SOCKS-сервер сам получит IP-адрес по DNS-имени. Таким образом, в ЛВС, использующих SOCKS v5, можно обойтись без локального DNS-сервера, наличия которого требовал протокол SOCKS v4.
2. В SOCKS v5 поддерживается не только протокол TCP, но и UDP. Вместе эти протоколы покрывают почти все множество используемых прикладных протоколов. Из широко используемых программ только диагностические утилиты PING и TRACERT пользуются протоколом ICMP и не могут работать через TCP и UDP.

3. Предусмотрена аутентификация пользователей, от имени которых обращаются SOCKS-клиенты. SOCKS-сервер может согласовывать с SOCKS-клиентом способ аутентификации. Аутентификация делает возможным разграничение доступа к компьютерным ресурсам. Допускается также двухсторонняя аутентификация, т.е. пользователь может, в свою очередь, убедиться, что соединился с нужным SOCKS-сервером
4. SOCKS v5 допускает использование не только текущих схем адресации в соответствии с протоколом IPv4, но и будущих, предусмотренных в IPv6.

Обобщенная схема установления соединения по протоколу SOCKS v5 выглядит следующим образом [3].

1. Запрос прикладного клиента, желающего установить соединение с каким-либо прикладным сервером в сети, перехватывает установленный на этом же компьютере SOCKS-клиент.
2. SOCKS-клиент соединяется с SOCKS-сервером и сообщает ему идентификаторы всех методов аутентификации, которые он поддерживает.
3. SOCKS-сервер решает, каким методом аутентификации воспользоваться; если же SOCKS-сервер не поддерживает ни один из методов аутентификации, предложенных пользователем, соединение разрывается.
4. При поддержке каких-либо предложенных методов аутентификации SOCKS-сервер в соответствии с выбранным методом аутентифицирует пользователя, от имени которого выступает SOCKS-клиент; в случае безуспешной аутентификации SOCKS-сервер разрывает соединение.
5. После успешной аутентификации SOCKS-клиент передает SOCKS-серверу DNS-имя или IP-адрес запрашиваемого прикладного сервера в сети и далее SOCKS-сервер на основе имеющихся правил разграничения доступа принимает решение об установлении соединения с этим прикладным сервером.
6. В случае установления соединения прикладной клиент и прикладной сервер взаимодействуют друг с другом по цепочке соединений, в которой SOCKS-сервер ретранслирует данные, а также может выполнять функции посредничества по защите

сетевого взаимодействия; например, если в ходе аутентификации SOCKS-клиент и SOCKS-сервер обменялись сеансовым ключом, то весь трафик между ними может шифроваться.

Аутентификация пользователя, выполняемая SOCKS-сервером, может основываться на сертификатах открытых ключей формата X.509 или паролях. Для шифрования трафика между SOCKS-клиентом и SOCKS-сервером могут использоваться любые протоколы, ориентированные на сеансовый и более низкие уровни модели OSI. Максимальную функциональность по криптозащите обеспечит протокол SSL. Помимо аутентификации пользователей, трансляции IP-адресов и криптозащиты трафика SOCKS-сервер может выполнять также такие функции, как:

- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрация потока сообщений, например, динамический поиск вирусов;
- регистрация событий и реагирование на задаваемые события;
- хэширование данных, запрашиваемых из внешней сети.

SOCKS-клиенты, выполняющие перехват запросов клиентских приложений и взаимодействие с SOCKS-сервером, могут быть изначально встроены в универсальные клиентские программы. К приложениям, имеющим встроенную поддержку протокола SOCKS, относятся популярные Web-навигаторы Netscape Navigator (Communicator) и Microsoft Internet Explorer. Существуют также специальные программы, называемые соксификаторами, дополняющие клиентские приложения поддержкой протокола SOCKS. Например, к таким программам относятся NEC SocksCap, а также Hummingbird SOCKS Client. При установке соксификатор внедряется между пользовательскими приложениями и стеком коммуникационных протоколов. Далее в процессе работы он перехватывает коммуникационные вызовы, формируемые приложениями, и перенаправляет их в случае надобности на SOCKS-сервер. Если нет нарушений установленных правил безопасности, то работа SOCKS-клиента совершенно прозрачна для клиентских приложений и пользователей.

Таким образом, для формирования VPN по протоколу SOCKS в точке сопряжения каждой ЛВС с Internet на компьютере-шлюзе

устанавливается SOCKS-сервер, а на рабочих станциях в ЛВС и на компьютерах удаленных пользователей устанавливаются SOCKS-клиенты (рис. 29). SOCKS-сервер является ни чем иным, как МЭ, поддерживающим протокол SOCKS.

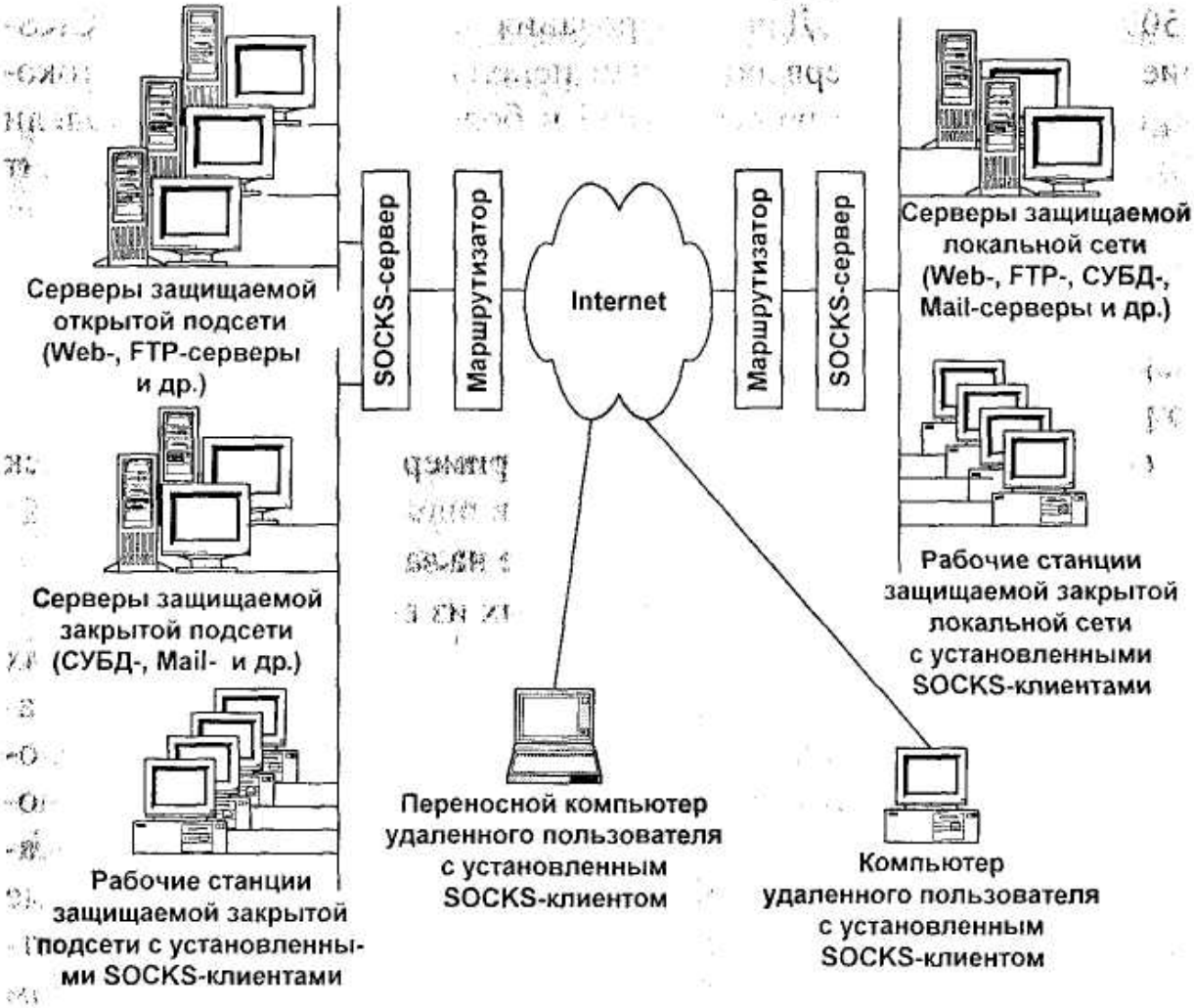


Рис. 29. Схема сетевого взаимодействия по протоколу SOCKS

Удаленные пользователи могут подключаться к Internet любым способом — по коммутируемой или выделенной линии. При попытке пользователя VPN установить соединение с каким-либо прикладным сервером SOCKS-клиент начинает взаимодействовать с SOCKS-сервером. По завершении первого этапа взаимодействия пользователь будет аутентифицирован, а проверка правил доступа покажет, имеет ли он право соединяться с конкретным серверным приложением, функционирующим на компьютере с указанным ад-

ссом. Дальнейшее взаимодействие может происходить по криптографически защищенному каналу.

Помимо защиты ЛВС от НСД, на SOCKS-сервер может возлагаться контроль доступа пользователей этой локальной сети к открытым ресурсам Internet (Telnet, WWW, SMTP, POP и др.). Доступ является полностью авторизованным, так как идентифицируются и аутентифицируются конкретные пользователи, а не компьютеры, с которых они выходят в сеть. Правила доступа могут запрещать или разрешать соединения с конкретными ресурсами Internet в зависимости от полномочий конкретного сотрудника. Действие правил доступа может зависеть и от других параметров, например, от метода аутентификации или времени суток. В дополнение к функциям разграничения доступа может выполняться регистрация событий и реагирование на задаваемые события.

Для достижения наиболее высокой степени безопасности сетевого взаимодействия серверы ЛВС, к которым разрешен доступ со стороны Internet, должны быть выделены в отдельный подсоединяемый к SOCKS-серверу сегмент, образующий защищаемую открытую подсеть (см. ЛВС слева на рис. 29). За счет трансляции сетевых адресов серверы и рабочие станции ЛВС, подсоединенной к Internet через SOCKS-сервер, могут не иметь зарегистрированных сетевых адресов и доменных имен. Разрешение адресов и имен производится SOCKS-сервером. При такой конфигурации пользователи VPN получают доступ ко всем серверам ЛВС, входящим в состав VPN, так, как если бы эти серверы находились в одной ЛВС.

Контрольные вопросы по разделу 2

1. На каких уровнях модели OSI работают какие протоколы создания VPN?
2. Что и какими средствами защищается на прикладном уровне?
3. Какие протоколы выполняют защиту данных в VPN на канальном уровне? Сравните их возможности.
4. Расскажите об особенностях протокола PPTP. Рассмотрите схемы его применения. Нарисуйте структуру пакета PPTP.
5. Расскажите об особенностях протокола L2F.

6. Расскажите об особенностях протокола L2TP. Рассмотрите схемы его применения. Сравните с протоколом PPTP.
7. Какие протоколы выполняют защиту данных в VPN на сетевом уровне? Сравните их возможности.
8. Расскажите об особенностях протокола IPSec и решаемых им задачах. Рассмотрите схемы его применения.
9. Что такое протокол IKE? Его функции.
10. Рассмотрите назначение и особенности протокола AH. Нарисуйте структуру заголовка и результирующего пакета в разных режимах.
11. Рассмотрите назначение и особенности протокола ESP. Нарисуйте структуру заголовка и результирующего пакета в разных режимах.
12. Сравните протоколы AH и ESP.
13. Что такое SA? Как она устанавливается и в каких основных режимах применяется?
14. Расскажите о базе данных политик безопасности.
15. Расскажите об особенностях протокола SKIP. Нарисуйте структуру SKIP-пакета и формат заголовка при использовании AH в SKIP.
16. Какие протоколы выполняют защиту данных в VPN на сеансовом уровне? Сравните их возможности.
17. Расскажите об особенностях протокола SSL. Поясните работу протокола диалога SSL.
18. Расскажите об особенностях протокола TLS.
19. Расскажите об особенностях протокола SOCKS. Поясните обобщенную схему установления соединения по протоколу SOCKS. Сравните 4-ю и 5-ю версии протокола.

3. УПРАВЛЕНИЕ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ

Как было показано ранее, в основе большинства средств защиты, применяемых в виртуальных частных сетях, лежат криптографические алгоритмы и протоколы или механизмы защиты, так или иначе их использующие. При этом предполагалось, что участники VPN уже имеют секретные и открытые ключи, необходимые для выполнения криптографических операций, и им необходимо только грамотно использовать средства защиты, в которых реализованы соответствующие криптографические алгоритмы и протоколы. Однако на практике применение криптографических средств защиты информации сталкивается с целым рядом задач, связанных с необходимостью надлежащим образом распоряжаться криптографическими ключами участников VPN. Обозначенный круг вопросов принято относить к одному из разделов прикладной криптографии – управлению криптографическими ключами.

3.1. Жизненный цикл криптографических ключей

Традиционно управление ключами считалось криптографами неосновным, "вспомогательным" разделом криптографии. Действительно, основной задачей криптографа является конструирование и анализ надежных криптографических алгоритмов и протоколов. Но в соответствии с современными представлениями стойкость любой криптосистемы определяется только степенью безопасности используемых в ней ключей, так как все долговременные элементы

криптосистемы (множество правил шифрования, его механизм и пр.) рано или поздно станут известными злоумышленнику. Указанный принцип был сформулирован еще в конце XIX в. и получил название "правило Керкхоффа".

Цель хорошей криптографической конструкции – свести более сложные проблемы к надлежащему управлению и безопасному хранению небольшого количества криптографических ключей, безопасность которых и доверие к ним пользователей достигается путем их физической изоляции и организационных мер защиты. При этом для обеспечения безопасности криптографических ключей можно и нужно использовать любые доступные методы:

- технические средства охраны (изолированные помещения, сигнализация и т.п.);
- защищенную от взлома аппаратуру (при этом, однако, важно обеспечить надежную аутентификацию пользователя при работе с нею);
- концентрацию ключевого материала в небольшом количестве легко наблюдаемых и внушающих доверие компонентов системы.

В основе данного раздела прикладной криптографии лежит ряд понятий, которые будут рассмотрены ниже. Большинство из них сформулировано на основе [13].

Ключевым отношением называется состояние, в котором взаимодействующие стороны разделяют общие данные – ключевой материал, — необходимые для выполнения криптографических алгоритмов и протоколов.

Управление ключами (key management) – это совокупность технологий и процедур, посредством которых устанавливаются и поддерживаются ключевые отношения между участниками криптографического протокола.

Цель управления ключами – поддерживать ключевые отношения таким образом, чтобы проявились угрозы ключевому материалу, основными из которых являются следующие:

- утрата конфиденциальности (секретности) секретных криптографических ключей;

- утрата аутентичности секретных или открытых ключей. Требование аутентичности включает знание или возможность проверки идентичности лица, обладающего ключевым материалом, заявленному субъекту;
- несанкционированное использование секретных или открытых ключей, например, использование недействительного ключа, нецелевое использование ключа.

Компрометация ключа – это событие, в результате которого произошла или могла произойти утрата одного из свойств криптографического ключа, обеспечивающего безопасность криптосистемы.

Таким образом, можно заключить, что основными задачами управления ключами являются:

- обеспечение *секретности, подлинности и целостности* для *секретных* криптографических ключей;
- обеспечение *подлинности и целостности* для *открытых* криптографических ключей.

Здесь под секретными криптографическими ключами понимаются как общие секретные ключи симметричных криптосистем, так и секретные ключи асимметричных криптосистем (которые, в отличие от первых, не являются общими для двух или более абонентов, а известны исключительно своим владельцам).

На практике дополнительной целью управления ключами является согласие с поддерживающейся *политикой безопасности* системы.

Основным международным стандартом в области управления криптографическими ключами является стандарт Международной организации по стандартизации и Международной электротехнической комиссии ISO/IEC 11770, состоящий из трех частей:

- ISO/IEC 11770-1 – Key management – Introduction.
- ISO/IEC 11770-2 – Key management – Symmetric techniques.
- ISO/IEC 11770-3 – Key management – Asymmetric techniques.

В указанном стандарте задачи управления ключами выводятся из задачи обеспечения безопасности криптографических ключей на всех этапах их жизненного цикла.

Жизненный цикл криптографического ключа – это последовательность состояний, в которых пребывает ключевой материал за время своего существования в криптосистеме.

Как известно, любой объект (например, любое промышленное изделие) имеет определенное, конечное время жизни, за которое он проходит определенные стадии своего развития от "рождения" до "гибели". Не являются в этом смысле исключением и криптографические ключи. Для любого объекта стандартизации стандартами ISO определяются четыре стадии жизненного цикла: предоперационная, операционная, постоперационная стадии и стадия выхода из эксплуатации.

Применительно к криптографическим ключам эти стадии означают следующее:

- на предоперационной стадии ключ еще не доступен для штатного использования в криптосистеме;
- находясь в операционной стадии жизненного цикла, ключ доступен пользователям криптосистемы и используется ими в штатном режиме;
- на постоперационной стадии ключ более не используется в штатном режиме, но он доступ в особом режиме для специальных целей;
- на стадии выхода из эксплуатации ключ более не доступен, а все записи, содержащие значение ключа, удалены из криптосистемы.

Внутри указанных общих стадий жизненного цикла можно более точно выделить различные состояния, в которых пребывает ключ, и условия переходов между ними (рис. 30).

1. Регистрация пользователя: субъект становится авторизованным пользователем криптосистемы, приобретает или создает безопасным, одноразовым способом начальный ключевой материал (пароли, персональные коды и др.).

2. Инициализация пользователя: субъект криптосистемы инициализирует свои криптографические приложения, например, производит инсталляцию программного и аппаратного обеспечения, включая инсталляцию на него начального ключевого материала, полученного во время регистрации.

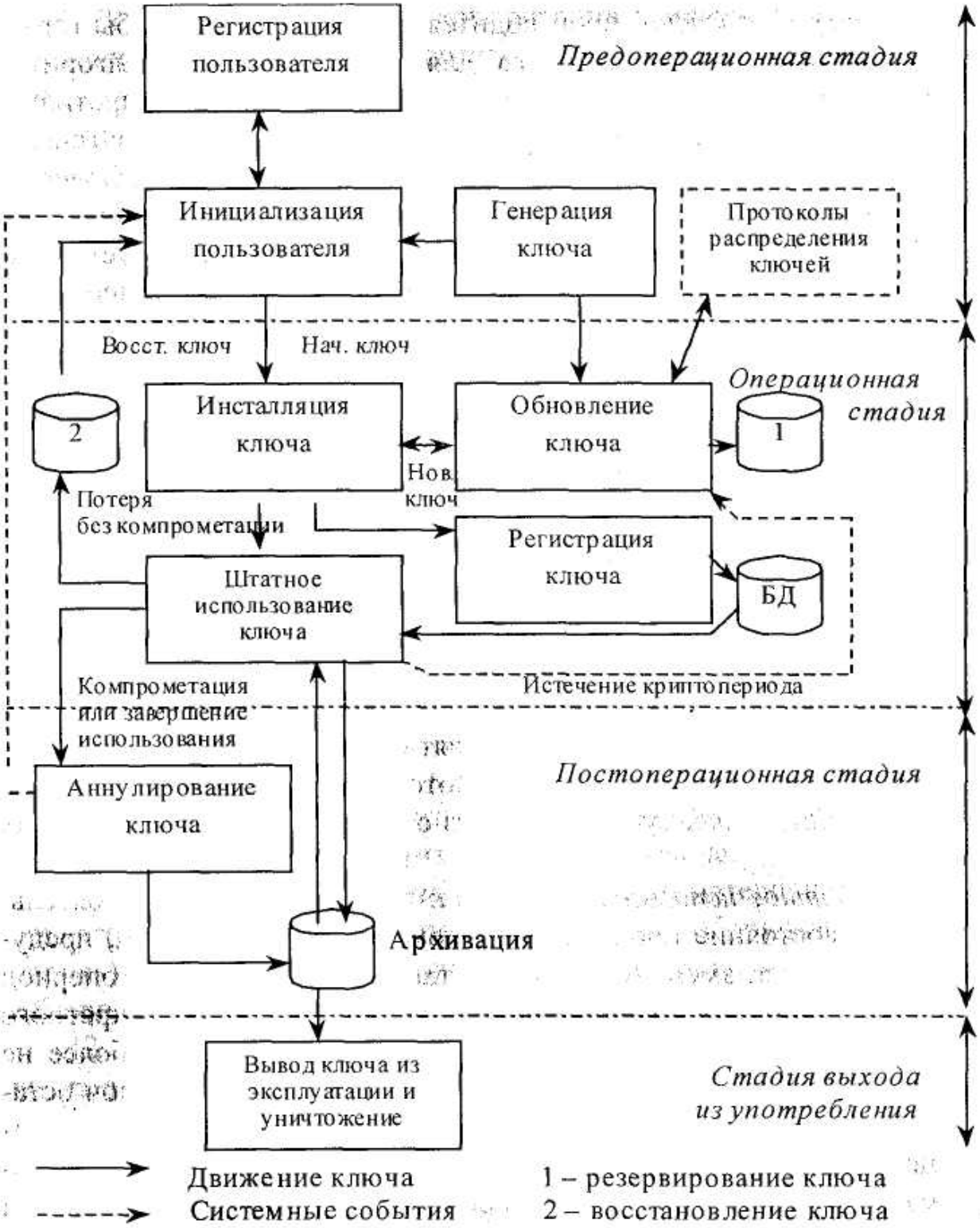


Рис. 30. Жизненный цикл криптографических ключей

3. Генерация ключа: производится таким образом, чтобы гарантировать необходимые свойства для приложения или алгоритма и случайность (в смысле возможности предсказания его противником с пренебрежимо малой вероятностью). Субъект может генерировать свои собственные ключи или приобретать ключи от доверенного компонента криптосистемы.

4. Инсталляция ключа: ключевой материал инсталлируется для функционального использования в программном или аппаратном обеспечении субъекта, включая один из следующих способов: ручной ввод пароля или персонального кода, запись на магнитный диск, в постоянную память, микроэлектронную схему или другую аппаратуру. Начальный ключевой материал может служить для установления сеанса с доверенным компонентом криптосистемы, во время которого в реальном масштабе времени согласуются рабочие ключи. Во время последовательных обновлений новый ключевой материал заменяет используемый.

5. Регистрация ключа: одновременно с инсталляцией ключа ключевой материал может быть публично записан как ассоциированный с уникальным именем субъекта системы. Для открытых ключей регистрация может выполняться специально выделенной третьей стороной, при посредстве которой они становятся доступными для остальных субъектов через открытые директории или др. средства.

6. Штатное использование ключа: при нормальных обстоятельствах это состояние продолжается, пока не истечет период, предусмотренный регламентом системы (так называемый криптопериод ключа), но он может быть разделен, например, для пар секретного и открытого ключей шифрования (когда открытый ключ более не является действительным для шифрования, а секретный ключ остается в нормальном использовании для расшифрования). Цель жизненного цикла – содействовать операционной доступности ключевого материала для стандартных криптографических целей. Иными словами, фаза жизненного цикла является самой основной, центральной, ради которой поддерживаются все остальные фазы и инфраструктура криптосистемы.

7. Резервирование ключа: копирование ключевого материала на независимом, безопасном носителе обеспечивает источник данных для восстановления ключа. Резервирование подразумевает кратковременное хранение во время операционного использования.

8. Обновление ключа: по истечение периода, предусмотренного регламентом системы, операционный ключевой материал заменяется на новый. Это может включать процедуры генерации ключа, наследования ключа, выполнение протоколов распределения ключей. Для открытых ключей обновление и регистрация новых ключей обычно включает безопасные коммуникационные протоколы с доверенной третьей стороной.

9. Архивация ключа: ключевой материал, более не используемый в штатном режиме, может быть заархивирован, чтобы обеспечить источник восстановления ключа при специальных обстоятельствах (например, в случае возникновения конфликтов о принадлежности ЭЦП). Архивация подразумевает долговременное хранение ключей в постоперационной стадии, при этом могут применяться алгоритмы сжатия данных с целью сокращения объема хранимых ключей.

10. Вывод из эксплуатации и уничтожение: когда более нет необходимости поддерживать ассоциацию ключа с субъектом, ключ выводится из эксплуатации, т.е. удаляется из всех публичных записей, и все копии ключа уничтожаются. В случае секретных ключей должны быть безопасно стерты все "следы" ключа.

11. Восстановление ключа: если ключевой материал потерян, но при этом не случилось компрометации (сбой оборудования, забыт пароль), должно быть возможно восстановить ключевой материал с безопасной резервной копии.

12. Аннулирование ключа: может быть необходимо удалить ключи из операционного использования до истечения предполагаемого срока по различным причинам, включая компрометацию ключей или выбытие владельца ключа из системы.

3.2. Особенности управления ключевой системой асимметричных криптосистем. Концепция инфраструктуры открытых ключей

Изображенный на рис. 30 жизненный цикл ключа более соответствует асимметричным криптосистемам. В симметричных он, как правило, проще (например, сеансовые ключи не регистрируются, не резервируются, не восстанавливаются, не архивируются).

Важно обратить внимание на то, что с точки зрения обеспечения безопасности криптографических ключей ни одна из указанных стадий жизненного цикла и ни одно из состояний ключа *не является более или менее важным по сравнению с другими*. Действительно, если безопасность ключа нарушена *хотя бы на одной из стадий*, хотя бы в одном из состояний или при переходе из одного состояния в другое, то это приведет *к нарушению безопасности криптосистемы в целом*. Различные фазы жизненного цикла отличаются только с точки зрения технической сложности обеспечения безопасности ключей, но с точки зрения логической организации процесса управления ключами все они равноправны и в равной степени важны. При разработке и эксплуатации систем криптографической защиты информации большое внимание должно уделяться вопросам грамотной организации управления криптографическими ключами на всех этапах их жизненного цикла.

Если рассматривать жизненный цикл ключей с точки зрения сложности реализации мер обеспечения безопасности ключей, выделяют четыре наиболее сложные фазы, на которых необходимо решать задачи управления ключами: генерация, распространение, хранение и уничтожение ключей. Из них самой сложной для реализации и самой потенциально опасной является фаза распространения ключей, включающая транспортировку ключей между участниками криптосистемы.

В последнее время преимущественное распространение получили такие средства и системы защиты информации, в которых ведущую роль играют методы криптографической защиты информации, основанные на асимметричных криптосистемах, а симметричные криптосистемы играют по отношению к ним подчиненную роль и используются как необходимое средство в тех случаях, когда

асимметричные методы не удовлетворяют требованиям производительности криптосистемы. Ярким примером такого подхода являются, в частности, виртуальные частные сети. В связи с этим ведущую роль приобретает именно организация управления ключами асимметричных криптосистем. Она, в свою очередь, включает две подзадачи: управление частными секретными ключами участников и управление их открытыми ключами.

Задача управления секретными ключами здесь проще, чем в симметричных криптосистемах, так как секретные ключи никогда не выходят за пределы собственности их владельцев: нет необходимости передавать их по каким-либо каналам связи, распространять среди других участников. Оставшиеся задачи генерации, надежного хранения и распространения секретных ключей участниками асимметричных криптосистем вполне решаемы традиционными средствами, хорошо отработанными в процессе развития симметричных криптосистем.

Задача управления открытыми ключами является новой по сравнению с симметричными криптосистемами и требует своих особых методов решения. Для ее решения в последнее время наметилось отдельное научно-практическое направление прикладной криптографии, а сама идея решения этой задачи выразилась в создании специальной инфраструктуры в рамках криптосистемы, получившей наименование *инфраструктуры открытых ключей* (что является дословным переводом с английского термина Public Key Infrastructure).

Напомним, что под инфраструктурой понимаются составные части общего устройства системы, носящие вспомогательный, подчиненный характер и обеспечивающие нормальную деятельность системы в целом. Следовательно, в данном случае речь идет о таких вспомогательных элементах криптосистемы, которые берут на себя организацию управления открытыми ключами, освобождая участников криптосистемы от необходимости решения второстепенных для них задач и выполнения несвойственных для них функций.

Инфраструктура открытых ключей (ИОК) – это универсальная концепция организованной поддержки криптографических средств защиты информации в крупномасштабных информационных систе-

мах в соответствии с принятыми в них политиками безопасности, которая реализует управление криптографическими ключами на всех этапах их жизненного цикла, обеспечивая взаимодействие всех средств защиты распределенной системы.

Логически ИОК объединяет механизмы, субъекты, правила и взаимосвязи, которые необходимы для доступа к криптографическим ключам и для ассоциирования открытых криптографических ключей со своими владельцами.

Физически ИОК состоит из программ, форматов данных, коммуникационных протоколов, политик и процедур, требуемых для использования в организации криптосистем с открытым ключом.

ИОК может быть интегрирована со всеми основными ОС, сетевым программным обеспечением и основными прикладными программами. Чтобы использовать сервисы, предоставляемые ИОК, в прикладных программах, они должны быть адаптированы, или разработаны новые прикладные программы.

Важно иметь в виду, что создание инфраструктуры открытых ключей имеет целью комплексную поддержку *всего жизненного цикла открытых криптографических ключей в целом*, а не только каких-либо отдельных его фаз, например, распространения ключей (хотя последняя задача и является технически наиболее сложной).

Модель SPKI (Simple Public Key Infrastructure) – наиболее простая модель ИОК, разработанная Международной инженерной организацией по сети Internet IETF. Проект SPKI направлен на создание простой, минимально необходимой криптографической инфраструктуры и представлен двумя документами серии RFC (Request for Comments):

- RFC 2692 – SPKI Requirements;
- RFC 2693 – SPKI Certificate Theory.

Модель PKIX (Public Key Infrastructure for X.509) обеспечивает существенно более широкую функциональность и основана на стандарте Международного телекоммуникационного Союза ITU X.509. Ее составляют несколько уже утвержденных стандартов RFC и порядка двадцати проектов (draft) стандартов RFC. К утвержденным стандартам относятся:

- RFC 2459 – Internet X.509 Public Key Infrastructure Certificate and CRL;
- RFC 2510 – Internet X.509 Public Key Infrastructure Certificate Management Protocols;
- RFC 2511 – Internet X.509 Certificate Request Message Format;
- RFC 2527 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 2528 – Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates;
- RFC 2559 – Internet X.509 Public Key Infrastructure Operational Protocols – LDAP v2;
- RFC 2560 – Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP;
- RFC 2585 – Internet X.509 Public Key Infrastructure Operational Protocols – FTP and HTTP;
- RFC 2559 – Internet X.509 Public Key Infrastructure LDAP v2 Schema.

В настоящее время именно модель PKIX претендует стать стандартом ИОК не только в сети Internet, но и вообще в любых сетях, построенных на базе коммуникационной архитектуры TCP/IP. В связи с тем, что данная модель имеет существенное значение и для организации инфраструктуры открытых ключей в виртуальных частных сетях, ниже она будет рассмотрена более детально.

Модель APKI (Architecture for Public Key Infrastructure) описывает архитектуру для инфраструктуры открытых ключей с целью создания всеобъемлющей, полнофункциональной схемы поддержки всей многоуровневой иерархии механизмов защиты: от примитивов до прикладных протоколов (рис. 31) [14].

Основными уровнями инфраструктуры открытых ключей в модели являются: криптографические примитивы, криптографические сервисы, сервисы манипулирования долговременными ключами, сервисы защиты протоколов, защищенные протоколы. Дополнительно в архитектуру APKI включены: системные сервисы обеспечения защиты, сервисы реализации политики безопасности, сервисы поддержки. APKI опирается на широкую базу стандартов RFC.

Рис. 31. Архитектурная модель APKI

Использование общепринятых стандартов при реализации ИОК позволяет удовлетворить основные требования, предъявляемые к открытым информационным системам: переносимость и способность к взаимодействию – в части реализации функций обеспечения безопасности информации. Использование концепции ИОК в том или ином виде предусмотрено в большинстве моделей защиты информационных систем более широкого профиля, таких как CDSA (Common Data Security Architecture).

Элементы технологии ИОК реализуются множеством производителей программного обеспечения, включая такие известные фирмы, как IBM, RSA, Entrust Technologies и др. На уровне отдельной организации, систем документооборота между организациями или в пределах одной отрасли эта технология уже может быть реализована имеющимися средствами программного обеспечения. На государственном уровне в России реализация ИОК – это, по-видимому, вопрос более или менее недалекого будущего: по крайней мере, та-

кую перспективу открывает введенный в начале 2002 г. "Закон об электронной цифровой подписи" [15] (будет рассмотрен далее, в п. 3.5). На глобальном, общемировом уровне работы по стандартизации ИОК на базе сети Internet ведутся рядом международных организаций.

3.3. Метод сертификации открытых ключей

Как отмечалось выше, наиболее сложным для обеспечения безопасности открытых ключей является этап распространения их среди участников криптосистемы. Известен целый ряд подходов к решению этой задачи [13, гл. 13]:

1. Передача открытого ключа через доверенный канал связи, обеспечивающий секретность, целостность и аутентичность.
2. Прямой доступ субъектов в доверенную базу данных (файл, директорию).
3. Использование доверенного сервера в режиме реального времени.
4. Использование сервера в режиме отложенного доступа и метода сертификации открытых ключей.
5. Использование криптосистем, неявно гарантирующих аутентичность открытых ключей, в том числе:
   - системы, основанные на идентификаторах;
   - системы с неявно сертифицированными открытыми ключами (например, схемы Гюнтера и Гираулта).

Среди всех указанных методов преобладающим на практике является метод сертификации открытых ключей. Остальные в силу различных, многочисленных причин находят лишь ограниченное применение.

Рассмотрим кратко основное содержание метода сертификации открытых ключей.

Пусть имеется криптосистема, включающая большое число участников (абонентов), например, VPN (рис. 32). Среди участников криптосистемы выделяется специальный участник, которому доверяют все остальные, получивший название *"центр сертификации ключей"*, или *"агентство сертификации"* (Certification Authority),

или *"удостоверяющий центр"* (УЦ). Его функции может выполнять, например, администратор системы, оснащенный соответствующим аппаратным и программным обеспечением (сервер регистрации и сертификации ключей). Все остальные участники являются обычными, "рядовыми" абонентами криптосистемы, например, узлами VPN, выполняющими функции криптографической защиты данных.

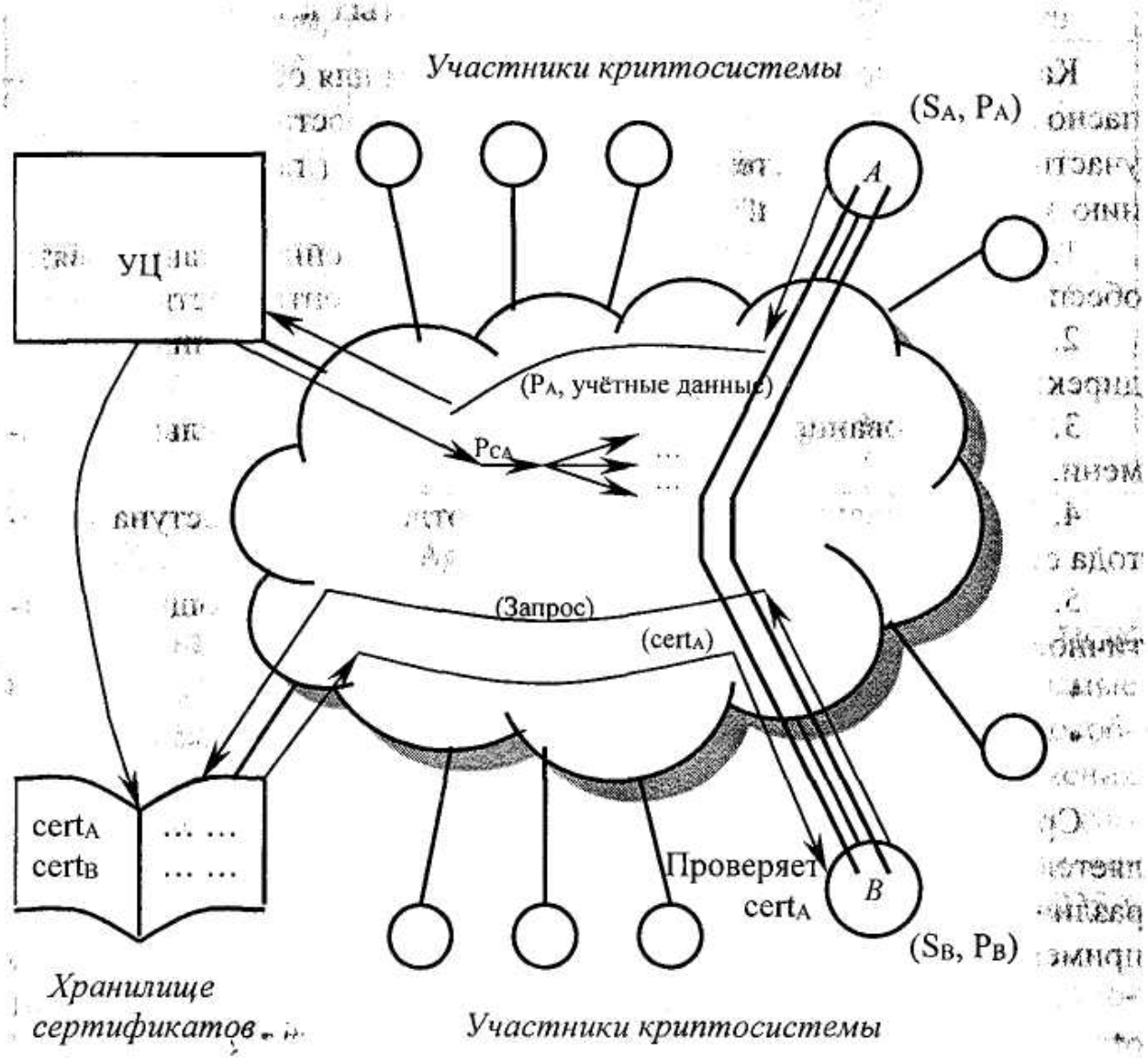


Рис. 32. Процессы получения и использования сертификатов участниками криптосистемы

При введении в систему каждого из этих участников – возьмем для примера участника *A* – он должен пройти процедуру регистра-

ции в криптосистеме (что соответствует первой фазе жизненного цикла его криптографического ключа). Для этого он контактирует с УЦ, чтобы зарегистрировать свой открытый ключ и получить от него так называемый сертификат своего открытого ключа. УЦ должен проверить представленные ему учетные данные, а также (что очень важно!) *знание секретного ключа, соответствующего представленному для регистрации открытому ключу*. Решить эту задачу можно различными способами: в самом простом случае УЦ может попросить *A* зашифровать на своем секретном ключе текст заданного формата и проверить правильность его расшифрования при помощи представленного открытого ключа, а можно воспользоваться протоколом доказательства знания ключа с нулевым разглашением знаний.

Сертификат открытого ключа – специальная структура данных, состоящая из полей данных и поля подписи. Поле данных содержит, как минимум, какие-либо признаки абонента (идентификатор, атрибуты) и его открытый ключ. Поле подписи – это ЭЦП УЦ под полем данных, логически связывающая признаки абонента с его открытым ключом.

Все абоненты, заинтересованные в связи с абонентом *A*, получают впоследствии его сертификат либо путем обмена с абонентом *A*, либо извлекая его из открытого общедоступного справочника, который заводится в криптосистеме. Сертификат, таким образом, является средством для хранения, распространения и передачи через небезопасные каналы связи открытых ключей без опасения их необнаружимого изменения.

Различают две формы сертификатов открытых ключей: *идентификационные* и *атрибутные*.

В *идентификационном сертификате* обязательно присутствует идентификатор субъекта – владельца ключа, по которому можно однозначно установить его личность. Основным стандартом по идентификационным сертификатам является стандарт Международного телекоммуникационного Союза ITU X.509. В соответствии со стандартом X.509 сертификат имеет следующий формат (рис. 33).

Сертификат состоит из двух полей: поля данных и поля подписи. Поле данных имеет формат, описанный в стандарте. Поле подписи

содержит ЭЦП УЦ открытых ключей под полем данных. Существуют две версии этого стандарта, которые принято обозначать X.509v2 и X.509v3. Различие между ними заключается в том, что в версии 2 определены поля "Уникальный идентификатор УЦ, выпустившего сертификат" и "Уникальный идентификатор владельца открытого ключа", а в версии 3 стандарта эти поля исключены, но предусмотрено наличие в поле данных дополнительного поля расширения, содержание которого не определено: оно может специфицироваться другими стандартами, зависеть от области применения информационной системы и т.п.

Версия сертификата
Серийный номер сертификата
Идентификатор алгоритма ЭЦП, используемого УЦ
Имя УЦ (директориальное имя по стандарту X.500)
Период действия сертификата
Имя владельца открытого ключа (директориальное имя по стандарту X.500)
Информация об открытом ключе владельца: • идентификатор алгоритма; ▪ значение открытого ключа
Уникальный идентификатор УЦ, выпустившего сертификат (v2)
Уникальный идентификатор владельца открытого ключа (v2)
Поле расширения (v3): содержание не определено
Цифровая подпись УЦ под всеми предыдущими полями

Рис. 33. Формат сертификата открытого ключа по стандарту ITU X.509

Наиболее разработанными и широко применяемыми на практике логическими моделями инфраструктуры открытых ключей на базе идентификационных сертификатов являются:

- X9.55 – американский стандарт для финансовой индустрии;
- PKIX – проект стандарта IETF на базе стандарта X.509v3, адаптирующий положения этого стандарта для использования в сети Internet;
- APKI – архитектура для ИОК, описанная в документах The Open Group.

Однако использование идентификационных сертификатов не всегда желательно для пользователей, так как при этом может происходить доступ к информации, не имеющей отношения к тому случаю, по которому необходим данный конкретный факт доступа к сертификату. Возможность однозначно установить личность владельца по сертификату может привести к установлению "тотального контроля" над действиями участников криптосистемы в информационной системе. В этой связи было предложено использовать другую форму сертификатов

Атрибутные сертификаты связывают открытый ключ с одним или более "атрибутов", которые в соответствии со стандартом Международного телекоммуникационного Союза X.501 (ISO/IEC 9594-2) определяются как "информация любого типа". Таким образом, один и тот же участник в зависимости от ситуации и используемой прикладной программы может предстать в разных "ипостасях", между которыми невозможно установить однозначную связь. К примеру, атрибутом может быть роль пользователя в информационной системе, например, путем указания его должности. Тогда можно реализовать модель управления доступа "по ролям", т.е. участники системы, занимающие одну и ту же должность, имеют абсолютно одинаковые права в системе, и невозможно установить, кто именно из них совершил конкретное действие с применением данного конкретного сертификата.

Наиболее разработанными и широко применяемыми на практике логическими моделями инфраструктуры открытых ключей на основе атрибутных сертификатов являются:

- X9.57 – американский стандарт для финансовой индустрии;

- SPKI – проект стандарта IETF для использования в сети Internet.

УЦ открытых ключей – это специально выделенный участник криптосистемы, которому доверяют все остальные участники ("центр доверия"), чья подпись служит гарантией подлинности ключей и который выполняет следующие функции:

- сбор сведений об участниках системы, необходимых для сертификации: имя, почтовый адрес, права доступа, должность, номер кредитной карты и т.п. (зависит от конкретного приложения);
- генерация и рассылка (либо помещение в общедоступное хранение) сертификатов открытых ключей;
- уничтожение сертификатов с истекшим сроком годности;
- обновление сертификатов;
- аннулирование сертификатов.

Аннулирование сертификата может потребоваться в случаях, когда срок санкционированного использования открытого ключа участника системы прерывается досрочно, ранее, чем это предусмотрено принятым в системе регламентом, например:

- при компрометации секретного ключа участника криптосистемы, соответствующего данному открытому ключу;
- при удалении (выбытии) пользователя из системы;
- при смене роли пользователя в системе (перемещении пользователя).

Аннулирование сертификата – это чрезвычайное обстоятельство, о котором необходимо оповестить всех участников криптосистемы. Существуют два способа решения этой задачи.

- *Проверка статуса сертификата в режиме реального времени.* Для этого требуется выполнение специального протокола с УЦ открытых ключей, который отвечает на вопрос, не был ли запрошенный сертификат аннулирован.
- *Периодическое создание и рассылка списков аннулированных сертификатов* (CRL – Certificate Revocation List). Формат CRL определен в стандарте ITU X.509 v2 (рис. 34).

Второй способ на практике используется чаще. Однако у него есть один существенный недостаток: между двумя последовательными рассылками списка аннулированных сертификатов всегда существует какой-то временной "зазор", т.е. об аннулировании серти-

фиката какого-либо участника все остальные участники узнают не мгновенно, а только по прошествии некоторого времени. Наличие такого разрыва создает угрозу несанкционированного использования аннулированного ключа.

УЦ рассылает всем участникам системы свой открытый ключ, который нужен им для проверки подписи на сертификатах. Считается, что подменить его невозможно в силу трех причин: массовости рассылки, периодического повтора и общедоступности.

В криптосистемах с большим числом участников или с большой интенсивностью потока требований к УЦ функции регистрации участников нередко возлагают на специально выделяемый центр регистрации (Registration Authority – RA).

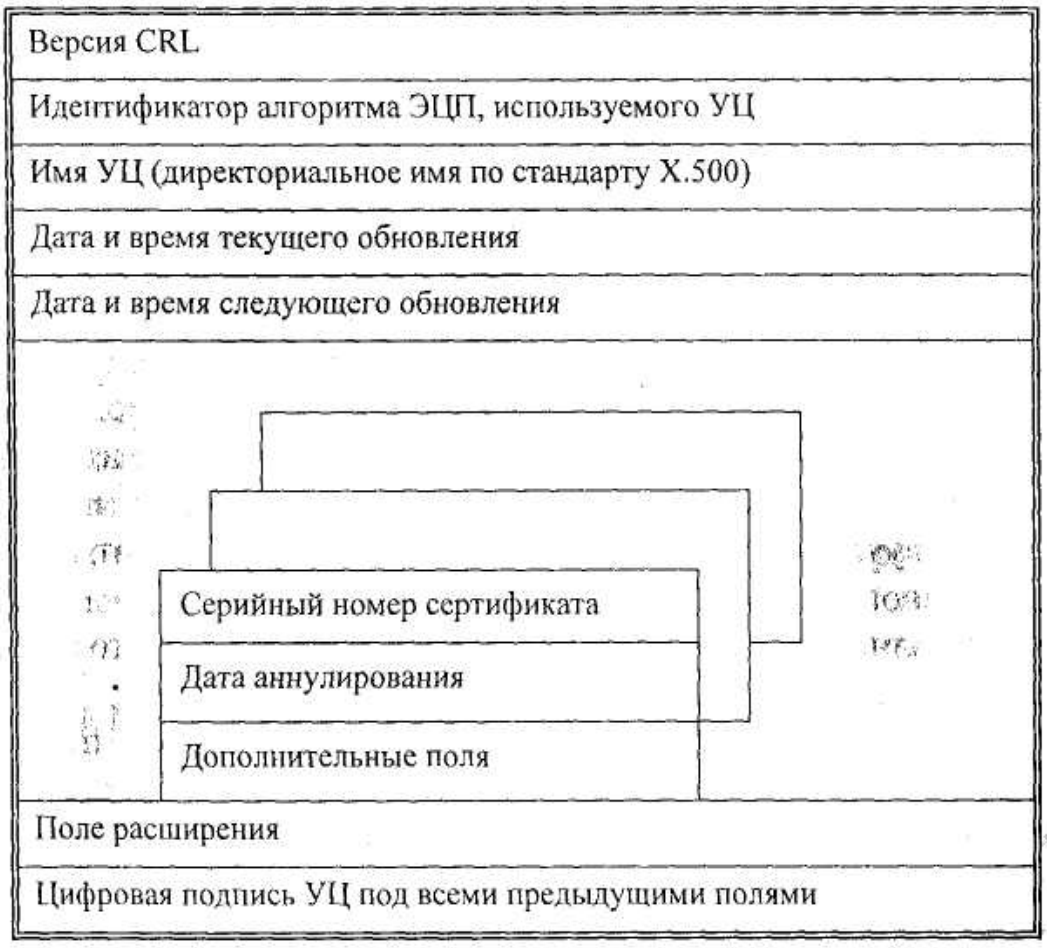


Рис. 34. Формат списка аннулированных сертификатов по стандарту ITU X.509 v2

Сертификаты всех участников криптосистемы могут либо храниться в специальном общедоступном хранилище, либо рассылаться по сети. На практике преимущественно используется первый способ, причем физически хранилище сертификатов чаще всего реализуется либо с использованием директориального сервиса (как директория, к которой открыт доступ на чтение всем участникам), либо веб-сервиса (как веб-страница, с которой все участники криптосистемы могут забирать сертификаты).

Преимущество сертификата в том, что два участника системы (к примеру, два узла VPN), доверяющие одному и тому же УЦ, могут не знать и не хранить открытые ключи никаких других абонентов, а при необходимости обратиться в УЦ и получить необходимые ключи. Для этого ему достаточно знать только открытый ключ УЦ. Это позволяет применять метод сертификации открытых ключей в криптосистемах со сколь угодно большим и даже неопределенным числом участников, где все участники не покрыты непосредственной сетью контактов между собой.

Теперь для того, чтобы узнать открытый ключ любого интересующего его абонента, участнику криптосистемы (обозначим его *B*) необходимо однократно приобрести аутентичный открытый ключ УЦ открытых ключей (что технически реализовать не сложно). Далее для установления связи с абонентом *A* ему необходимо:

1) приобрести сертификат открытого ключа *A* одним из следующих способов: обратившись в хранилище сертификатов, непосредственно получив его от УЦ или от абонента *A* (зависит от порядка, установленного в системе);

2) выполнить процедуру проверки сертификата, состоящую из следующих действий:

- проверки текущей даты и времени и сравнения с периодом действия сертификата;
- проверки действительности в данный момент времени открытого ключа самого УЦ;
- проверки подписи УЦ на сертификате открытого ключа абонента *A*, используя открытый ключ УЦ;
- проверки, не был ли сертификат аннулирован к текущему моменту времени.

3) в случае, если все проверки окончились с положительным результатом, принять открытый ключ, извлеченный из сертификата *A* как аутентичный ключ.

Далее *B* может использовать открытый ключ абонента *A* для выполнения любых необходимых ему криптографических алгоритмов или протоколов. К примеру, участники *A* и *B*, приобретя таким образом открытые ключи друг друга, могут выполнить протокол открытого распределения Диффи–Хеллмана, выработать с его помощью общий секретный ключ для симметричной криптосистемы и использовать далее для шифрования трафика VPN какой-либо симметричный алгоритм: DES, ГОСТ 28147-89 и др.

Заметим, что, хотя сертификат является вспомогательным средством для транспортировки и обеспечения подлинности открытого ключа, он, как и сам ключ, имеет свой жизненный цикл. В его жизненном цикле можно выделить те же стадии и ряд состояний, в которых пребывает сертификат: создание, рассылка, штатное использование, обновление или аннулирование, уничтожение сертификата.

Недостаток метода сертификации открытых ключей – в том, что часто участникам криптосистемы после проверки сертификата все равно необходим доступ в базу данных об участниках криптосистемы в реальном масштабе времени (например, для проверки аннулирования сертификата либо чтобы получить какие-то дополнительные данные об этом участнике, необходимые для работы прикладных программ). Это не всегда удобно, поэтому сейчас наблюдается "откат" к модели ИОК с УЦ ключей, работающим в реальном масштабе времени.

3.4. Модель инфраструктуры открытых ключей PKIX

Концепция инфраструктуры открытых ключей предоставляет основу для практического использования асимметричных криптосистем с целью повышения уровня защищенности крупномасштабных информационных систем. Инфраструктура открытых ключей является основой использования криптографии во многих прикладных программах и коммуникационных протоколах, таких как Secure Sockets Layer (SSL), Secure Multimedia Internet Mail Extensions

(S/MIME), IP Security (IPSec), Secure Electronic Transactions (SET), Pretty Good Privacy (PGP). В связи с этим международной организацией IETF с 1995 г. ведется работа по созданию целостной модели ИОК на базе стандарта ITU X.509 v3. Данная модель получила наименование PKIX (Public Key Infrastructure for X.509). Предполагается, что она станет одной из самых широко используемых в сети Internet. В связи с этим целесообразно остановиться на этой модели более подробно.

Основными элементами модели PKIX являются (рис. 35):

- конечные субъекты End-Entities (EE);
- УЦ ключей Certificate Authority;
- репозиторий (хранилище) сертификатов Certificate Repository (CR);
- центр регистрации Registration Authority (RA);
- цифровые сертификаты согласно стандарту X.509 v3.

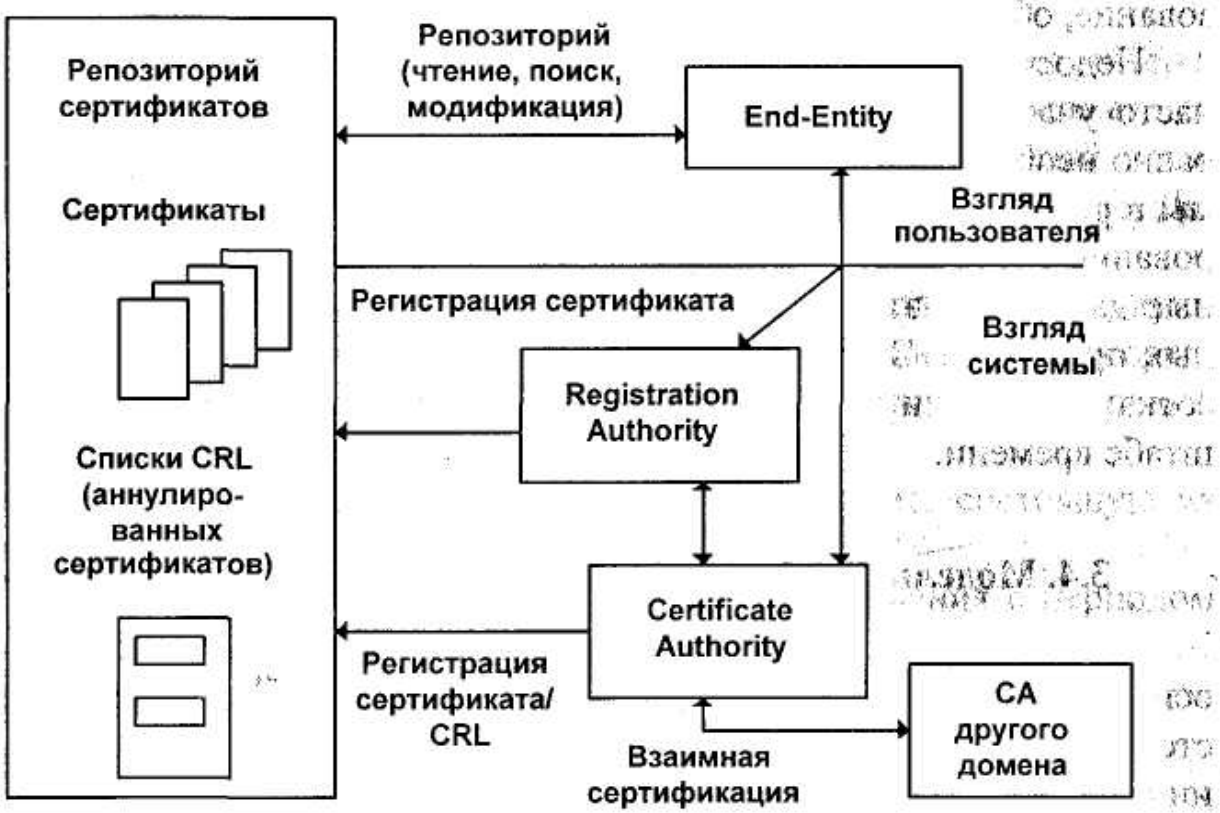


Рис. 35. Общая структура ИОК согласно модели PKIX

Конечные субъекты определяются в модели как пользователи ИОК или как системы конечных пользователей, которые являются субъектами сертификации. Другими словами, этот термин означает любого субъекта, который пользуется некоторыми сервисами или функциями системы ИОК, который может быть либо владельцем сертификата, либо лицом, его запрашивающим.

УЦ – субъект ИОК, подписывающий сертификаты. УЦ вместе с RA несут ответственность за идентификацию субъектов сертификации. Логический домен, в котором УЦ выпускает в обращение сертификаты и управляет ими, называется доменом безопасности. Физически он может охватывать организацию, предприятие, большое подразделение организации или другую логическую общность пользователей. Основные операции, выполняемые УЦ, — это выпуск, обновление и аннулирование сертификатов.

УЦ может выпускать несколько видов сертификатов:

- сертификаты пользователей;
- сертификаты УЦ, в том числе самоподписанные сертификаты (или корневые сертификаты), а также сертификаты УЦ, подчиненных данному УЦ;
- кросс-сертификаты – сертификаты УЦ, находящегося в другом домене безопасности.

Каждый сертификат имеет период, в течение которого он остается действительным для санкционированного использования в системе. При наступлении даты окончания его действия должен быть произведен процесс обновления сертификата, в результате чего для данного конечного субъекта будет выпущен новый цифровой сертификат.

В случае наступления чрезвычайных обстоятельств сертификат может быть выведен из употребления до истечения его срока действия. Если это необходимо, УЦ публикует сертификат в списке аннулированных сертификатов (Certificate Revocation List, CRL). Субъекты ИОК, которым необходимо знать, является ли сертификат действительным, могут производить поиск в CRL для проверки любых записей об аннулировании сертификатов.

Репозиторий сертификатов (CR) – это хранилище выпущенных в обращение сертификатов и списков аннулированных сертифика-

тов. Хотя CR не является обязательным элементом ИОК, он значительно улучшает доступность и управляемость системы.

Поскольку стандарт X.509, на котором основывается модель PKIX, является составной частью стандартов на директориальный сервис серии X.500, наиболее естественной реализацией репозитория сертификатов является директория. Поэтому в модель PKIX включен стандарт RFC 2587, определяющий метод доступа в репозиторий, при помощи которого конечные субъекты или УЦ могут доставать или изменять сертификаты или списки аннулированных сертификатов, хранящиеся в репозитории. Метод основан на использовании протокола LDAP v2 (Lightweight Directory Access Protocol), являющегося стандартом де-факто для коммуникационной архитектуры TCP/IP.

Возможны и другие способы реализации репозитория сертификатов (например, веб-страницы), хотя они и не рекомендованы моделью PKIX.

Центр регистрации (RA) является необязательным компонентом ИОК. В некоторых случаях функции RA включены в УЦ. Иногда центр регистрации отделяется от УЦ с целью повышения производительности или безопасности системы.

Цифровые сертификаты, согласно модели PKIX, – это сертификаты открытых ключей конечных субъектов ИОК, соответствующие стандарту ITU X.509 v3. Кроме того, сертификатам могут присваиваться классы, означающие степень возможного доверия к ним. Тот или иной класс назначается сертификату при его создании на основании тщательности проведенного RA процесса регистрации конечного субъекта и объема проверенной при этом информации.

К *вспомогательным элементам* ИОК относятся:

- списки аннулированных сертификатов;
- протоколы ИОК;
- средства аудита ИОК.

Списки аннулированных сертификатов – средство уведомления субъектов ИОК об аннулировании цифровых сертификатов. В модели PKIX предложен и принят формат списков аннулированных сертификатов согласно ITU X.509 v2. Список содержит серийные номера аннулированных сертификатов, метки времени, соответствующие

моментам их аннулирования, подписи УЦ и некоторые расширения. Списки могут выпускаться периодически (например, раз в сутки) или в случае аннулирования хотя бы одного сертификата (если такие события происходят сравнительно редко). Любой субъект ИОК может проверить сертификат путем сверки его номера с серийными номерами аннулированных сертификатов в CRL. Существует несколько методов организации CRL, включая использование директориального сервиса, веб-сервиса, специально создаваемых баз данных. Модель PKIX рекомендует использовать директориальный сервис и протокол LDAP для доступа к директориям.

С целью описания процедур взаимодействия основных компонентов ИОК в модели PKIX описаны несколько групп *протоколов*: административные, операционные и статусные (табл. 4).

Таблица 4. **Основные протоколы ИОК согласно модели PKIX**

Тип протоколов	Назначение	Выполняемые функции	Стандарты
Административные	Обеспечение базовых взаимодействий между компонентами ИОК в режиме реального времени: между пользователями и УЦ (RA), между УЦ и RA, между различными УЦ	Начальная регистрация и сертификация открытых ключей пользователей, восстановление и обновление ключевой пары, обновление сертификата, обработка запросов на аннулирование сертификатов, кросс-сертификация	**RFC 2510** – Internet X.509 PKI Certificate Management Protocols (CMP), **RFC 2511** – Internet X.509 PKI Certificate request message format
Операционные	Доступ к информации, связанной с функционированием ИОК: сертификатам в формате X.509 и CRL, хранящимся в CR	Чтение из репозитория, поиск в репозитории, модификация репозитория (изменение данных, добавление и удаление сертификатов)	**RFC 2559** – Internet X.509 Public Key Infrastructure Operational Protocols: LDAP v2, **RFC 2585** — Internet X.509 Public Key Infrastructure Operational Protocols: FTP & HTTP
Статусные	Получение сведений о текущем состоянии (статусе) сертификата (при более жестких операционных требованиях или более своевременно, чем это возможно с CRL)	Выдача по запросу данных, записанных в полях сертификата, без привлечения CRL	**RFC 2560** — X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP

В качестве стандарта по операционным протоколам используется RFC 2559 в том случае, если репозиторий реализован в виде директории, и RFC 2585 в том случае, если он является веб-сайтом. Статусный протокол OCSP является альтернативным по отношению к спискам аннулированных сертификатов методом получения субъектами ИОК информации об аннулировании (т.е. о статусе) цифровых сертификатов. Этот метод предлагается применять для тех прикладных программ, для которых разница во времени между очередными опубликованиями списков аннулированных сертификатов неприемлема. Субъект всегда может узнать статус интересующего его сертификата, выполнив этот протокол с репозиторием сертификатов.

Инфраструктура открытых ключей основывается на доверии всех субъектов ИОК к УЦ. С целью усиления защищенности УЦ должны быть предприняты дополнительные меры, в том числе наличие *средств аудита*, позволяющих отслеживать события, угрожающие безопасности системы.

Для нормального функционирования инфраструктуры открытых ключей в модели PKIX предусмотрено наличие в распределенной среде дополнительных компонентов поддержки, а именно:

- директориального сервиса;
- средств обеспечения качества сервиса доставки сертификатов и списков аннулированных сертификатов;
- криптографической аппаратуры, защищенной от "взлома" злоумышленником;
- интеллектуальных (пластиковых) карт;
- прикладных программ и протоколов прикладного уровня, поддерживающих операции ИОК;
- политик безопасности, поддерживающих использование ИОК и нуждающихся в ИОК.

Основным стандартом, посвященным вопросам реализации посредством ИОК политики безопасности информационной системы, является стандарт RFC 2527 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Политики безопасности имеют результатом процессы, которые должны быть правильно реализованы. Процессы описывают пути использования ИОК администраторами и пользователями. Процессы

могут включать следующие основные варианты использования цифровых сертификатов:

- выпуск, запрос, распространение и аннулирование сертификатов (базовую функциональность ИОК);
- использование сертификатов для аутентификации клиентов;
- использование сертификатов для обеспечения безопасности электронной почты;
- использование сертификатов для обмена данными между организациями;
- процедуры, которым необходимо следовать при обнаружении фактов нарушения безопасности системы;
- создание руководств по управлению секретными криптографическими ключами и сертификатами открытых ключей;
- процедуры и технологии разработки прикладных программ, использующих услуги ИОК (таких, как программы аутентификации пользователей с использованием сертификатов).

Для более подробного знакомства с моделью PKIX целесообразно обратиться к первоисточникам – указанным выше документам серии RFC, которые опубликованы в сети Internet на страницах международной организации IETF по адресу http://www.ietf.org.

Модель PKIX является не единственным стандартом де-факто, получившим распространение на практике. Довольно часто используются также стандарты группы PKCS, разработанные фирмой RSA Laboratories. Ознакомиться с ними можно на сайте этой фирмы по адресу http://www.rsasecurity.com.

3.5. Закон Российской Федерации "Об электронной цифровой подписи"

Рассмотренные до сих пор модели организации ИОК, в том числе на основе применения метода сертификации открытых ключей, описывают техническую сторону процесса управления ключами. На практике существенное значение имеют правовые вопросы регулирования деятельности, связанной с управлением ключами в сложных информационных системах, таких как виртуальные частные сети.

В Российской Федерации основным документом, регулирующим правовые аспекты деятельности, связанной с задачами управления ключами и функционированием УЦ, является Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи" [15]. Целью этого закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной (традиционной) подписи в документе на бумажном носителе. Его действие распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

Закон выделяет два вида информационных систем, в которых может иметь место деятельность, связанная с поддержанием ИОК: информационные системы общего пользования и корпоративные информационные системы. Под информационной системой общего пользования понимается "информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано". Корпоративная информационная система, согласно определению, данному в законе, — это "информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы".

Закон определяет условия использования ЭЦП, давая юридическую трактовку понятий и условий, возникающих при использовании ИОК. Так, ЭЦП признается равнозначной собственноручной подписи при соблюдении следующих трех условий:

- сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность ЭЦП в электронном документе;
- ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Обязательным условием использования средств ЭЦП в информационных системах общего пользования в Российской Федерации является применение только сертифицированных средств ЭЦП. Возмещение убытков, причиненных в связи с созданием ключей ЭЦП несертифицированными средствами ЭЦП, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством Российской Федерации. Согласно закону, использование несертифицированных средств ЭЦП и созданных ими ключей ЭЦП в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается. Сертификация средств ЭЦП осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг.

Закон определяет состав информации, которая в обязательном порядке должна заноситься в сертификат открытого ключа. Это уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре УЦ, фамилия, имя и отчество владельца сертификата ключа подписи или его псевдоним, открытый ключ электронной цифровой подписи, наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи, наименование и место нахождения УЦ, выдавшего сертификат ключа подписи, сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение. Определяются также порядок проверки сертификата, при котором он признается действительным, сроки архивного хранения сертификатов ключей подписи с целью разрешения возможных конфликтных ситуаций, связанных с принадлежностью ЭЦП.

В законе "Об электронной цифровой подписи" также изложены правовые основы деятельности УЦ. Так, определяется статус УЦ.

- УЦ, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные законом "Об электронной цифровой подписи". При этом УЦ

должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

- Статус УЦ, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы.

Деятельность УЦ подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности.

В законе "Об электронной цифровой подписи" детально изложены права и обязанности УЦ, порядок выдачи им сертификатов ключей подписи, отношения между УЦ и уполномоченными федеральными органами исполнительной власти РФ, обязательства УЦ по отношению к владельцу сертификата ключа подписи, обязательства владельца сертификата ключа подписи. Описаны порядок приостановления действия и аннулирования ключа цифровой подписи. Определяется возможность и описывается порядок прекращения действия УЦ на территории Российской Федерации.

Особая часть закона посвящена особенностям использования ЭЦП в Российской Федерации. Отдельные статьи закона посвящены использованию ЭЦП в сфере государственного управления, в корпоративных информационных системах, вопросам признания иностранных сертификатов ключей ЭЦП, а также случаям, когда ЭЦП может замещать собственноручные подписи на документах, заверенных печатями организаций.

Следует помнить о различиях между нормативно-техническими документами международных организаций (рассмотренными в пп. 3.2 – 3.4) и законодательными актами. Закон "Об электронной цифровой подписи" регулирует правоотношения, возникающие при создании и деятельности УЦ только в целях обеспечения возможности использования ЭЦП и организации электронного документооборота. Нормативные технические модели международных организаций, с одной стороны, не ограничивают возможности использования УЦ

для той или иной конкретной цели (наряду с открытыми ключами ЭЦП УЦ мог бы заверять и любые другие ключи, необходимые для использования в защищенных коммуникационных протоколах любого уровня, не ограничиваясь только задачами электронного документооборота), но с другой стороны, не могут давать никаких юридических гарантий использования таких УЦ. В отличие от них закон формулирует правовые основы деятельности УЦ в Российской Федерации, но только в части, связанной с использованием ЭЦП в электронных документах.

Контрольные вопросы по разделу 3

1. Что понимается под термином управление криптографическими ключами? Какова основная цель и основные задачи управления ключами?
2. Что такое жизненный цикл ключа? Каковы его основные стадии?
3. В каких состояниях пребывают криптографические ключи за время своего жизненного цикла? При каких условиях происходят переходы из одного состояния в другое?
4. В чем отличие жизненного цикла секретных и открытых криптографических ключей?
5. Что такое инфраструктура открытых ключей? Какова ее логическая и физическая структура?
6. Какие основные *логические модели* инфраструктуры открытых ключей разработаны международными организациями? В чем заключаются их особенности?
7. Каковы перспективы практического применения концепции инфраструктуры открытых ключей?
8. Каковы основные способы распространения открытых ключей в криптосистемах?
9. Изложите в общих чертах существо метода сертификации открытых ключей. В чем заключаются преимущества и недостатки этого метода?
10. В чем различие между идентификационными и атрибутными сертификатами?
11. Какие основные стандарты, описывающие форматы сертификатов и списков аннулированных сертификатов, разработаны и приняты международными организациями?
12. Каковы основные элементы *модели инфраструктуры* открытых ключей PKIX?

13. Какие способы хранения сертификатов и списков аннулированных сертификатов Вам известны? Какие из них рекомендованы моделью PKIX?
14. Какие основные группы протоколов используются в инфраструктуре открытых ключей согласно модели PKIX?
15. Наличие каких дополнительных компонентов предполагается моделью PKIX для обеспечения нормального функционирования инфраструктуры открытых ключей?
16. Каковы особенности российского законодательства в сфере организации инфраструктуры открытых ключей и регулирования деятельности удостоверяющих центров?

4. ПОСТРОЕНИЕ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

Выбор решения для организации определяется тремя факторами: размером сети, техническими навыками, которыми обладают сотрудники организации, и объемом трафика, который планируется обрабатывать. Процесс шифрования данных требует существенных вычислительных ресурсов и может перегрузить компьютер, когда несколько VPN-соединений одновременно участвуют в передаче данных. В этом случае, чтобы разгрузить центральный процессор, возможно, придется установить специальные ускорительные платы.

Какой бы путь ни был выбран, все равно придется столкнуться с проблемой управления VPN-устройствами и поддержания согласованных правил безопасности для VPN и МЭ в масштабах всей организации. В этой области успех или неудача в очень значительной степени зависят от квалификации персонала ИТ-службы.

4.1. Требования к продуктам построения виртуальных частных сетей

При корпоративном применении продукты VPN, независимо от способа их реализации, должны удовлетворять некоторым базовым требованиям. Эти продукты выполняют крайне ответственные для предприятия функции, что предъявляет высокие требования к *надежности защиты* и *производительности* таких устройств. Продукты VPN для образования защищенных каналов взаимодействуют с аналогичными продуктами, установленными в сетях данного предприятия или предприятий-партнеров, поэтому для них особенно важна *совместимость* и *поддержка стандартных протоколов VPN.*

Для обеспечения корректной работы VPN-продуктов необходимо проведение большого объема работ по конфигурированию и администрированию. Отсюда вытекают требования к поддержке продуктами VPN *централизованной справочной службы* и *средств управления.*

При выборе средств построения VPN необходимо учитывать такие характеристики этих средств, как функциональная полнота и гибкость.

1. Производительность. Основными операциями средств VPN являются шифрование по различным алгоритмам и аутентификация, которая, в свою очередь, также использует шифрование. Шифрование требует значительных вычислительных ресурсов. На рис. 36 приведены (по данным VPNet Technologies, www.vpnet.com) относительные вычислительные затраты на шифрование по алгоритмам DES и Triple DES, аутентификацию пакетов с использованием хэширования, а также затраты на выполнение операций маршрутизации и фильтрации пакетов.

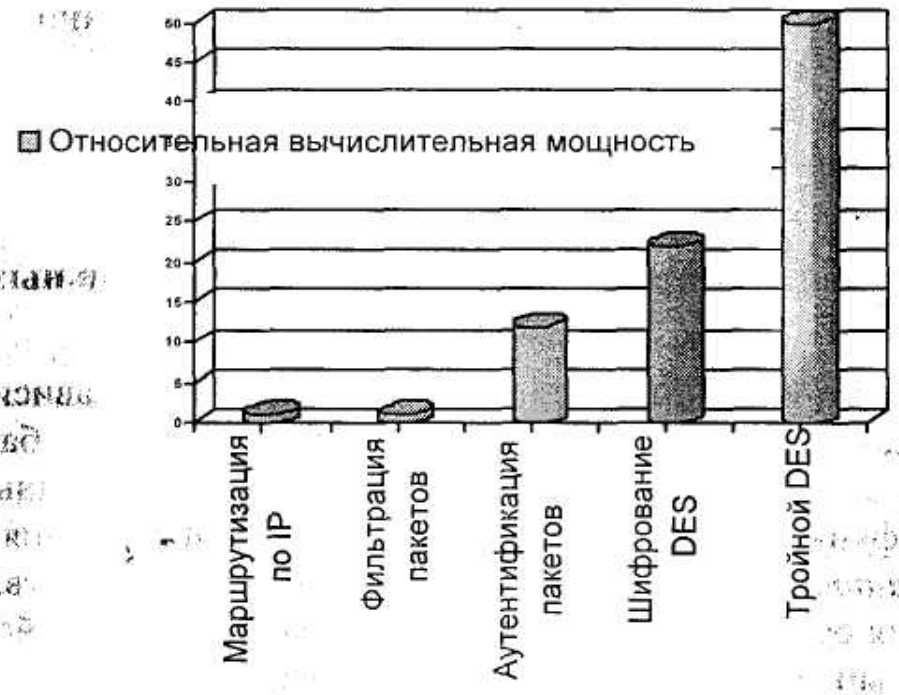


Рис. 36. Относительная вычислительная мощность для выполнения основных операций маршрутизатора, МЭ и устройства VPN

Данные, приведенные на рисунке, объясняют, почему большинство VPN-продуктов, выполненных на основе маршрутизатора или МЭ, а также ПО персонального компьютера обладают низкой производительностью (чаще всего — ниже 10 Мбит/с). Для получения производительности порядка 100 Мбит/с необходимы аппаратные решения, которые используют специальные процессоры для выполнения операции шифрования.

При выборе средств создания VPN следует учитывать, что шифрование требует значительных вычислительных ресурсов. Например, обычные серверы класса Pentium имеют достаточную производительность шифрования для заполнения канала на 10 Мбит/с, но не 100 Мбит/с. Для обеспечения высокой скорости шифрования некоторые производители предлагают специальные аппаратные дополнения к платформе общего назначения. Однако использование специализированных аппаратных устройств снижает гибкость средств построения защищенных туннелей. Поэтому наиболее перспективным решением является реализация алгоритмов скоростной криптозащиты.

Все задержки, возникающие при криптографической обработке трафика, можно разделить на три типа.

- Задержки при установлении защищенного соединения между VPN-устройствами.
- Задержки, связанные с зашифрованием и расшифрованием защищаемых данных, а также преобразованиями, необходимыми для контроля их целостности.
- Задержки, связанные с добавлением нового заголовка к передаваемым пакетам.

Реализация трех видов VPN предусматривает установление защищенных соединений не между абонентами сети, а только между VPN-устройствами. С учетом криптографической стойкости используемых алгоритмов смена ключа возможна через достаточно длительный интервал времени. Поэтому задержки первого типа на скорость обмена данными при использовании средств построения VPN практически не влияют. Разумеется, этот тезис касается стойких алгоритмов шифрования, использующих ключи не менее 128 бит

(Triple DES, ГОСТ 28147-89 и т.д.). Устройства, использующие стандарт DES, могут вносить определенные задержки в работу сети.

Задержки второго типа начинают играть роль только при передаче данных по высокоскоростным каналам (от 10 Мбит/с). Во всех остальных случаях быстродействие программной или аппаратной реализации выбранных алгоритмов шифрования и контроля целостности обычно достаточно велико и в цепочке операций "шифрование пакета — передача пакета в сеть" и "прием пакетов из сети — расшифрование пакета" время зашифрования (расшифрования) значительно меньше времени, необходимого для передачи данного пакета в сеть.

Основная проблема связана с добавлением дополнительного заголовка к каждому пакету, пропускаемому через VPN-устройство.

В качестве примера, рассмотрим систему диспетчерского управления, которая осуществляет обмен данными в реальном масштабе времени между удаленными станциями и центральным пунктом. Размер передаваемых данных не велик — не более 25 байтов. Данные сопоставимого размера передаются в банковской сфере (платежные поручения) и в IP-телефонии. Интенсивность передаваемых данных — 50—100 переменных в секунду. Взаимодействие между узлами осуществляется по каналам с пропускной способностью в 64 кбит/с.

Пакет со значением одной переменной процесса имеет длину 25 байтов (имя переменной — 16 байтов, значение переменной — 8 байтов, служебный заголовок — 1 байт). IP-протокол добавляет к длине пакета еще 24 байта (заголовок IP-пакета). При использовании в качестве среды передачи каналов FR добавляется еще 10 байтов заголовка. Всего — 59 байтов (472 бита). Таким образом, для передачи 750 значений переменных процесса за 10 с (75 пакетов в секунду) необходима полоса пропускания 75 x 472 = 34,5 кбит/с, что нормально вписывается в имеющиеся ограничения пропускной способности в 64 кбит/с.

Теперь посмотрим, как ведет себя сеть при включении в нее средства построения VPN.

Первый пример — средства на основе протокола SKIP. К 59 байтам данных добавляется 112 байтов дополнительного заголовка (для

ГОСТ 28148-89), что составит 171 байт (1368 бит). 75 х 1368 = 102,6 кбит/с, что на 60 % превышает максимальную пропускную способность имеющегося канал связи.

Для протокола IPSec и вышеуказанных параметров пропускная способность будет превышена на 6 % (67,8 кбит/с). Это при условии, что дополнительный заголовок для алгоритма ГОСТ 28147-89 составит 54 байта. Для протокола, используемого в российском программно-аппаратном комплексе "Континент-К" дополнительный заголовок, добавляемый к каждому пакету, составляет всего 36 байтов (или 26 — в зависимости от режима работы), что не приводит к снижению пропускной способности (57 и 51 кбит/с соответственно).

2. *Управляемость.* Многие поставщики VPN-продуктов разрабатывают утилиты управления, которые имеют графический интерфейс "клиент-сервер" или Web-интерфейс для конфигурирования и администрирования своих VPN-устройств.

Управляющие программы могут поддерживать администрирование одного или сразу нескольких VPN-устройств. Для целей управления в некоторых VPN-продуктах поддерживаются различные уровни привилегий (например, один администратор имеет право только просматривать параметры политики безопасности, поэтому ему даются права read only, а другой должен их изменять, соответственно ему даются права write и т.п.). Для срочного вмешательства в работу аппаратного VPN-устройства обычно предусматривается консольный порт. Обновление ПО VPN-устройства также может происходить с использованием этих утилит управления.

Очень важно, чтобы при управлении VPN-устройством через публичную сеть протокол управления мог работать через защищенный канал, поскольку при управлении передаются такие важные данные, как пароли или секретные ключи.

К сожалению, не существует общего интерфейса управления VPN-продуктами. Поэтому если предприятие использует в некоторых филиалах продукты разных производителей, то для централизованного управления ими нужно поддерживать несколько консолей управления.

Отдельной задачей администрирования является инсталляция и конфигурирование ПО VPN-клиента на компьютерах удаленных пользователей. Обычно такой клиент модифицирует сетевое ядро ОС персонального компьютера для добавления функций VPN (например, добавления протокола IPSec), а модификация сетевого ядра ОС представляет собой сложную задачу, особенно для рядового пользователя. Многие инсталляции требуют обновления существующего сервиса удаленного доступа (Dial-up Networking) и транспортных уровней ОС.

Аудит представляет собой одну из важных составляющих системы администрирования. Однако многие VPN-устройства пока недостаточно поддерживают базовые функции аудита, состоящие в протоколировании событий и рассылке предупреждений при возникновении нештатных ситуаций. Так как большинство VPN-устройств не используют дисковую память, то они обычно посылают данные аудита на сервер, ведущий системный журнал. Проблема здесь в том, что у такого сервера может не хватить интеллекта для сортировки предупреждений, которые могут варьироваться в широких пределах: от неудачных аутентификаций до системных ошибок или обнаружения вторжения.

3. Совместимость. Очевидно, что построение крупной VPN на продуктах одного производителя весьма проблематично. Особенно, если VPN строится для экстрасети нескольких предприятий-партнеров. Все это делает совместимость VPN-продуктов одним из важнейших требований, предъявляемых к ним.

Наиболее очевидный путь достижения совместимости продуктов — следование открытым стандартам на основные компоненты VPN. Задача обеспечения совместимости осложняется тем, что стандарты VPN образуют достаточно большое семейство, которое к тому же допускает использование необязательных расширений. Поясним проблему совместимости на примере стандарта VPN IPSec. Большинство специалистов сходятся во мнении, что добиваться совместимости VPN-продуктов следует именно на его основе. В последнее время широкомасштабное применение этого протокола в проекте ANX (Automotive Network Exchange) сделало IPSec явным лидером в области создания защищенных каналов. Рабочая группа автомо-

бильной промышленности AIAG, состоящая из General Motors, Ford, Crysler и их поставщиков и бизнес-партнеров, инициировала проект ANX. Это было сделано для переноса их интенсивного трафика электронного обмена данными с более дорогих частных сетей, построенных на основе выделенных линий, и систем удаленного доступа по телефонной сети на VPN, использующую Internet.

Однако оказалось, что недостаточно взять два произвольных VPN-продукта, которые удовлетворяют спецификациям IPSec, чтобы гарантировать их совместную работу. Поскольку IPSec — это набор протоколов, может случиться так, что по одному протоколу совместимость соблюдается, а по другому — нет. Кроме того, каждый член семейства IPSec представляет собой открытый и расширяемый стандарт, так что разные производители могут использовать свои варианты расширения (например, поддерживать помимо хэш-функций MD5 и SHA, обязательных для реализации в IPSec, еще и хэш-функцию RC4, которую не поддерживает другой производитель).

Для гарантий совместимости разработчики стандартов IPSec предусмотрели обязательный набор функций и алгоритмов для каждого протокола, чтобы взаимодействующие стороны нашли общие параметры для совместной работы. Но и тут пользователя могут поджидать неприятности. Например, в тестировании VPN-продуктов, предпринятом журналом Data Communications (Июнь 1999, *IPSec, Johan Allard и Svante Nygren),* была в целом обнаружена хорошая совместимость многих VPN-шлюзов при работе по протоколу IPSec. Однако брандмауэр Firewall-1 компании Check Point Software не смог установить защищенные каналы в режиме "шлюз—шлюз" с продуктами других достаточно известных производителей, таких, как Axent Technologies, Cisco Systems, Data Fellows, IBM, Intel Network Systems (ранее Shiva Corp.), Northern Telecom (Nortel), Radguard, 3Com и Timestep. Специалисты, проводившие тестирование, выяснили, что проблема заключалась в различном использовании защищенных каналов при защите подсети за шлюзом. Firewall-1 соглашался устанавливать с другими продуктами только индивидуальные каналы для каждого хоста подсети и отказывался использовать один канал для всей подсети. Спецификации же IPSec позволя-

ют использовать защищенный канал как для индивидуального IP-адреса, так и для диапазона IP-адресов, но не детализируют рекомендации по использованию того или иного режима. Поэтому выявленная при тестировании проблема весьма характерна — разные производители по-разному используют возможности стандарта.

Для устранения проблем несовместимости организация ICSA Inc. проводит масштабную сертификацию VPN-продуктов для работы в сети ANX (http://www.icsa.org). Уже проведена сертификация 13 продуктов от 9 поставщиков на так называемый уровень сертификации ANX 1.0, который включает тестирование на общую функциональность, совместимость с другими IPSec-продуктами, функции управления ключами и работу с цифровыми сертификатами. Результатами сертификации ICSA можно воспользоваться при выборе VPN-продуктов для своей интрасети или при построении экстрасети с бизнес-партнерами.

Стандарты IPSec сегодня являются основным механизмом обеспечения совместимости VPN-продуктов разных производителей. Можно, конечно, добиться совместимости и по другим протоколам (например, PPTP или SSL), но сейчас уже ясно, что будущее при построении масштабных VPN принадлежит IPSec, а термин IPSec-совместимый становится синонимом стандартный.

4. Поддержка справочной службы. Технология построения VPN основана на аутентификации пользователей и криптозащите информации. Наиболее высокая эффективность выполнения данных функций обеспечивается при комплексном использовании асимметричных и симметричных криптосистем. Комплексное применение симметричных шифров и схем шифрования с открытым ключом обеспечивается в протоколах туннелирования IPSec и SSL/TLS, которые предполагают наличие ИОК. Данная инфраструктура, обеспечивающая управление открытыми ключами и аутентификацию пользователей на основе цифровых сертификатов, будет приобретать все большую значимость. Сегодня существует четкая тенденция использования единой справочной службы для хранения в ней не только учетных данных пользователей и компьютеров (именно с этого начинались все современные справочные службы, такие как NDS (Novell Directory Services) компании Novell, Directory Services ком-

пании Microsoft, Street Talk компании Banyan), но и всех параметров сети, в том числе параметров политики безопасности предприятия — паролей, секретных ключей и т.п. Создание новых каталогов для хранения такой информации потребует дополнительных издержек. Использование одной службы каталогов, управляющей всей служебной информацией в компьютерной сети, позволяет существенно повысить эффективность администрирования сети и работы конечных пользователей. В центральном каталоге, способном полностью взаимодействовать с другими каталогами и приложениями, должны храниться не только данные, имеющие отношение к политике защиты, но и информация для управления производительностью и выделения вычислительных ресурсов.

На основе справочной службы работает и инфраструктура ИОК, которую может использовать протокол обмена ключами IKE, работающий в IPSec. Ввиду отсутствия общепринятого стандарта на справочную службу основой для совместимости сегодня является протокол доступа к данным, хранящимся в справочной службе — упрощенного протокола доступа к каталогу (Lightweight Directory Access Protocol, LDAP). Поэтому продукты VPN, поддерживающие LDAP, считаются перспективней продуктов, не обладающих такой поддержкой. Взаимодействие с сервером политики по протоколу LDAP позволяет администратору сети достаточно просто задавать признаки, в зависимости от которых шлюз решает, какой трафик следует шифровать, какой пересылать без шифрования, а какой — просто блокировать. Провайдер может хранить в сервере политики данные безопасности, полученные от администраторов предприятий-клиентов сервиса VPN, и шлюз будет легко их отрабатывать. Наличие средств защищенного удаленного управления шлюзом позволит провайдеру отдать такой шлюз в аренду своему клиенту, но не терять над ним контроль и выполнять ежедневное обслуживание без необходимости отправлять на предприятие своих специалистов.

5. Надежность защиты и функциональная полнота. Надежность защиты и функциональная полнота VPN-продукта зависит от мощности и разнообразия методов защиты, протоколов и используемых в них алгоритмов и режимов, а также от длины ключей шифрования. Естественно, все эти свойства будут полезны потреби-

телю только в том случае, если они качественно реализованы в поставляемом продукте.

Надежность защиты и функциональная полнота могут быть оценены теоретически — путем анализа используемых в продукте стандартов, протоколов, алгоритмов и ключей. Качество реализации можно проверить только экспериментальным путем — длительной эксплуатацией и всесторонним тестированием продукта.

Для высоконадежной защиты обычно применяют алгоритм шифрования Triple DES и асимметричные методы.

Функциональная полнота VPN-продуктов заключается в поддержке базовых алгоритмов создания защищенных каналов. Это шифрование по DES, Triple DES и аутентификация с использованием зависящих от ключа хэш-функций MD5 и SHA-1, а также поддержка ИОК на основе цифровых сертификатов и справочной службы с протоколом доступа LDAP. Кроме того, чем больше разнообразных новых алгоритмов шифрования поддерживает продукт, тем лучше, так как использование незнакомого алгоритма шифрования повышает степень защиты передаваемых данных.

Так как система IPSec поддерживает все базовые алгоритмы шифрования и аутентификации, может работать с ИОК (хотя такой режим не является обязательным для IPSec-продуктов), а также позволяет легко встраивать новые алгоритмы и протоколы, то считается, что поддержка IPSec является признаком функциональной зрелости продукта.

Более ограниченное применение отводится продуктам, поддерживающим только протокол защищенного канала PPTP. Этот протокол позволяет создавать защищенный канал на основе алгоритма шифрования DES, но не поддерживает Triple DES, ИОК, не является открытым, и не позволяет легко наращивать свои функции за счет включения новых алгоритмов шифрования.

Наделение VPN-продукта функциями МЭ или маршрутизатора существенно повышает его функциональную полноту. Это добавляет к функциям защиты данных при передаче мощные средства контроля доступа к внутренним ресурсам сети, а также средства защиты от внешних атак. И если такое совмещение функций не вредит про-

изводительности устройства, то оно может только приветствоваться потребителями.

4.2. Варианты реализации

Производители предлагают разнообразные схемы организации VPN: на базе чисто аппаратных решений, программно-аппаратных комплексов, либо полностью программные реализации [1].

1. В виде ***программного решения***, устанавливаемого на обычный компьютер, функционирующий, как правило, под управлением ОС Unix. Российские разработчики полюбили ОС FreeBSD и именно на ее базе построены отечественные решения "Континент-К" и "Шип". Для ускорения обработки трафика могут быть использованы специальные аппаратные ускорители, заменяющие функции программного шифрования. Так же в виде программного решения реализуется абонентские пункты, предназначенные для подключения к защищаемой сети удаленных и мобильных пользователей.

Программное решение для VPN — это, как правило, готовое приложение, которое устанавливается на подключенном к сети компьютере со стандартной ОС. Из соображений защиты и производительности для установки VPN-приложений лучше всего выделять отдельные машины, которые должны устанавливаться на всех концах соединения. Ряд производителей (Axent Technologies, Check Point Software Technologies и NetGuard) поставляет VPN-пакеты, которые легко интегрируются с программными МЭ и работают на различных ОС, включая Windows NT/2000, Sun Solaris и Linux.

Поскольку для построения VPN на базе специализированного ПО требуется создание отдельной компьютерной системы, такие решения обычно сложнее для развертывания, чем аппаратные. Создание подобной системы предусматривает конфигурирование сервера для распознавания данного компьютера и его ОС, VPN-пакета, сетевых плат для каждого соединения и специальных плат для ускорения операций шифрования. Такая работа в ряде случаев может оказаться затруднительной даже для опытных специалистов.

С другой стороны, программные решения для VPN стоят относительно недорого. В зависимости от размера сети можно приобре-

сти VPN-пакет за сумму от 2000 до 25000 долл. без стоимости оборудования, локальных соединений и времени, которое ИТ-персонал или консультанты должны будут потратить на установку и обслуживание системы.

2. В виде ***специализированного программно-аппаратного обеспечения***, предназначенного именно для решения задач VPN. Такие устройства могут применяться в тех случаях, когда необходимо обеспечить защищенный доступ большого числа абонентов.

Аппаратные VPN-решения включают в себя все, что необходимо для соединения — компьютер, частную (как правило) ОС и специальное ПО. Ряд компаний, в том числе Cisco Systems, NetScreen и Sonic, предлагает целый спектр решений, которые могут масштабироваться в зависимости от количества одновременных VPN-соединений, с которыми предполагается работать, и ожидаемого объема трафика. Примером такого решения является российский комплекс "Континент-К".

Развертывать программно-аппаратные решения, безусловно, легче. Они включают в себя все, что необходимо для конкретных условий, поэтому время, за которое их можно запустить, исчисляется минутами или часами. Еще одним серьезным преимуществом этих VPN-решений является гораздо более высокая производительность и более высокая по сравнению с другими решениями защищенность. В них используются специальные печатные платы и ОС, оптимизированные под данную задачу и освобожденные от необходимости поддерживать какие-либо избыточные функции, которые содержатся в универсальных ОС.

К минусам можно отнести их высокую стоимость. Целесообразно ориентироваться на диапазон цен от 10000 долл. за устройство для удаленного офиса до сотен тысяч долларов за VPN-концентратор уровня предприятия.

Недостаток таких решений состоит и в том, что управляются они отдельно от других решений по безопасности, что усложняет задачу администрирования инфраструктуры безопасности. На первое место эта проблема выходит при построении крупной и территориально-распределенной сети, насчитывающей десятки устройств построения VPN.

3. ***Интегрированные решения***, в которых функции построения VPN реализуются наряду с функцией фильтрации сетевого трафика, обеспечения качества обслуживания или распределения полосы пропускания. Основные преимущества такого решения — централизованное управление всеми компонентами с единой консоли и более низкая стоимость в расчете на каждый компонент по сравнению с тем, когда такие компоненты приобретаются отдельно. Самым известным примером такого интегрированного решения является VPN-1 от компании Check Point Software, включающий в себя помимо VPN-модуля модуль, реализующий функции МЭ, модуль, отвечающий за балансировку нагрузки, распределение полосы пропускания и т.д. Этот продукт имеет сертификат Гостехкомиссии РФ.

4.3. Шлюзы и клиенты

VPN отличают друг от друга многие характеристики: набор функциональных возможностей, точки размещения VPN-устройств, тип платформы, на которой эти средства работают, применяемые протоколы шифрования и аутентификации. Облик VPN во многом определяется типом примененных VPN-устройств. Устройства VPN могут играть роль шлюза или клиента (рис. 37).

Шлюз VPN — это сетевое устройство, подключенное к нескольким сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов позади него. Размещение шлюза VPN должно быть аналогично размещению МЭ, т.е. таким, чтобы через него проходил весь трафик, предназначенный для внутренней КС. (Если в сети имеется и МЭ, и VPN-шлюз, то их относительное расположение представляет собой нетривиальную задачу, требующую особого рассмотрения.) Сетевое соединение VPN прозрачно для пользователей позади шлюза — оно представляется им выделенной линией, хотя в действительности прокладывается через сеть с коммутацией пакетов.

В зависимости от стратегии безопасности предприятия исходящие пакеты либо шифруются, либо посылаются в открытом виде, либо блокируются шлюзом. Для входящих туннелируемых пакетов

внешний адрес является адресом VPN-шлюза, а внутренний адрес — адресом некоторого хоста позади шлюза.

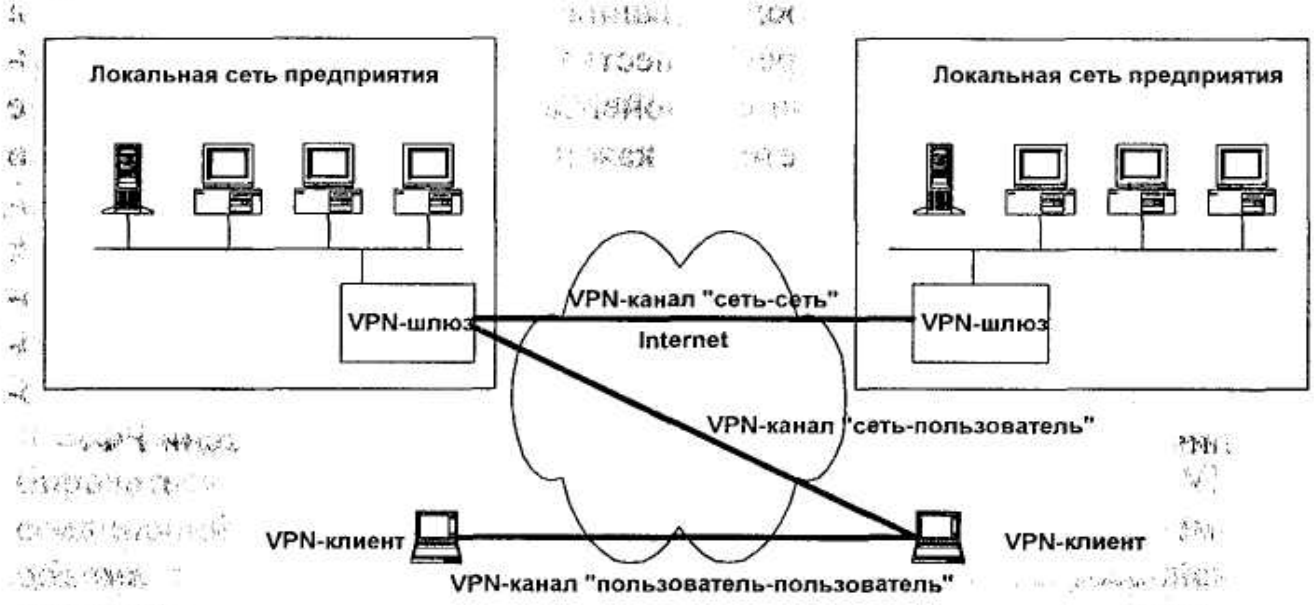


Рис. 37. Шлюзы и клиенты VPN

Шлюз VPN может быть реализован несколькими способами, т.е. в виде отдельного аппаратного устройства, отдельного программного решения, а также в виде МЭ или маршрутизатора, дополненных функциями VPN.

Клиент VPN — это программный или программно-аппаратный комплекс, обычно на базе персонального компьютера. Его сетевое транспортное обеспечение модифицировано для выполнения шифрования и аутентификации трафика, которым устройство обменивается с шлюзами VPN и/или другими VPN-клиентами. Ввиду стоимостных ограничений реализация VPN-клиента чаще всего представляет собой программное решение, дополняющее стандартную ОС, например, Windows 98 или Unix.

Для создания VPN крупного предприятия нужны как VPN-шлюзы, так и VPN-клиенты. Шлюзы целесообразно использовать для защиты ЛВС предприятия, а VPN-клиенты— для удаленных и мобильных пользователей, которым требуется устанавливать соединения с КС через Internet. В том случае, когда организацию VPN берет на себя провайдер, вся VPN может быть построена на его

шлюзах, прозрачно для сетей и удаленных пользователей предприятия.

Выделяют VPN-продукты нескольких типов: выделенные аппаратные VPN-шлюзы, выделенные программные VPN-шлюзы, программные VPN-клиенты.

4.4. Решения для построения виртуальных частных сетей

В реальности приходится строить VPN на базе следующих решений [7, 11, 12]:

- VPN на базе сетевых ОС;
- VPN на базе маршрутизаторов;
- VPN на базе МЭ;
- VPN на базе специализированного ПО;
- VPN на базе аппаратных средств.

Каждое из названных решений имеет свои достоинства и недостатки, которые будут рассмотрены на примере наиболее часто встречающихся в России VPN-продуктов.

Протоколы построения VNP могут быть реализованы сетевыми средствами различных категорий:

- серверами удаленного доступа, позволяющими создавать защищенные туннели на канальном уровне эталонной модели сетевого взаимодействия (модели OSI);
- маршрутизаторами, которые могут поддерживать протоколы создания защищенных виртуальных сетей на канальном и сетевом уровне модели OSI;
- МЭ, возможно включающими в свой состав серверы удаленного доступа и позволяющими создавать VPN как на канальном и сетевом, так и на сеансовом уровне модели OSI;
- автономным ПО, позволяющим создавать защищенные виртуальные сети в основном на сетевом и сеансовом уровне модели OSI;
- отдельными специализированными аппаратными средствами на основе специализированной ОС реального времени, имеющими два или более сетевых интерфейса и аппаратную криптографическую поддержку — так называемый "черный ящик VPN" *(VPN*

black box) и ориентированными на формирование защищенных туннелей на канальном и сетевом уровне модели OSI;

- комбинированными пограничными устройствами, которые включают в себя функции маршрутизатора, МЭ, средства управления пропускной способностью и функции VPN.

Серверы удаленного доступа (RAS) могут включать функции создания защищенных туннелей при удаленном доступе пользователей к ЛВС. Эти серверы чаще всего поддерживают протоколы туннелирования PPTP, L2F и L2TP, соответствующие канальному уровню модели OSI. Следует учесть, что не все поставщики RAS, позволяющих формировать защищенные туннели с удаленными компьютерами, предлагают соответствующее клиентское ПО. Поэтому, учитывая, что в качестве ОС, наиболее часто используемых на компьютерах удаленных пользователей, выступают Windows 95/98/NT, целесообразно выбирать RAS, поддерживающие протокол PPTP. Данный протокол входит в состав Windows 98/NT. Существует также немало автономных программных средств удаленного доступа, реализующих PPTP для Windows 95. В ближайшее время ожидается переориентация средств удаленного доступа на более совершенный протокол туннелирования L2TP, который, например, реализован в Windows 2000 (NT 5.0).

Маршрутизаторы могут поддерживать функции формирования защищенных туннелей по умолчанию или в качестве дополнительной возможности, предлагаемой за отдельную плату. Эти устройства чаще всего ориентируются на создание VPN по протоколам L2F, L2TP и IPSec, соответствующим канальному и сетевому уровням модели OSI. При выборе маршрутизатора в качестве средства создания VPN необходимо обратить внимание на его производительность и загрузку. Если процессор маршрутизатора работает с 80-процентной загрузкой без выполнения функций VPN, то добавление большого числа защищенных туннелей ухудшит прохождение всего трафика.

В качестве эффективных средств построения VPN выступают МЭ, которые могут включать в свой состав и RAS. Учитывая, что МЭ специально предназначены для защиты информационного взаимодействия с открытыми сетями, можно сделать вывод, что при

реализации этими устройствами и функций создания VPN обеспечивается комплексная защита информационного обмена. МЭ могут поддерживать любые существующие протоколы построения защищенных туннелей. На канальном уровне модели OSI могут быть реализованы протоколы PPTP, L2F и L2TP, на сетевом уровне — IPSec и SKIP, а на сеансовом — SSL/TLS и SOCKS.

Важной особенностью МЭ как средств построения VPN является возможность контроля не только открытого, но и криптозащищенного трафика. Контроль доступа со стороны МЭ ко всему трафику, в том числе и туннелируемому, обеспечивает более высокую защиту межсетевого взаимодействия. Такой контроль особенно эффективен, если другую сторону туннеля представляет объект, стратегия защиты которого неизвестна или не внушает доверия. В случае, когда необходим контроль туннелируемого трафика и требуется защищать поток сообщений вплоть до получателя в ЛВС, конечная точка основного туннеля должна находиться на МЭ, который должен после расшифровки и контроля трафика выполнять обратное шифрование пропускаемых пакетов сообщений. Таким образом, одно из преимуществ использования продуктов туннелирования, тесно интегрированных с МЭ, состоит в том, что можно открывать туннель, применять к нему правила защиты МЭ, накладывать криптозащиту снова и перенаправлять трафик получателям в защищаемой МЭ подсети. Но если МЭ и без выполнения функций туннелирования обеспечивает низкую пропускную способность, то реализация VPN только усугубит ситуацию из-за необходимости дополнительных вычислений.

Для реализации протоколов формирования защищенных туннелей разрабатываются также *специализированные программные и аппаратные средства*. Программные средства по сравнению с аппаратными устройствами обладают более высокой гибкостью, так как при невысоких денежных затратах обеспечивается возможность модернизации и обновления версий, а также оперативность устранения ошибок. Ряд чисто программных продуктов, функционирующих на соответствующих серверах, может не только создавать защищенные туннели, но и выполнять функции МЭ, а также хэшировать страницы Web. Аппаратные средства, которые могут быть как одно-, так

и многофункциональными, характеризуются более высокой производительностью. Пограничные многофункциональные аппаратные устройства включают в свой состав маршрутизатор, МЭ, средства управления пропускной способностью и средства создания VPN. Подобные устройства, которые можно отнести к комплексным МЭ, проще обслуживать. Ведь легче использовать один интегрированный пользовательский интерфейс, чем поддерживать и конфигурировать такие отдельные устройства, как маршрутизатор, МЭ, VPN и модуль управления пропускной способностью. Однако в многофункциональных устройствах производительность одного приложения зачастую повышается в ущерб другому.

Обобщенные достоинства и недостатки средств создания VPN различных категорий представлены в табл. 5 [3].

При интенсивном обмене важной информацией между филиалами для построения VPN лучше использовать специализированное оборудование, однако при ограниченных средствах можно обратить внимание и на чисто программное решение. В случае, кода происходит обмен информацией в небольших объемах, оправданным является использование именно программных средств.

4.4.1. Виртуальные частные сети на базе сетевой операционной системы

Сегодня в России наибольшее распространение среди сетевых ОС, позволяющих строить VPN штатными средствами самой ОС (протокол PPTP и IPSec), получила Windows NT/2000. Для создания VPN Microsoft использует протокол PPTP, который интегрирован в ОС Windows NT. В работе VPN на базе Windows NT используется база пользователей, хранящаяся в Primary Domain Controller (PDC). При подключении к PPTP-серверу пользователь авторизуется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования используется нестандартный протокол от Microsoft Point-to-Point Encryption с 40- или 128-битным ключом, получаемым в момент установки соединения.

Таблица 5. **Достоинства и недостатки средств создания VPN различных категорий**

Категория	Достоинства	Недостатки
VPN на базе маршрутизаторов	Функции поддержки сетей VPN могут быть встроены в маршрутизирующие устройства, что не потребует дополнительных расходов на приобретение средств, реализующих эти функции. Упрощается администрирование VPN	Функционирование VPN может отрицательно повлиять на другой трафик. Канал между получателем информации внутри ЛВС и маршрутизатором может стать уязвимым звеном в системе защиты
ПО VPN для МЭ	Возможен контроль туннелируемого трафика. Достигается высокая эффективность администрирования защищенных виртуальных сетей. Обеспечивается комплексная защита информационного обмена. Отсутствует избыточность аппаратных платформ для средств сетевой защиты	Операции, связанные с шифрованием данных, могут чрезмерно загружать процессор и снижать производительность МЭ. Если защищенный туннель завершается на МЭ, то канал между получателем информации внутри ЛВС и МЭ может стать уязвимым звеном в системе защиты. При повышении производительности серверных продуктов аппаратное обеспечение потребуется модернизировать
VPN на базе специализированого ПО	Возможность модернизации и обновления версий. Оперативность устранения ошибок. Не требуются специальные аппаратные средства	Администрирование VPN может потребовать отдельного приложения, возможно, даже выделенного каталога. При повышении производительности серверных продуктов аппаратное обеспечение может потребоваться модернизировать
VPN на базе аппаратных средств	Обеспечивается более высокая производительность. Многофункциональные аппаратные устройства облегчают конфигурацию и обслуживание. Однофункциональные аппаратные устройства допускают тонкую настройку для достижения наивысшей производительности	В многофункциональных блоках производительность одного приложения повышается зачастую в ущерб другому. Однофункциональные устройства могут требовать отдельных инструментов администрирования и каталогов. Модернизация для повышения производительности нередко оказывается слишком дорогостоящей или невозможной. Канал между получателем информации внутри ЛВС и аппаратным устройством шифрования трафика может стать уязвимым звеном в системе защиты

Недостатки данной системы — отсутствие проверки целостности данных и невозможность смены ключей во время соединения, а также выявленные в ходе независимых тестов ошибки и слабые места существующих версий самой ОС. Достоинства — легкость интеграции с Windows. Это решение считается достаточно удобным и дешевым средством создания VPN.

4.4.2. Виртуальные частные сети на базе маршрутизаторов

Другой способ построения VPN предполагает для создания защищенных каналов применение маршрутизаторов [3] (рис. 38). Поскольку вся информация, исходящая из ЛВС проходит через маршрутизатор, то на него возлагаются и задачи шифрования. В связи с тем, что маршрутизатор пропускает через себя все пакеты, передаваемые из ЛВС, он может использоваться также для шифрования этих пакетов. Кроме того, маршрутизатор может выполнять и функцию расшифровывания защищенного входящего трафика. Поддержка функций построения VPN в настоящее время включается во многие маршрутизирующие и коммутирующие устройства. Лидерами в этой области являются компании Cisco Systems и 3Com.

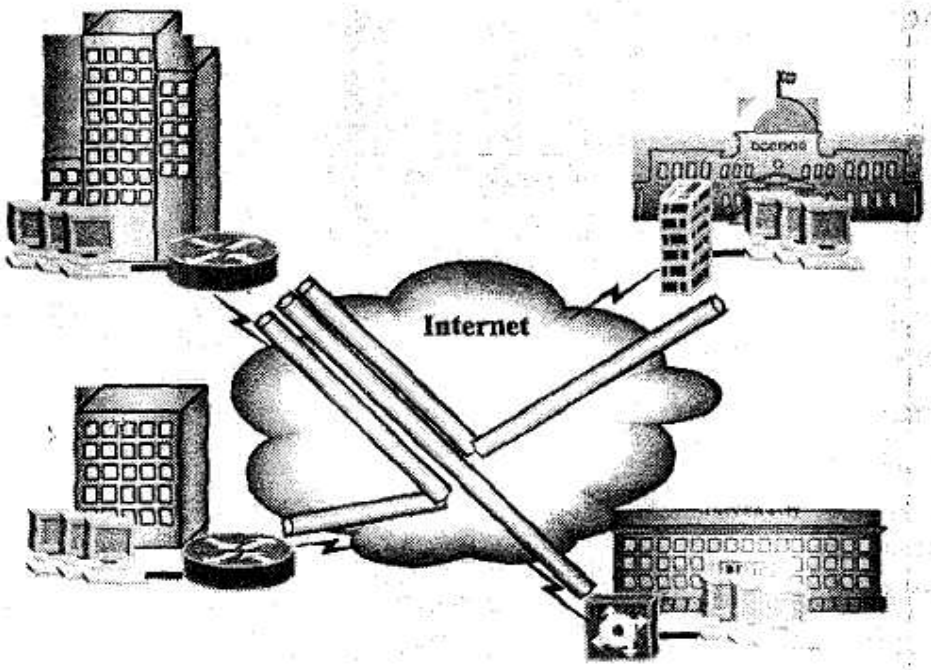


Рис. 38. Построение VPN на базе маршрутизаторов

Компания Cisco Systems включила в ОС IOS 11.3 (Internetwork Operating System 11.3), разработанную для своих маршрутизаторов, поддержку протоколов L2TP и IPSec (начиная с версии IOS 11.3(3)). Если на пограничные маршрутизаторы Cisco отделений компании установлена данная ОС, то имеется возможность сформировать корпоративную VPN (протоколы L2TP и IPSec), состоящую из совокупности виртуальных защищенных туннелей типа "точка-точка" от одного мартшутизатора к другому. Как правило, для шифрования данных в канале по умолчанию используется американский алгоритм DES с длиной ключа 56 бит. Существенно, что в этом случае криптообработка пакетов является дополнительной функцией, требующей значительных вычислительных ресурсов. Поэтому, если маршрутизатор заказчика имеет достаточно большой запас по производительности, то он вполне может выполнять и функции VPN, такие, как идентификация при установлении туннельного соединения и обмен ключами.

Протокол L2F стал компонентом IOS еще раньше и поддерживается во всех выпускаемых Cisco устройствах межсетевого взаимодействия и удаленного доступа. Разработанная Cisco Systems технология построения VPN отличается высокой производительностью и гибкостью. Обеспечивается туннелирование с шифрованием для любого IP-потока, передаваемого в "чистом" или инкапсулированном виде. Защищенный туннель строится на основании заданных адресов источника и назначения, номеров портов TCP/UDP и установленных параметров качества сервиса IP (IP Quality of Service). Если в ЛВС уже имеется маршрутизатор с ОС IOS, не поддерживающей протоколы L2TP и IPSec, можно установить на нем дополнительное ПО шифрования данных. При необходимости повысить производительность целесообразно воспользоваться производимой Cisco Systems платой расширения ESA (Encryption Service Adapter). На ней установлен специализированный сопроцессор для шифрования.

Подобно прочим устройствам шифрования данных, плата ESA не только криптографически защищает информацию, но и предотвращает проникновение злоумышленника в систему, а также реагирует на все подозрительные ситуации. Если просто вытащить плату

из маршрутизатора (даже отключив напряжение питания), то на лицевой панели загорится индикатор "Tamper" ("Злоумышленник") и для повторного запуска маршрутизатора понадобится вмешательство обслуживающего персонала. Для этого необходимо либо знать пароль, устанавливаемый при первом вводе платы в эксплуатацию, либо быть готовым к тому, что вся ее оперативная память будет очищена. Если вскрыть модуль ESA, то активизируется специальный выключатель и произойдет очистка оперативной памяти. Шифрование данных на аппаратном уровне позволяет повысить производительность и снижает влияние функций поддержки защищенных туннелей на пропускную способность маршрутизатора.

Как и Cisco Systems, компания 3Com при реализации технологии VPN с самого начала ориентировалась на стандарты. Она является одним из крупнейших производителей концентраторов удаленного доступа, поддерживающих протоколы PPTP и L2TP. Поддержка VPN встроена в ее маршрутизаторы NetBuilder II, продукты SuperStack II NetBuilder и платформы QfficeConnect NetBuilder Platform. Сети VPN от 3Com совместимы и IPSec и разработаны для взаимодействия с внешними каталогами, включая Novell KDS и Windows NT Directory Services. Компания разработала также программное приложение TranscendWare Secure VPN Manager, основанное на Web-технологии и предназначенное для контроля загруженности VPN, а также сбора статистики и информации о происходящих событиях. Кроме того, 3Com выпускает инструментарий настройки на базе Web, позволяющий легко создавать криптозащищенные туннели. Еще одним уникальным предложением от 3Com является поддержка коммутации защищенных туннелей. Такая коммутация позволяет туннелю миновать МЭ и завершиться в конкретной подсети или даже на конкретной клиентской машине.

4.4.3. Виртуальные частные сети на базе межсетевых экранов

Сначала сделаем краткое отступление, посвященное МЭ (более подробную информацию по МЭ можно найти в учебном пособии Н.Г.Милославской и А.И.Толстого "Интрасети: доступ в Internet, защита". М.: ЮНИТИ, 2000.).

Системы анализа трафика и блокировки доступа называются межсетевыми экранами (дословный перевод Firewall – "пожарная стена"). На основе заданного набора правил они анализируют пакеты на предмет разрешенных/запрещенных адресов и сервисов (TCP/UDP-портов). Обычно при конфигурации системы указывают, с каких адресов, по каким портам и с какими компьютерами можно работать, а с какими нет. Таким образом, МЭ регламентирует использование ресурсов одних сетей пользователями других. Он не является симметричным, так как для него определены понятия "внутри" и "снаружи".

МЭ в простейшем случае состоит из двух механизмов: один ограничивает перемещение данных, второй ему способствует (т.е. осуществляет перемещение данных). Поэтому МЭ представляет собой последовательность фильтров. Это система, позволяющая разделить сеть на две или более частей и реализовать набор правил, которые определяют условия прохождения пакетов из одной части в другую. Как правило, граница проводится между сетью предприятия и внешней сетью, хотя ее можно провести и внутри сети.

В июле 1997 г. вышел руководящий документ "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа" Гостехкомиссии при Президенте РФ (полный текст можно найти в информационном бюллетене "Jet Info" № 17-18 1997 г. и на узле http://www.infotecs.ru/gtc/RD_ekran.htm). В этом документе дана классификация МЭ в зависимости от степени обеспечиваемой ими защиты от НСД. Определение самого МЭ таково: МЭ – это локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Устанавливается пять классов защищенности МЭ: пятый (самый низкий) — применяется для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый — для 1Г, третий — 1В, второй — 1Б, первый (самый высокий) — для 1А. (Напомним, что Гостехко-

миссией РФ определено девять классов защищенности АС от НСД, каждый из которых характеризуется определенной совокупностью требований к средствам защиты. Классы подразделяются на три группы, отличающиеся спецификой обработки информации. Класс с цифрой "1" включает многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют равные права доступа.)

В самом общем случае МЭ должен:

- обеспечивать безопасность внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи;
- обладать мощными и гибкими средствами управления для полного и простого воплощения в жизнь политики безопасности организации;
- обеспечивать простую реконфигурацию МЭ при изменении структуры сети;
- работать незаметно для пользователей сети и не затруднять выполнение ими легальных действий;
- работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в пиковых режимах;
- обладать свойствами самозащиты от любых НСД;
- иметь возможность централизованно обеспечивать несколько внешних подключений (например, удаленных филиалов) для проведения единой политики безопасности;
- иметь средства авторизации доступа пользователей через внешние подключения.

Выделяют три основных компонента МЭ, выполняющих функции администрирования, сбора статистики и предупреждения об атаке и аутентификации.

Администрирование. Легкость администрирования является одним из ключевых аспектов при создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать лазейку, через которую рано или поздно будет взломана система. Поэтому в большинстве МЭ реализованы сервисные утилиты, облегчающие ввод, удаление и просмотр набора правил. Нали-

чие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактировании правил. Обычно эти утилиты позволяют просматривать информацию, сгруппированную по каким-либо критериям, например, все, что относится к конкретному пользователю или сервису.

Системы сбора статистики и предупреждения об атаке. Информация обо всех событиях: отказах, входящих, выходящих соединениях, числе переданных байт, использовавшихся сервисах, времени соединения и т.д., – накапливается в файлах статистики. Многие МЭ позволяют гибко определять подлежащие протоколированию события, описывать порядок действия при атаках или попытках НСД: сообщение на консоль, почтовое послание администратору системы и т.д. Немедленный вывод сообщения о попытке взлома на экран консоли или администратора может помочь, если попытка оказалась успешной и атакующий уже проник в систему. В состав многих МЭ входят генераторы отчетов, служащие для обработки статистики и позволяющие собрать статистику по использованию ресурсов конкретными пользователями, по использованию сервисов, отказам, источникам, с которых проводились попытки несанкционированного доступа и т.д.

Аутентификация. Прежде чем пользователю будет предоставлено право получить тот или иной сервис, необходимо убедиться, что он действительно тот, за кого себя выдает (предполагается, что этот сервис для данного пользователя разрешен: процесс определения, какие сервисы разрешены, называется авторизацией; авторизация обычно рассматривается в контексте аутентификации – как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы). При получении запроса на использование сервиса от имени какого-либо пользователя, МЭ проверяет, какой способ аутентификации определен для данного пользователя, и передает управление серверу аутентификации. После получения положительного ответа МЭ формирует запрашиваемое пользователем соединение.

При конфигурировании МЭ следует выбрать стратегию защиты. Типичным является "запрещено все, что не разрешено", однако можно выбрать и противоположный подход, а именно "разрешено

все, что не запрещено". Лучшие из реализаций МЭ блокируют по умолчанию всякий доступ, а затем пропускают только те пакеты, прохождение которых специально разрешено и может быть проконтролировано.

МЭ, который может быть программный, аппаратный или программно-аппаратным, имеет список контроля доступа, ограничивающий или разрешающий прохождение IP-пакетов по тому или иному адресу (или целому набору адресов) и по заданным номерам портов (сервисам).

Естественно, что именно из соображений производительности аппаратные МЭ наиболее эффективно использовать совместно с маршрутизаторами, соединяющими внутреннюю и внешние сети. В этом случае вся защита концентрируется в наиболее уязвимом месте – на стыке ЛВС, находящейся в техническом и административном ведении компании, и внешней сети, принадлежащей организации, предоставляющей транспортные услуги. Тогда фильтрация пакетов происходит на маршрутизаторе.

Большинство из существующих МЭ предусматривает также сокрытие внутренней структуры IP-сети организации (NAT). Как правило, адрес системы, находящейся внутри защищаемой МЭ сети, заменяется адресом самого МЭ.

Все МЭ можно разделить на четыре типа (табл. 6):

- пакетные фильтры (packet filter);
- серверы (шлюзы) уровня соединения (circuit gateways);
- серверы (шлюзы) прикладного уровня (application gateways);
- МЭ экспертного уровня (stateful inspection firewall).

Таблица 6. **Соотношение протоколов, уровней модели OSI и типов МЭ**

Уровень модели OSI	Протоколы Internet	Категория МЭ
Прикладной	Telnet, FTP, DNS, NFS, PING, SMTP, HTTP	Шлюз прикладного уровня, МЭ экспертного уровня
Представления данных		
Сеансовый	TCP, UDP	Шлюз сеансового уровня
Транспортный	TCP, UDP	
Сетевой	IP, ICMP	МЭ с фильтрацией пакетов
Канальный	-	-
Физический	-	-

Работа всех МЭ основана на использовании информации разных уровней модели OSI. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им соответствующий уровень защиты.

Пакетные фильтры. Роль МЭ с пакетной фильтрацией чаще всего играют экранирующие маршрутизаторы. МЭ с пакетными фильтрами принимают решение о том, пропускать пакет или отбросить, просматривая в заголовке этого пакета все IP-адреса, флаги или номера TCP-портов. IP-адрес и номер порта – это информация соответственно сетевого и транспортного уровней, но пакетные фильтры используют и информацию прикладного уровня – все стандартные сервисы в TCP/IP ассоциируются с определенным номером порта. Для описания правил прохождения пакетов составляют таблицы типа:

Действие	Тип пакета	Адрес источника	Порт источника	Адрес назначения	Порт назначения	Флаги

Поле "Действие" может принимать значения: пропустить или отбросить. Тип пакета – TCP, UDP или ICMP. Флаги – флаги из заголовка IP-пакета. Поля "Порт источника" и "Порт назначения" имеют смысл только для TCP- и UDP-пакетов (ICMP имеет дело только с адресами).

Серверы уровня соединения. Сервер уровня соединения представляет из себя транслятор TCP-соединения. Пользователь устанавливает соединение с определенным портом на МЭ, который производит соединение с местом назначения по другую от себя сторону. Во время сеанса этот транслятор копирует байты в обоих направлениях. Как правило, пункт назначения задается заранее, в то время как источников может быть много – соединение типа "один – много".

Сервер уровня соединения следит за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), проверяя, является ли допустимым запрашиваемый сеанс связи. При копировании и перенаправлении пакетов в этих серверах используются так называемые канальные посредники, которые устанавлива-

все, что не запрещено". Лучшие из реализаций МЭ блокируют по умолчанию всякий доступ, а затем пропускают только те пакеты, прохождение которых специально разрешено и может быть проконтролировано.

МЭ, который может быть программный, аппаратный или программно-аппаратным, имеет список контроля доступа, ограничивающий или разрешающий прохождение IP-пакетов по тому или иному адресу (или целому набору адресов) и по заданным номерам портов (сервисам).

Естественно, что именно из соображений производительности аппаратные МЭ наиболее эффективно использовать совместно с маршрутизаторами, соединяющими внутреннюю и внешние сети. В этом случае вся защита концентрируется в наиболее уязвимом месте – на стыке ЛВС, находящейся в техническом и административном ведении компании, и внешней сети, принадлежащей организации, предоставляющей транспортные услуги. Тогда фильтрация пакетов происходит на маршрутизаторе.

Большинство из существующих МЭ предусматривает также сокрытие внутренней структуры IP-сети организации (NAT). Как правило, адрес системы, находящейся внутри защищаемой МЭ сети, заменяется адресом самого МЭ.

Все МЭ можно разделить на четыре типа (табл. 6):

- пакетные фильтры (packet filter);
- серверы (шлюзы) уровня соединения (circuit gateways);
- серверы (шлюзы) прикладного уровня (application gateways);
- МЭ экспертного уровня (stateful inspection firewall).

Таблица 6. **Соотношение протоколов, уровней модели OSI и типов МЭ**

Уровень модели OSI	Протоколы Internet	Категория МЭ
Прикладной	Telnet, FTP, DNS, NFS, PING, SMTP, HTTP	Шлюз прикладного уровня, МЭ экспертного уровня
Представления данных		
Сеансовый	TCP, UDP	Шлюз сеансового уровня
Транспортный	TCP, UDP	
Сетевой	IP, ICMP	МЭ с фильтрацией пакетов
Канальный	-	-
Физический	-	-

Работа всех МЭ основана на использовании информации разных уровней модели OSI. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им соответствующий уровень защиты.

Пакетные фильтры. Роль МЭ с пакетной фильтрацией чаще всего играют экранирующие маршрутизаторы. МЭ с пакетными фильтрами принимают решение о том, пропускать пакет или отбросить, просматривая в заголовке этого пакета все IP-адреса, флаги или номера TCP-портов. IP-адрес и номер порта – это информация соответственно сетевого и транспортного уровней, но пакетные фильтры используют и информацию прикладного уровня – все стандартные сервисы в TCP/IP ассоциируются с определенным номером порта. Для описания правил прохождения пакетов составляют таблицы типа:

Действие	Тип пакета	Адрес источника	Порт источника	Адрес назначения	Порт назначения	Флаги

Поле "Действие" может принимать значения: пропустить или отбросить. Тип пакета – TCP, UDP или ICMP. Флаги – флаги из заголовка IP-пакета. Поля "Порт источника" и "Порт назначения" имеют смысл только для TCP- и UDP-пакетов (ICMP имеет дело только с адресами).

Серверы уровня соединения. Сервер уровня соединения представляет из себя транслятор TCP-соединения. Пользователь устанавливает соединение с определенным портом на МЭ, который производит соединение с местом назначения по другую от себя сторону. Во время сеанса этот транслятор копирует байты в обоих направлениях. Как правило, пункт назначения задается заранее, в то время как источников может быть много – соединение типа "один – много".

Сервер уровня соединения следит за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), проверяя, является ли допустимым запрашиваемый сеанс связи. При копировании и перенаправлении пакетов в этих серверах используются так называемые канальные посредники, которые устанавлива-

ют между двумя сетями виртуальный канал связи и поддерживают несколько служб TCP/IP.

Используя различные порты, можно создавать различные конфигурации. Данный тип сервера позволяет создавать транслятор для любого, определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Серверы прикладного уровня. МЭ этого типа используют серверы конкретных сервисов – telnet, ftp, proxy server и т.д., запускаемые на МЭ и пропускающие через себя весь трафик, относящийся к данному сервису. Таким образом, между клиентом и сервером образуются два соединения: от клиента до МЭ и от МЭ до места назначения.

Полный набор поддерживаемых серверов различается для каждого конкретного МЭ, однако чаще всего встречаются серверы-посредники для следующих сервисов: терминалы (telnet, rlogin), передача файлов (ftp), электронная почта (SMTP, POP3 – Post Office Protocol), WWW (HTTP, SHTTP), Gopher, Wais, X Window System (X11), Принтер, Rsh, Finger, новости (NNTP – Network News Transfer Protocol) и т.д.

Использование серверов прикладного уровня позволяет решить важную задачу – скрыть от внешних пользователей структуру интрасети, включая информацию в заголовках почтовых пакетов или службы доменных имен.

Другим положительным качеством является возможность аутентификации – подтверждения действительно ли пользователь является тем, за кого он себя выдает.

При описании правил доступа используются такие параметры, как название сервиса, имя пользователя, допустимый период времени использования сервиса, компьютеры, с которых можно обращаться к сервису, схемы аутентификации. Серверы протоколов прикладного уровня позволяют обеспечить наиболее высокий уровень защиты – взаимодействие с внешним миром реализуется через небольшое число прикладных программ, полностью контролирующих весь входящий и выходящий трафик.

Сфера действия этих МЭ — уровень прикладных программ, они принимают запросы клиента и обращаются за необходимой информацией к серверу-адресату от имени клиента. По замыслам разработчиков средств защиты безопасность гарантирована, поскольку каждый запрос проходит через МЭ, но зачастую МЭ рассчитаны только на классические приложения, реализующие протоколы HTTP и FTP и программы электронной почты SMTP, они не отличаются эффективностью при работе с новыми приложениями. Особенно трудно приходится МЭ, когда они имеют дело с современными приложениями на базе протокола UDP, например предназначенными для коллективной работы или передачи потоков мультимедиа.

Сравнительные характеристики. Приведем основные преимущества и недостатки пакетных фильтров и серверов прикладного уровня.

К положительным качествам пакетных фильтров следует отнести следующие:

- относительно невысокая стоимость;
- гибкость в определении правил фильтрации, т.е. простота конфигурации и установки;
- минимальное влияние на производительность сети из-за небольшой задержки при прохождении пакетов;
- прозрачность для ПО из-за отсутствия специальных требований к содержимому пакетов, посылаемых пользователями.

Недостатки у данного типа МЭ следующие:

- ЛВС видна (маршрутизируется) из Internet;
- правила фильтрации пакетов трудны в описании, поэтому требуются очень хорошие знания технологий TCP и UDP;
- при нарушении работоспособности МЭ все компьютеры за ним становятся полностью незащищенными либо недоступными;
- аутентификацию с использованием IP-адреса можно обмануть при помощи IP-спуффинга, когда атакующая система выдает себя за другую, используя ее IP-адрес;
- отсутствует аутентификация на пользовательском уровне.

К преимуществам серверов прикладного уровня следует отнести следующие:

- ЛВС невидима из Internet;

- при нарушении работоспособности МЭ пакеты перестают проходить через МЭ, тем самым не возникает угрозы для защищаемых им компьютеров;
- защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, снижая тем самым вероятность взлома с использованием дыр в ПО;
- при организации аутентификации на пользовательском уровне может быть реализована система немедленного предупреждения о попытке взлома.

Недостатками этого типа серверов являются:

- более высокая, чем для пакетных фильтров стоимость;
- невозможность использования протоколов RPC и UDP;
- производительность ниже, чем для пакетных фильтров.

МЭ экспертного уровня. Эти МЭ сочетают в себе элементы всех трех описанных выше категорий. Как и МЭ с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. МЭ экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И наконец, МЭ экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

При использовании метода "таможенного" контроля (stateful inspection) МЭ экспертного уровня устанавливается прозрачно между внутренней и внешней сетями, с тем чтобы проверять пакеты на линии передачи данных или на сетевом уровне по мере их прохождения. МЭ может выполнять и вполне интеллектуальную функцию отслеживания сеансов обмена информацией между клиентом и сервером. К примеру, МЭ пропустит ответ от сервера только в том случае, если запрос клиента был санкционирован.

В последнее время отмечается постепенное стирание различий между двумя типами МЭ — фильтрами пакетов и шлюзами приложений. Эту тенденцию, по мнению специалистов, нельзя назвать абсолютно отрицательной, так как под ее воздействием можно сформироваться более однородный рынок МЭ.

У МЭ есть и свои недостатки. Много бед способны натворить проникшие через МЭ вирусы и вредоносные Java-утилиты. Существует простой подход — заблокировать все файлы и Java-утилиты, но это не лучшее решение. МЭ — это как раз то самое место, где можно "разглядеть" подобные угрозы.

Обычный МЭ настраивается, как минимум, на два интерфейса: внутренний — для ЛВС и внешний — для Internet. Кроме того, МЭ может иметь интерфейс для подключения так называемых "демилитаризованных зон" (например, из Web и FTP-серверов).

Для подключения МЭ используются различные схемы.

1. МЭ может работать в качестве внешнего маршрутизатора, используя поддерживаемые типы устройств для подключения к внешней сети. Известны два основных метода использования МЭ: в классическом варианте МЭ устанавливаются на границе ЛВС и открытых сетей и для защиты отдельных подсетей в ЛВС с особыми политиками безопасности МЭ устанавливаются в этих подсетях. Для первого случая возможна установка одного МЭ или целого ряда узкоспециализированных МЭ – для связи с бизнес-партнерами, для обслуживания пользователей, подключаемых к ЛВС с помощью различных мобильных средств связи, для создания VPN и т.д.

2. Если МЭ может поддерживать два Ethernet-интерфейса – так называемый "двудомный" (dual-homed) МЭ, то чаще всего подключение осуществляется через внешний маршрутизатор. При этом между внешним маршрутизатором и МЭ имеется только один путь, по которому идет весь трафик. Обычно маршрутизатор настраивается таким образом, что МЭ является для него единственным, видимым снаружи компьютером. Эта схема является наиболее предпочтительной с точки зрения безопасности и надежности защиты.

Реже используется другая схема, но ее нужно применять только в крайнем случае, поскольку требуется очень аккуратная настройка маршрутизаторов, и даже небольшие ошибки могут образовать серьезные проблемы с защитой. Но эта схема позволяет дополнительно контролировать трафик в зависимости от направления его передачи до и после МЭ.

Как вариант возможна схема, когда исходная сеть разделяется на защищаемую и незащищаемую части. Возможна схема подключения

МЭ, когда он защищает только одну подсеть из нескольких серверов, выходящих из маршрутизатора – защита "бастиона" серверов. В незащищаемой области часто располагают серверы, видимые снаружи: WWW, FTP и т.д. Некоторые МЭ предлагают разместить эти серверы на них самих – это решение, далеко не лучшее с точки зрения загрузки компьютера и безопасности самого МЭ.

Существуют решения, которые позволяют организовать из видимых снаружи серверов третью сеть, что обеспечивает контроль за доступом при сохранении необходимого уровня защиты компьютеров в основной сети. Для защиты каждый сервер можно подключить на отдельный сетевой интерфейс МЭ для 100 % контроля трафика сервера. При этом достаточно много внимания уделяется тому, чтобы пользователи внутренней сети не могли случайно или умышленно открыть вход в ЛВС через эти видимые снаружи серверы.

3. Еще один вариант подключения – с выделением так называемой "демилитаризованной зоны" (ДМЗ). Организация ДМЗ предназначена не только для защиты от атак из Internet, но и внутри от компьютеров самой организации. ДМЗ – это часть КС, содержащая шлюз (или два шлюза: внутренний и внешний) и отделенная с одной стороны от защищенной части КС внешним МЭ, а с другой – от незащищенной части КС, имеющей подключение к Internet, внутренним МЭ или маршрутизатором с фильтрами. В ДМЗ могут находиться, например, Web, FTP, SMTP, DNS-серверы.

Для повышения уровня защищенности возможно использовать в одной сети несколько МЭ, стоящих друг за другом (выполняющих разные проверки пакетов) или параллельно друг другу (второй МЭ начинает работать, например, при выходе из строя первого), или выделенных в отдельную экранирующую подсеть. При этом как открытая, так и закрытая части ЛВС имеют доступ к изолированной сети. Преимуществами данного подхода являются: возможность использования механизма трансляции адресов, что позволяет скрыть внутреннюю структуру ЛВС; возможность решения вопросов большого трафика при прохождении пакетов через разные бастионы (если они установлены параллельно, а не последовательно). К недостаткам данного подхода можно отнести необходимость технического сопровождения функционирования экранирующей подсети толь-

ко высококвалифицированными специалистами и необходимость использования только высокопроизводительных бастионов в связи с большим объемом вычислений.

Через МЭ локальной сети, как и через маршрутизатор, пропускается весь трафик. Соответственно функции шифрования исходящего и расшифрования входящего трафика может выполнять и МЭ. К ПО собственно МЭ добавляется модуль шифрования. Ведущими производителями МЭ, поддерживающих функции построения VPN, являются компании Check Point Software Technologies, Axent Technologies, Network Associates и Secure Computing. Поддержка VPN обеспечивается также в МЭ, выпускаемых отдельными производителями сетевых ОС. К таким продуктам относится, например, МЭ BorderManager компании Novell.

Сегодня, по мнению специалистов, построение VPN на базе МЭ является оптимальным решением для обеспечения комплексной безопасности корпоративной информационной системы от атак из открытых сетей [3]. Действительно, объединение функций МЭ и VPN шлюза в одной точке под контролем единой системы управления и аудита является решением не только технически грамотным, но и удобным для администрирования.

В России для построения корпоративных VPN на базе МЭ очень часто используются программные продукты компании CheckPoint Software Technologies – CheckPoint Firewall-1/VPN-1 (протокол IPSec), а для шифрования трафика в каналах CheckPoint Firewall-1 применяются известные криптоалгоритмы DES, CAST, IDEA, FWZ и др. Весь ряд продуктов CheckPoint VPN-1 реализован на базе открытых стандартов (IPSec). Согласно последнему исследованию Dataquest продукция данной компании занимает 52 % мирового рынка VPN.

Семейство МЭ FireWall-1 включает подсистему формирования защищенных туннелей VPN-1. В основу криптозащиты потока сообщений положен протокол IPSec. На обычных настольных рабочих станциях развиваются скорости шифрования более 10 Мбит/с. FireWall-1 обеспечивает контроль не только открытого, но и криптозащищенного трафика. С помощью VPN-1 МЭ расшифровывает поступившие к нему данные, затем применяет к ним установленные

администратором правила управления доступом, а потом снова зашифровывает пакеты сообщений, пропускаемые дальше. Подсистема VPN-1 выполняет не только криптографическое закрытие трафика, но и аутентификацию пакетов сообщений. Для распределения ключей может использоваться стандарт IPSec, а также протокол SKIP. Для криптографического закрытия информации реализованы симметричные криптосистемы DES, RC4 и FWZ1 (криптосистема FWZ1 является собственной разработкой компании Check Point). Для аутентификации пакетов сообщений могут использоваться алгоритмы MD5, SHA-1, CBC DES и MAC. Поддерживаются два режима криптографической защиты:

- защита передаваемого по Internet трафика между МЭ FireWall-1;
- защита трафика при удаленном доступе к ЛВС, защищаемой МЭ FireWall-1.

В первом случае все функции защиты реализуются прозрачно системами FireWall-1, между которыми устанавливается связь. Во втором случае функции криптографической защиты выполняются МЭ FireWall-1 ЛВС, к которой осуществляется удаленный доступ, и специальным компонентом FireWall-1 SecuRemote, который должен быть установлен на удаленном компьютере. В компьютерах с шиной PCI для ускорения шифрования может использоваться поставляемая Check Point дополнительная плата.

Компания Axent Technologies, которая в 1998 г. приобрела фирму Raptor, являющуюся производителем МЭ Eagle FireWall, переименовала этот продукт в Raptor FireWall. Версия Raptor FireWall 5.0 обеспечивает построение VPN по протоколу IPSec. Как и FireWall-1 компании Check Point, МЭ Raptor FireWall может применять установленные правила доступа к туннелируемому трафику. Компания Axent также поставляет семейство мобильных клиентов для VPN между пользователями и ЛВС.

Компания Trusted Information Systems, разработавшая МЭ Gauntlet FireWall, вошла в состав компании Network Associates. Подсистема данного МЭ Gauntlet Global VPN, основанная на протоколе IPSec, поддерживает два режима криптографической защиты трафика:

- от МЭ до МЭ, реализуемого с помощью шлюзов SmartGate;

- от МЭ до компьютера удаленного пользователя, реализуемого ПО удаленного клиента Gauntlet PC Extender.

В Gauntlet Global VPN используется алгоритм шифрования DES. Наряду с поддержкой IPSec, продукт Gauntlet Global VPN поставляется с ПО УЦ. С помощью этого ПО организации могут выполнять генерацию и проверку цифровых сертификатов, соответствующих стандарту X.509.

Программные средства построения VPN на базе МЭ выпускает и компания Secure Computing. Ее продукты, известные ранее как BorderWare и Sidewinder, теперь переименованы и получили название SecureZone. Технология VPN от Secure Computing реализована в виде встроенной функции МЭ SecureZone. С помощью SecureZone можно комбинировать сети VPN в группы с единообразной политикой и затем каждой группой управлять как единым целым. МЭ SecureZone является IPSec-совместимым. Кроме того, SecureZone поддерживает сертификаты X.509 Netscape Certificate Server, а также программные УЦ таких компаний, как Entrust и VeriSign. МЭ SecureZone включает и IPSec-совместимый клиентский модуль для удаленного доступа, а также собственную нестандартную ОС для компьютеров на платформе Intel. Пользовательский интерфейс и процедуры конфигурирования SecureZone построены на базе Java. Компания Secure Computing также планировала реализовать поддержку вспомогательного аппаратного средства шифрования Ravlin от RedCreek Communications.

МЭ BorderManager от компании Novell также поддерживает функции построения VPN. Помимо этого он обеспечивает разграничение пользовательского доступа, фильтрацию пакетов и трансляцию сетевых адресов, предлагает услуги посредника HTTP, хэширует страницы Web, имеет шлюзы на уровне канала, выполняет многопротокольную маршрутизацию и поддерживает удаленный доступ. BorderManager интегрирован со службой каталогов NDS, что обеспечивает эффективное управление VPN. При использовании МЭ BorderManager распределение ключей шифрования выполняется на основе криптосистемы RSA и протокола Диффи–Хеллмана. Для криптографического закрытия и аутентификации пакетов сообще-

ний используются криптосистемы RC2 и RSA. BorderManager поддерживает протокол IPSec.

В VPN, построенной на основе МЭ BorderManager, один из МЭ должен быть основным, исполняющим роль центра управления. В качестве основного МЭ рекомендуется выбирать МЭ, защищающий центральную ЛВС организации. Процесс конфигурации VPN начинается с настройки основного МЭ с помощью специальной утилиты VPNCFG.NLM. Во время этого процесса будет собрана или получена следующая информация об основном МЭ:

- IP-адрес его интерфейса Internet;
- IP-адрес его VPN туннеля;
- открытый и закрытый ключи RSA;
- параметры алгоритма Диффи–Хеллмана;
- открытый и закрытый ключи Диффи–Хеллмана.

IP-адрес сетевого интерфейса, подключенного к Internet, будет использоваться всеми внешними клиентами и должен быть уникальным в Internet.

Во время конфигурации сервера также необходимо определить IP-адрес VPN-интерфейса. Этот адрес может быть любым. Остальные параметры будут созданы процедурой конфигурации и нужны для шифрования информации, пересылаемой через VPN. После того, как эта информация получена, необходимо передать ее, за исключением закрытых ключей, в удаленные ЛВС, где она будет использоваться для аналогичной процедуры конфигурации остальных МЭ VPN. Полученные во время конфигурации параметры остальных МЭ должны быть переданы для окончательной настройки главному МЭ. После этого МЭ удаленных ЛВС могут устанавливать безопасные туннели через Internet с МЭ центральной ЛВС.

В VPN, построенной на основе МЭ BorderManager, обеспечивается формирование защищенных туннелей не только между МЭ, но и между МЭ каждой ЛВС и компьютерами удаленных пользователей. Все клиенты, пользующиеся удаленным доступом, должны иметь уникальный идентификатор и пароль удаленного доступа, которые хранятся в NDS. Поддерживаются стандартные протоколы NCAP (NetWare Connect Authentication Protocol), PAP, а также CHAP.

У этого решения есть и недостатки. Прежде всего, это высокая стоимость такого решения в пересчете на одно рабочее место КС и достаточно высокие требования к производительности аппаратного обеспечения, на котором работает МЭ, даже при умеренной ширине полосы пропускания выходного канала связи. При использовании МЭ на базе ПК надо помнить, что подобное решение подходит только для небольших сетей с небольшим объемом передаваемой информации.

4.4.4. Виртуальные частные сети на базе специализированного программного обеспечения

При реализации такого решения используется специализированное ПО, работающее на выделенном компьютере и в большинстве случаев выполняющее функции proxy-сервера [3]. Компьютер с таким ПО может быть расположен за МЭ. Все программные средства построения VPN позволяют формировать защищенные туннели чисто программным образом и превращают сервер, на котором они функционируют, в маршрутизатор TCP/IP, который получает зашифрованные пакеты, расшифровывает их и передает по ЛВС дальше, к конечной точке назначения.

Примерами подобных решений являются технология VipNet компании "Инфотекс" и ЗАСТАВА компании "Элвис+".

Продукт RRAS (Routing and Remote Access Service) от Microsoft поддерживает защищенную передачу данных от одной ЛВС к другой и от удаленного компьютера к ЛВС. RRAS работает только под управлением Windows NT 4.0 и выпускается в качестве бесплатного приложения к Windows NT 4.0. Использование RRAS фактически превращает сетевой сервер в маршрутизатор среднего уровня, поддерживающий протоколы маршрутизации RIP (Routing Information Protocol) и OSPF (Open Shortest Path First). Поддерживаются также отдельные функции по фильтрации трафика.

Как показывает практика, при защите потока сообщений между ЛВС RRAS обеспечивает достаточную пропускную способность только в небольших сетях с малозагруженными серверами. Поэтому этот продукт больше подходят для защищенного взаимодействия

с ЛВС удаленных пользователей. Работа с RRAS позволяет набраться опыта в применении защищенного туннелирования. Их можно запускать на уже существующих серверах, ресурсы которых используются и для других задач. При не слишком интенсивном трафике, особенно при необходимости обеспечить связь с ЛВС удаленных пользователей, обеспечивается достаточная производительность.

Продукт F-Secure VPN от компании Data Fellows имеет необычную архитектуру. В состав этого продукта входит своя собственная ОС. В начале с помощью подсистемы администрирования VPN, функционирующей под управлением Windows 95/98/NT, настраиваются параметры формируемой VPN. Затем с помощью этой же подсистемы создаются загрузочные дискеты для компьютеров на базе Intel, содержащие встроенную ОС F-Secure VPN. Если на компьютере загрузить ОС с такой дискеты, данный компьютер будет функционировать только как специализированная VPN-система. Такой подход занимает промежуточное положение между аппаратными и программными средствами построения защищенных туннелей. Это связано с тем, что такие преимущества чисто программной системы, как возможность совместного использования ресурсов и снижения затрат, при использовании F-Secure VPN отсутствуют.

Продукт VPN Server компании Aventail в решении задач туннелирования опирается на протоколы SOCKS 5 и SSL. Туннелирование выполняют программные посредники, область действия которых распространяется за МЭ и завершается в хорошо конфигурируемых и управляемых точках для каждого приложения в отдельности. Такие функциональные возможности наиболее полезны в случае наличия угроз перехвата трафика внутри ЛВС. VPN на основе протокола SOCKS заканчиваются на компьютерах пользователей, а не на МЭ. Поэтому на каждой рабочей станции, выступающей в качестве клиента, должно быть установлено специальное ПО.

4.4.5. Виртуальные частные сети на базе аппаратных средств

Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Такие средства чаще всего совместимы с протоколом IPSec и при-

меняются для формирования криптозащищенных туннелей между ЛВС. Однако оборудование для формирования VPN от некоторых производителей одновременно поддерживает и связь в режиме "удаленный компьютер — ЛВС". Программы под Windows, обеспечивающие туннелирование данных от удаленного пользователя к ЛВС, поставляют компании Bay Networks, Isolation Systems, RedCreek и Timestep. Другими производителями средств аппаратного туннелирования являются компании Radguard, Unified Access Communications, Internet Devices.

Простейший вариант работы аппаратных туннелей — мостовая связь с шифрованием [3]. Такие устройства чаще всего устанавливают на стыке между локальной и глобальной сетями сразу же после маршрутизатора (рис. 39). Они встраиваются в существующие сети TCP/IP и выполняют автоматическое шифрование всего заданного трафика.

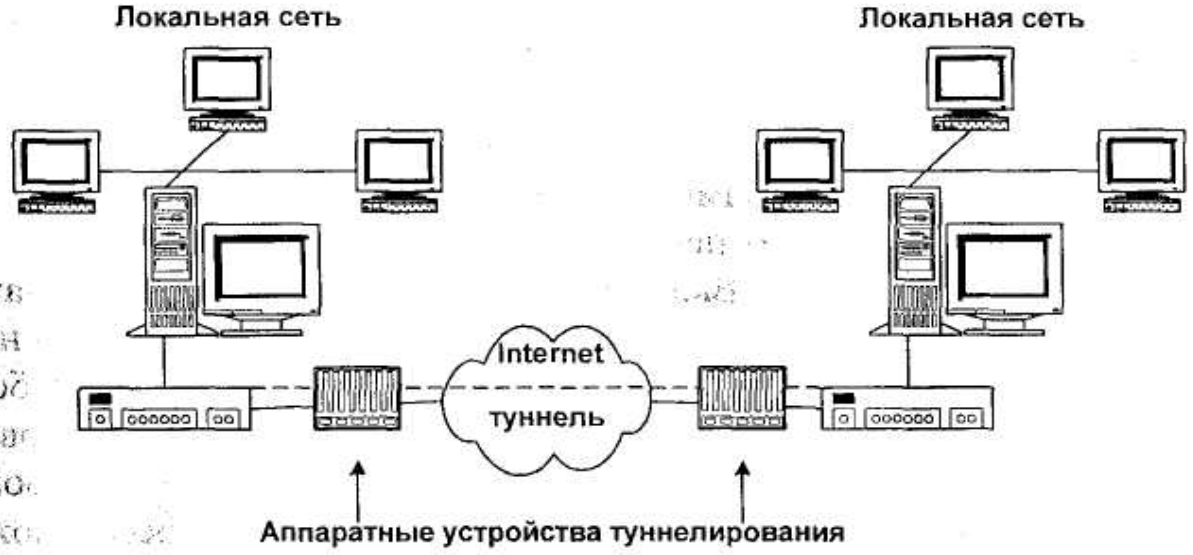


Рис. 39. Схема туннелирования на основе специализированных аппаратных средств

Основное преимущество данного подхода состоит в том, что рабочие станции и маршрутизаторы никаким образом не связаны с формируемым криптотуннелем, а соответственно, их не нужно переконфигурировать при установке VPN. Криптотуннель оказывается

совершенно невидимым для всех сетевых устройств. Определить факт шифрования пакетов сообщений на участке сети между устройствами туннелирования можно только с помощью сетевого анализатора, подключенного к этому участку.

Аппаратные устройства построения VPN отличаются простотой установки и дальнейшего использования. Управление такими устройствами фактически требует решения двух задач: управления ключами через УЦ и управления защищенным туннелированием. Большинство аппаратных устройств построения VPN поставляется вместе с управляющим ПО, способным функционировать под управлением ОС Windows 95/98/NT. Такие программы управления обеспечивают выполнение основных защитных функций туннеля и обработку ошибок. Аппаратными туннелями можно управлять централизованно с одного рабочего места. В большинстве средств аппаратного туннелирования УЦ представляют собой программные приложения под Windows. В отдельных продуктах, например в cIPro-VPN от компании Radguard, за управление ключами отвечает специальное дополнительное устройство. Некоторые аппаратные туннели не способны работать при отсутствии связи с УЦ.

Аппаратные туннели различаются и по своей гибкости. Хороший туннель позволяет администратору указывать, какой трафик следует шифровать, какой пересылать без шифрования, а какой — просто блокировать. Например, cIPro-VPN позволяет устанавливать следующие параметры фильтрации: адреса источника и точки назначения, используемые порты и протоколы, а также любой набор бит в IP-пакетах. Данный продукт, выполняя аппаратное шифрование, обеспечивает пропускную способность до 100 Мбит/с. Устройство с собственными средствами трансляции сетевых адресов можно дополнить платой МЭ. Поддерживается протокол IPSec, а также спецификации ISAKMP/Oakley и X.509.

В 1998 г. компания Bay Networks приобрела фирму New Oak Communications, в результате чего получила многоцелевой аппаратный продукт Contivity Extranet Switch, который кроме создания VPN способен исполнять роль маршрутизатора, МЭ, мультиплексора для интерфейсов T1 или T3, а также диспетчера пропускной способности. Как средство построения VPN, продукт Contivity Extranet Switch

поддерживает протоколы L2F, PPTP, L2TP и IPSec. Для проверки полномочий доступа, подлинности ключевой информации и других аналогичных данных, а также распределения ресурсов он может использовать службы каталогов NDS, Windows NT Directory Services, LDAP и RADIUS. В настоящее время этот продукт является одним из наиболее развитых аппаратных средств туннелирования. Кроме того, компания Bay Networks включила поддержку VPN в свое семейство концентраторов удаленного доступа.

Компания Internet Devices предлагает устройство Fort Knox Policy Router с возможностью установки нескольких приложений. Оно имеет IPSec-совместимые средства создания VPN и может использоваться как фильтр пакетов и посредник приложений, выполнять хэширование страниц Web, транслировать сетевые адреса и переадресовывать почту. Кроме сильных средств защиты и полного набора услуг, данный продукт характеризуется простотой использования и устойчивостью к ошибкам инсталляции и настройки. Управляющее ПО на базе Java не просто выводит на экран список параметров, а показывает опции конфигурации применительно к реализуемой политике. В будущих версиях продукта компания Internet Devices планирует реализовать поддержку протокола LDAP.

4.5. Виды виртуальных частных сетей

VPN можно применять для решения четырех разных задач:

- для организации глобальной связи между филиалами одной компании (интрасеть);
- для соединения частной сети компании с ее деловыми партнерами и клиентами (экстрасеть);
- для взаимодействия с КС отдельных мобильных пользователей или работающих дома сотрудников (удаленный доступ);
- для защиты трафика внутри сети корпорации (интрасеть).

Согласно этому компания Check Point предлагает выделить четыре основных вида VPN (рис. 40): Intranet VPN, Client/server VPN, Extranet VPN и Remote Access VPN [4, 5].

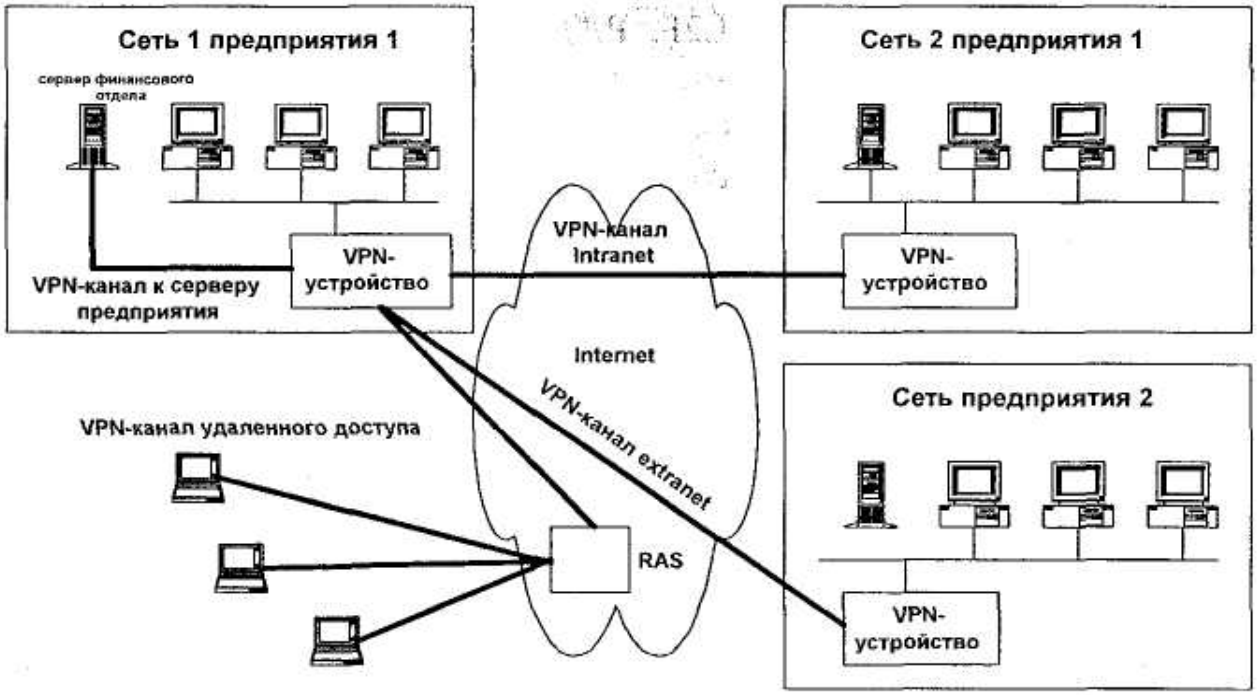


Рис. 40. Виды VPN

При образовании защищенных каналов между шлюзами различных ЛВС одного и того же предприятия, технология VPN используется для реализации услуг интрасетей. В результате образуются защищенные интрасети. При прокладке каналов VPN между шлюзами разных предприятий формируется защищенная экстрасеть. Администратор ЛВС должен так настроить VPN-шлюз, чтобы он поддерживал установление защищенных каналов только с определенными шлюзами своего предприятия (в рамках интрасети), и тех предприятий, с которыми оно обменивается конфиденциальной информацией (в рамках экстрасети).

4.5.1. Intranet VPN

Intranet VPN позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики. Intranet VPN по-

зволяет заказчику устанавливать связь между своими офисами используя IP-сеть оператора или сеть Internet (рис. 41).

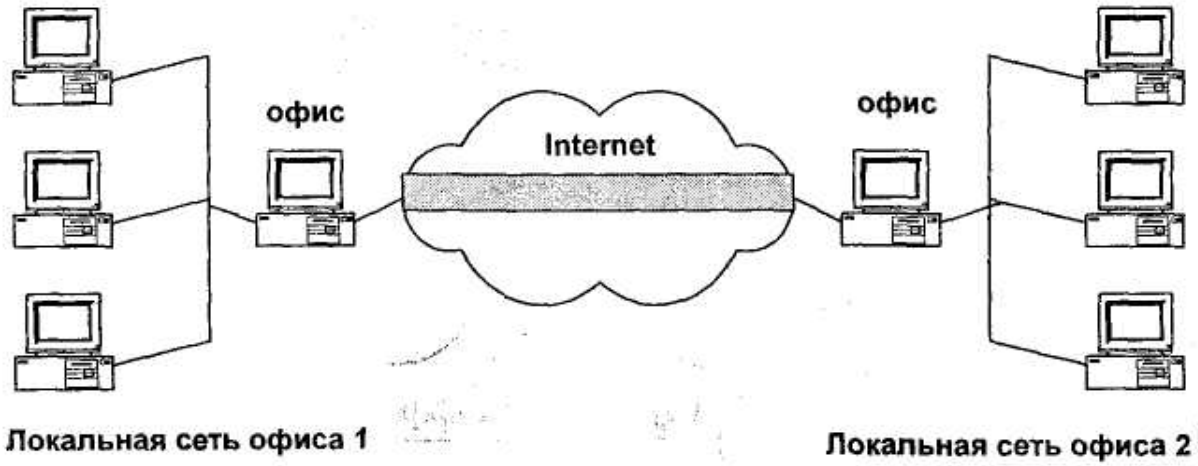


Рис. 41. Intranet VPN

Эта технология использует методы туннелирования GRE, L2TP или IPSec. Туннели устанавливаются между офисными маршрутизаторами для создания между офисами виртуальных соединений. Для повышения безопасности данные в виртуальном канале могут шифроваться. Шифрование выполняется только на выходе из офисов во внешние сети. Такая топология образует "защищенный периметр" вокруг ЛВС корпорации.

4.5.2. Client/server VPN

Client/server VPN обеспечивает защиту передаваемых данных между двумя узлами (не сетями) КС. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, которые обращаются к серверам, находящимся в одном физическом сегменте. Решается задача защиты трафика ряда приложений внутри КС (это также важно, поскольку большинство атак осуществляется из внутренних сетей), при этом

образуются отдельные, непересекающиеся VPN для выделенных групп пользователей или приложений (рис. 42).

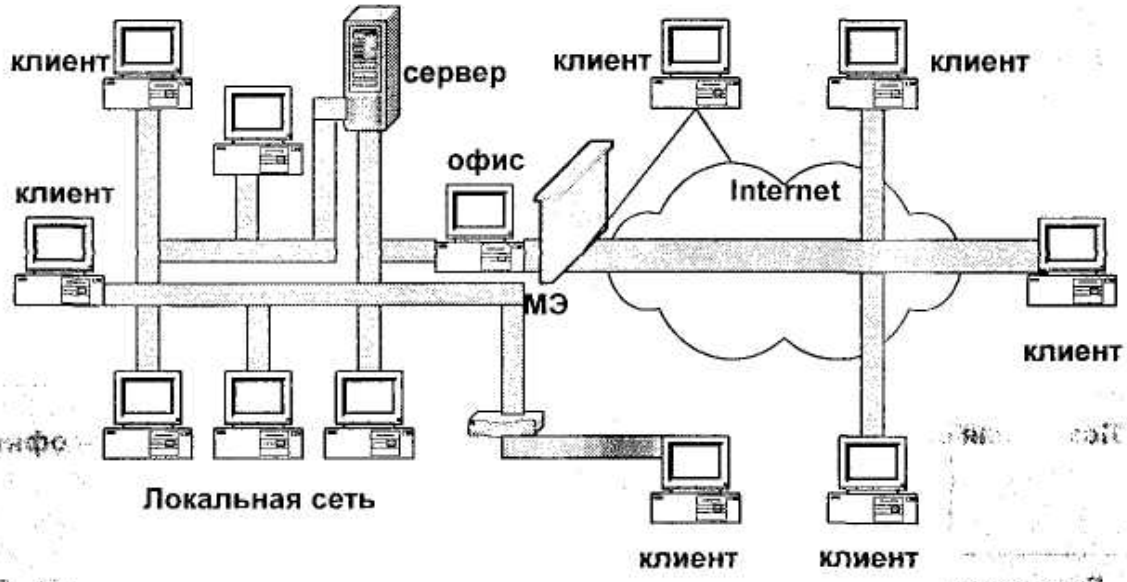


Рис. 42. Client/server VPN

Этот вариант похож на технологию виртуальных ЛВС (Virtual Local Area Network, VLAN), но вместо разделения трафика используется его шифрование.

Технология VLAN используется для структуризации современных ЛВС, построенных на базе коммутаторов, и для отделения одного типа трафика от другого. Независимо от адреса канального уровня (уникального, группового или широковещательного) смешение данных из разных VLAN невозможно. В то же время внутри одной VLAN кадры передаются как обычно, только на тот порт, на который указывает адрес назначения кадра.

Для задач построения VLAN разработан стандартный протокол IEEE 802.10 (принят в 1992 г.). Этот протокол предполагает, что пакеты VLAN имеют свои идентификаторы, которые и используются для их переключения. Полное название стандарта — IEEE 802.10 Interoperable LAN/MAN Security (MAN, Metropolitan Area Network — региональная или муниципальная сеть). Количество VLAN в пределах одной сети практически не ограничено. Протокол позволяет шифровать часть заголовка и информационное поле пакетов.

Узлы, входящие в VLAN, могут группироваться по различным признакам:

- по портам (классический и самый простой способ формирования VLAN, согласно которому каждому порту коммутатора соответствует номер VLAN);
- по MAC-адресам (принадлежность к VLAN определяется адресами доступа к среде (Media Access Control) — MAC-адресам сетевых пакетов);
- по номерам подсетей сетевого уровня (в данном случае VLAN является аналогом обычной подсети, которая известна по протоколам IP или IPX);
- по меткам (самый эффективный и надежный способ группирования узлов в VLAN, согласно которому номер VLAN добавляется к кадру, передаваемому между коммутаторами).

В глобальных сетях распространение получил аналог VLAN — технология MPLS (MultiProtocol Label Switching), которая также использует метки для разделения трафика и образования виртуальных каналов в IP-, ATM- и других сетях. Технология MPLS, основным поставщиком которой является компания Cisco Systems, может применяться только для связи "сеть — сеть" и не применима для соединения с отдельными узлами. Главный ее недостаток — данные разных пользователей хоть и не смешиваются, но все-таки их можно получить, прослушивая сетевой трафик. Кроме того, провайдер, предлагающий услуги MPLS, будет иметь доступ ко всей передаваемой информации. (Детальное рассмотрение этих технологий выходит за рамки данного учебного пособия.)

4.5.3. Extranet VPN

Extranet VPN предназначен для тех сетей, к которым подключаются так называемые пользователи "со стороны", уровень доверия к которым намного ниже, чем к своим сотрудникам. Extranet VPN позволяет разным компаниям связываться между собой и расширяет возможности компаний в электронной коммерции. Компании, желающие попасть на этот рынок, понимают, что недостаточно просто создать Web-сайт и предоставить доступ к нему всем желающим.

Доступ к определенным приложениям и главным компьютерам необходимо контролировать, шифровать данные для сохранения их конфиденциальности, когда они передаются через Internet, и устанавливать подлинность пользователей, чтобы быть уверенными, что они действительно имеют право доступа к сети.

Эта возможность оказывается особенно привлекательной для тех провайдеров, которые на данный момент предлагают лишь такие традиционные сервисы VPN, как объединение удаленных пользователей и филиалов компании в единую сеть. Установка и управление регулируемыми сервисами VPN внутри одной компании мало отличается от объединения пользователей сразу нескольких компаний, что и происходит в случаях с extranet.

"Между виртуальными частными сетями intranet и extranet нет особой разницы", — говорит Джо Барлетт, вице-президент по маркетингу провайдера широкополосных услуг HarvardNet. В своем сервисе RemoteConnect компания HarvardNet использует один и тот же подход как при предоставлении традиционных внутрикорпоративных VPN-услуг, так и при межкорпоративных услугах VPN-extranet. В обоих случаях компания прокладывает цифровую абонентскую линию DSL (Digital Subscriber Line) к DSL-маршрутизатору производства Cisco Systems, устанавливаемому на Web-узле компании. Такая конфигурация позволяет компании HarvardNet установить туннель на основе протокола IPSec между маршрутизатором компании Cisco и своими устройствами, установленными в других частях intranet или extranet.

Подобным образом поступает и компания Concentric Network, предлагая регулируемые услуги VPN, поддерживающие как внутрикорпоративную, так и внешнюю связь. Одним из клиентов Concentric, например, является фирма Hitachi Metals America Ltd., глобальный производитель собранной на заказ продукции из металла. Через регулируемую VPN Concentric предоставляет фирме Hitachi глобальную сеть, объединяющую ее филиалы, и extranet для ведения электронной торговли.

Некоторые финансовые учреждения используют услуги extranet компании Concentric для предоставления своим клиентам доступа к различным видам информации и услуг в зависимости от характера

их деятельности. Concentric использует такие возможности VPN, как аутентификация пользователей и контроль за доступом, для управления доступом к определенным приложениям и услугам, предлагаемым тем или иным финансовым учреждением.

Однако, несмотря на то, что компании HarvardNet и Concentric используют одинаковые VPN-услуги для предоставления удаленного доступа как внутри компании, так и к внешним клиентам, другие провайдеры услуг пытаются извлечь выгоду из рынка VPN-extranet, предлагая новые регулируемые услуги VPN, предназначенные специально для сетей extranet. Компания Global One предлагает сервис Global Internet VPN, использующий возможности туннелирования и шифрования данных протокола IPSec для безопасной передачи данных поверх Internet. Он дополняет Global Intranet VPN, предназначенный специально для КС intranet.

Одной из наиболее важных причин, делающих виртуальные сети extranet настолько популярными, является возможность совершать с их помощью безопасные сделки через Internet. Эта возможность привлекла внимание Национальной ассоциации кредитных союзов CUNA (Credit Union National Association), торговой ассоциации США, обслуживающей 11000 кредитных союзов и насчитывающей около 75 млн членов. "Мы ищем такое решение, с помощью которого наши члены могли бы конфиденциально вести с нами финансовые дела поверх безопасного Internet-соединения", — заявляет президент и генеральный директор CUNA Дэн Мика. В прошлом некоторые учреждения, входившие в состав CUNA, предлагали компьютерные банковские услуги, которые позволяли пользователям звонить в эти учреждения с помощью модема. CUNA обратилась к провайдеру услуг Aquis IP Communications, а также к компании Intelispan, специализирующейся на безопасных межкорпоративных коммуникациях, с тем чтобы они предоставили членам CUNA способ совершать электронные сделки с необходимым им высоким уровнем безопасности. Во всех VPN-услугах серии InteliGate компания Intelispan использует технологию шифрования открытым ключом. Эта технология обычно включает использование цифровых сертификатов, которые предоставляют более высокий уровень поль-

зовательской аутентификации, а также ту или иную систему регулирования ключей шифрования.

Помимо предоставления регулируемых услуг VPN-extranet корпорациям, провайдеры также ищут способы предоставления своих услуг провайдерам доступа к приложениям ASP (Application Service Providers). Многие ASP-провайдеры полагаются на провайдеров Internet, когда разговор заходит о связности между информационными центрами, где располагаются приложения, и точками присутствия в Internet, через которые получают доступ клиенты этих ASP-провайдеров. Однако ASP-провайдеры, пользующиеся вместо этого услугами VPN-extranet, получают не только необходимую связность компонентов, но и высокий уровень безопасности. Компания VPNX.com достигает такого результата, используя технологию шифрования открытым ключом компании VeriSign, включающую как программы, необходимые для безопасной передачи зашифрованных данных по Internet, так и цифровые сертификаты.

4.5.4. Remote Access VPN

Remote Access VPN — виртуальная частная сеть с удаленным доступом — позволяет мобильным пользователям получать доступ к КС своей компании через модем или канал ISDN. Он реализует защищенное взаимодействие между сегментом КС (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямо со своего собственного компьютера, на котором и устанавливается ПО, реализующее функции VPN. Компонент VPN для удаленного пользователя может быть выполнен как в программном, так и в программно-аппаратном виде. В первом случае ПО может быть как встроенным в ОС (например, в Windows 2000), так и разработанным специально (например, абонентский пункт "Континент-К"). Во втором случае для реализации VPN используются небольшие

устройства класса SOHO (Small Office\Home Office), которые не требуют серьезной настройки и могут быть использованы даже неквалифицированным персоналом (рис. 43).

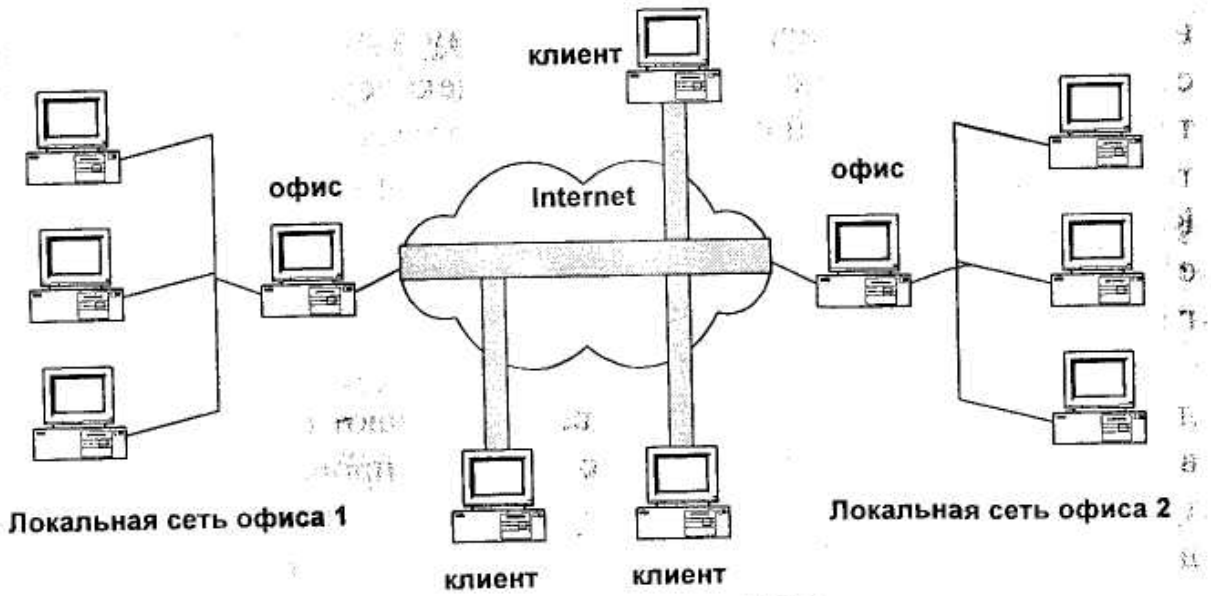


Рис. 43. Remote Access VPN

Уточним задачу. Пусть у некоторой организации имеется КС с набором информационных ресурсов (Web-серверы, почтовые серверы, специализированные базы данных и т.п.). По соображениям безопасности все эти ресурсы недоступны напрямую из публичных сетей. Тем не менее необходимо, чтобы сотрудники организации получали доступ к ресурсам своей КС, даже если они находятся за ее пределами. Для того чтобы был возможен такой доступ, КС подключается к опорной сети (как правило, к Internet, но иногда и к IP-сети крупного провайдера). Шлюз между опорной сетью провайдера и КС называется "домашним маршрутизатором" (Home Gateway). Эти шлюзы обычно используются в комбинации с МЭ для защиты КС от НСД. В задачу такого шлюза не входит маршрутизация между опорной и корпоративной сетями — она может вообще отсутствовать. Кроме того, как правило, в опорной и в КС используются разные схемы адресации.

Когда удаленному пользователю необходимо соединиться со своей КС, он сначала подключается к опорной сети (например, по коммутируемой линии). После установления этого соединения стро-

ится туннель до домашнего маршрутизатора КС клиента, который выдает удаленному пользователю адрес КС. Все пакеты, посылаемые на этот адрес из КС, поступают на домашний маршрутизатор. Он, в свою очередь, инкапсулирует их в пакеты с адресацией опорной сети и направляет по построенному туннелю через опорную сеть. На другом конце туннеля пакеты декапсулируются и приобретают тот вид, который они имели в КС пользователя. По описанной технологии пользователь получает коммутируемый доступ к своей КС из любой точки опорной сети провайдера, организовав таким образом свою виртуальную частную сеть (в английской терминологии — VPDN, Virtual Private Dialup Network) [2].

Существует несколько технологий предоставления услуг удаленного доступа к КС, но почти все они имеют одно общее свойство — при осуществлении такого доступа происходит построение туннеля с КС. Основное различие между разными технологиями доступа состоит в способе построения туннеля с КС и в используемом для этого протоколе. При создании защищенных каналов VPN-средства могут располагаться как в среде оборудования провайдера публичной сети, так и в среде оборудования предприятия. В зависимости от этого различают три варианта схемы образования защищенного канала:

- клиентская — все средства VPN размещают в сети предприятия;
- провайдерская — все средства VPN размещают в сети провайдера;
- смешанная — часть средств VPN размещены в сети провайдера, а часть — в сети предприятия.

В первом методе туннельное соединение устанавливается между домашним маршрутизатором КС и РС удаленного пользователя, во втором — между маршрутизатором опорной сети, к которому подключается удаленный пользователь, и домашним маршрутизатором КС.

1. Клиентские VPDN. При использовании первого метода задача удаленного доступа к КС возлагается на РС клиента, который имеет IP-адрес опорной сети и сам инициирует построение туннеля с домашним маршрутизатором (рис. 44). Для установления туннельного соединения на РС пользователя должно быть инсталлировано ПО,

в котором сконфигурирован IP-адрес опорного маршрутизатора сети. Необходимость поддержки и конфигурирования специализированного ПО на многих рабочих станциях, естественно, может оказаться неудобной для организаций, использующих этот метод предоставления своим сотрудникам доступа к КС.

Рис. 44. Клиентские VPDN

При построении туннелей от персонального компьютера клиента до домашнего маршрутизатора в качестве протоколов туннелирования фигурируют обычно PPTP и IPSec. Протокол PPTP инкапсулирует пакеты КС при отправке через туннель в открытом виде, что не гарантирует конфиденциальность и целостность передаваемой информации.

Для построения PPTP-туннелей в качестве клиентского ПО можно использовать утилиту Dialup Networking, входящую, например, в Windows 98. Если же строится туннель по протоколу IPSec, то информация передается в защищенном виде. В этом случае в качестве клиентского ПО рекомендуются решения от производителей имеющегося домашнего маршрутизатора (например, Cisco Secure VPN Client, Nortel Contivity), так как продукты различных производителей, работающие по этому протоколу, до сих пор не всегда и не полностью совместимы между собой.

Нежелательная особенность рассматриваемого метода состоит в том, что для подключения к своей КС пользователь должен получить доступ к ресурсам опорной сети. Обычно — к Internet, и многим организациям хотелось бы этого избежать.

В масштабах предприятия оно самостоятельно защищает данные, передаваемые по публичной сети, размещая VPN-шлюзы и VPN-клиенты в своей сети и на своей территории. Предприятие берет на себя полностью задачу обеспечения безопасности, а у провайдера только получает гарантированную (или негарантированную) пропускную способность. ЛВС предприятия защищаются чаще всего с помощью VPN-шлюзов. В условиях, когда услуги провайдера по поддержанию VPN не используются, такое решение наиболее экономично, так как один шлюз защищает сразу все узлы КС, расположенной позади него.

Отдельные компьютеры удаленных и мобильных сотрудников предприятия для организации защищенных связей должны самостоятельно поддерживать ПО VPN-клиента. С помощью собственного VPN-клиента эти компьютеры могут устанавливать защищенные каналы удаленного доступа с VPN-шлюзами собственного предприятия или со шлюзами предприятий-партнеров.

Достоинства:

- полный контроль администратора предприятия над защитой КС: выбор протоколов защищенного канала, настройка VPN на взаимодействие только с определенными абонентами или сетями, выбор стратегии смены паролей и т.п. Предприятие остается физическим владельцем устройств, которые содержат наиболее важную информацию о безопасности (такую, как пароли, ключи и т.д.);
- полный контроль над распределением пропускной способности защищенного канала для приложений. В том случае, когда провайдер предоставляет гарантии качества транспортного обслуживания, помещение пользователя является единственным местом для задания приоритетов исходящего трафика (поскольку у провайдера при получении зашифрованных пакетов не остается никаких признаков, на основании которых он мог бы осуществлять дифференцированное обслуживание). В этом случае VPN можно реализовать с использованием транспортных услуг многих провайдеров, не привязываясь к какому-нибудь определенному — главное, чтобы они предоставляли гарантии по пропускной способности канала и задержкам пакетов;

- безопасность реализуется "из-конца-в-конец": от места расположения пользователя до места назначения. Данные защищаются еще до выхода из помещения пользователя. Это свойство не всегда принимается во внимание, так как телефонные каналы и выделенные линии, которые используются для доступа к сети провайдера услуг Internet, чаще всего считаются вполне защищенными и без шифрования данных. Однако при передаче очень важных конфиденциальных данных такая защита может оказаться необходимой.

Недостатки:

- высокая стоимость VPN-устройств, а также их обслуживания;
- низкая степень масштабируемости VPN из-за децентрализованности применяемой схемы. При расширении VPN необходимо приобретать, устанавливать и конфигурировать новый VPN-шлюз в каждом вновь подключаемом филиале, а в каждом новом удаленном компьютере — клиентское ПО VPN. При использовании услуг провайдера все защищенные каналы проходят через несколько его шлюзов. Поэтому подключение нового филиала или удаленного пользователя требует гораздо меньших материальных и административных затрат, так как сводится в основном к внесению небольших изменений в конфигурационные настройки существующих шлюзов.

2. Провайдерские VPDN. На рис. 45 изображено альтернативное решение по доступу к КС — провайдерские VPDN.

Здесь задачу построения туннеля решает сервер сетевого доступа провайдера (NAS), т.е. маршрутизатор, к которому пользователь подключается при установлении коммутируемого соединения. В качестве туннельного используется протокол L2TP или L2F. После построения туннеля между NAS и домашним маршрутизатором уже между РС пользователя и домашним маршрутизатором его КС устанавливается PPP-соединение, при этом клиентский РС получает IP-адрес своей КС. Таким образом, построение туннеля с КС происходит незаметно для пользователя, для него все выглядит точно так же, как если бы он подключался непосредственно к КС. Пользователю нет необходимости иметь какое-либо дополнительное ПО на своем компьютере и заботиться о его конфигурировании, он может

применять любые программы удаленного соединения с сетью, в том числе любые версии утилиты Dialup Networking.

Рис. 45. Провайдерские VPDN

Рассмотрим типовую схему предоставления такого доступа. Для авторизации пользователей, подключающихся к NAS, на сети провайдера устанавливается сервер RADIUS. На RADIUS-сервере хранится база данных пользователей, причем их имена в ней имеют вид *имя_пользователя@имя_организации*. На этом же сервере хранится список организаций, имеющих домашние маршрутизаторы, и информация, необходимая для построения туннелей до них (IP-адреса, пароли и т.п.). При подключении пользователя из некоторой организации NAS посылает на авторизационный сервер запрос о том, нужно ли для данной организации (имя_организации) устанавливать туннельное соединение с домашним маршрутизатором, и если нужно, запрашивает его IP-адрес. Затем NAS устанавливает соединение с домашним маршрутизатором, используя полученную от авторизационного сервера информацию. Домашний маршрутизатор авторизует пользователя и выделяет ему IP-адреса из его КС.

Подобные технологии успешно используются уже несколько лет. Значительную популярность среди них приобрела упоминавшаяся выше технология MPLS, позволяющая строить высокопроизводительные сети с гарантированным качеством сервиса. Описанная схема легко трансформируется в пригодную для сети MPLS форму,

с той лишь разницей, что в качестве домашнего маршрутизатора используется любой из маршрутизаторов PE (Provider Edge), а RADIUS-сервер должен хранить вместо IP-адресов домашних маршрутизаторов метки виртуальных сетей клиентов.

Сравнительная характеристика различных способов организации коммутируемого доступа к частным сетям приведена в табл. 7.

Таблица 7. **Сравнительная характеристика организации коммутируемого доступа к частным сетям**

Протокол	Туннель	Клиентское ПО	Гарантия качества сервиса	Применение
PPTP	PC — HGW	MS DUN 1.2 VPN support	Нет	Редко
IPSec	PC — HGW	Cisco Remote VPN Client, Nortel Contivity	Нет	Редко (при передаче конфиденциальной информации)
L2TP	NAS — HGW	Любой PPP-клиент	Возможна	Часто
L2TP+ MPLS	NAS — PE	Любой PPP-клиент	Есть	Часто

Какие преимущества дает рассматриваемая технология корпоративному клиенту?

Во-первых, организация коммутируемого доступа много дешевле организации доступа по выделенной линии.

Второе преимущество вытекает из первого: пользователь не привязан к одному месту "проводом". Он может перемещаться в пространстве и пользоваться услугой именно там, где ему это необходимо. Главное здесь — это выбор оператора связи, имеющего максимальную зону присутствия как на территории одной страны, так и в международном масштабе.

Третье преимущество обусловлено уровнем развития современных технологий и заключается в том, что коммутируемый доступ перестал быть "медленным" видом связи. Большинство операторов предоставляет скорость подключения до 56 кбит/с, чего вполне достаточно для нужд единичного пользователя.

Унификация использования услуги является одним из основных условий ее успешного внедрения. Услуга должна быть максимально удобной для конечного пользователя, и ее функциональность ни в коем случае не должна нарушать привычный ритм его работы. Рассматриваемая технология предоставляет и это преимущество — гибкость политик обеспечения информационной безопасности ресурсов КС. Технология решает задачу надежной аутентификации пользователей, защиты от НСД, допускает различные разрешительные механизмы на основе задаваемых правил, ориентированных на группы, на отдельных пользователей либо на временную характеристику.

Кроме того, реализация услуги позволяет применять ее в гетерогенных сетях, в которых реализовано большое количество способов и методов организации связи.

И, наконец, услуга предусматривает возможность централизованного учета использованных ресурсов, что является немаловажным преимуществом для любой организации, тщательно учитывающей свою затратную часть.

Если говорить о всемирной доступности подобного сервиса, то лишь один-два российских оператора связи в настоящий момент способны справиться с поставленной задачей. Требуется учесть также и тот факт, что корпоративный рынок должен был насытиться услугами связи для того, чтобы осознать необходимость не просто потребления телекоммуникационного сервиса, но минимизации затратной части по данной статье.

Говоря о перспективах использования коммутируемого доступа на принципах туннелирования, заметим, что технология позволяет осуществить многие проекты, пока не реализованные из-за отсутствия удобного инструментария. Один из таких проектов основан на концепции использования "надомной рабочей силы", когда основное "производство" находится по месту жительства сотрудников компании, а общение с офисом обеспечивается посредством линии связи. Преимущество для работодателя — не нужно искать помещение под офис; не нужно его содержать; работник не тратит время на то, чтобы добраться до рабочего места; может использоваться высококвалифицированный персонал, привлечение которого ранее было за-

труднено (инвалиды, ухаживающие за иждивенцами и т.д.). Общее снижение издержек способно превысить 50 % себестоимости производимого товара или услуги.

Другим примером применения описанной технологии может стать объединение ее с технологиями передачи данных средствами мобильной (сотовой) связи в тех регионах, где подобные услуги предоставляются. При недоступности же мобильной связи работает традиционный вариант доступа через оператора проводной связи и сервис коммутируемого доступа. Таким образом, решается задача обеспечения глобальной доступности сервиса.

4.6. VPN-консорциум о виртуальных частных сетях

Недавно создан VPN-консорциум (Virtual Private Network Consortium) (http://www.vpnc.org). Это международная торговая ассоциация производителей VPN-продуктов, целями которой являются:

- реклама продуктов его членов потенциальным покупателям;
- решение вопросов совместимости продуктов разных производителей;
- обсуждение различных вопросов между производителями и пользователями;
- освещение VPN-технологий и стандартов в открытой печати;
- предоставление результатов тестирования по совместимости оборудования различных производителей.

Консорциум не создает стандарты, но он поддерживает стандарты организации IETF. В июне 2002 г. консорциумом был выпущен документ по VPN-технологиям "White paper on VPN technologies", в котором вводится определение и дается классификация VPN.

Согласно этому документу, VPN – это частная сеть передачи данных, использующая открытую телекоммуникационную инфраструктуру и сохраняющая при этом конфиденциальность передаваемых данных посредством применения протоколов туннелирования и средств защиты информации.

Выделяются четыре вида VPN:

- ***доверенная*** виртуальная частная сеть (trusted VPN);
- ***защищенная*** виртуальная частная сеть (secure VPN);

- ***смешанная*** виртуальная частная сеть (hybrid VPN);
- ***предоставляемая провайдером*** виртуальная частная сеть (provider-provisioned VPN).

Пока Internet еще не был так широко распространен, как сейчас, VPN состояли из одной или нескольких выделенных линий, арендованных у сервис-провайдера (СП). Каждая выделенная линия представляла собой канал связи в сети, управляемой пользователем. СП лишь иногда помогал пользователю управлять сетью. Основная идея заключалась в том, чтобы пользователь мог использовать эти выделенные линии так же, как и физические кабели, находящиеся в его локальной сети. Конфиденциальность в таких VPN основывалась на том, что СП гарантировал пользователю, что кроме него никто не будет использовать эти выделенные каналы передачи данных. Однако выделенные линии проходят через множество коммутаторов, и на каждом из них передаваемые данные могут быть скомпрометированы злоумышленником. Таким образом, пользователь доверяет СП обеспечение целостности каналов передачи данных и использование эффективных с его точки зрения средств защиты от прослушивания трафика. Это и есть ***доверенная VPN.***

Компании используют доверенные VPN, потому что хотят быть уверены, что их данные передаются только по каналам с параметрами, определенными в сервисном соглашении с СП, и эти каналы контролируются одним или несколькими доверенными СП. Пользователь уверен, что предоставленные ему каналы передачи данных удовлетворяют подписанному соглашению, а люди, которым пользователь не доверяет, не смогут получить доступ к каналу в любой части VPN или изменить поток данных. Заметим, что пользователю практически не реально знать каналы, по которым передаются его данные в доверенной VPN, или даже проверить – имеет ли место доверенная передача данных. Он должен полностью доверять своему СП.

По мере становления Internet как среды передачи корпоративных данных, проблемы обеспечения безопасности стали одним из основных вопросов, волнующих и пользователей и СП. Видя, что доверенные VPN не обеспечивают реальной безопасности передаваемых данных, производители стали создавать протоколы, которые позво-

лили шифровать трафик при входе в открытую сеть (например, Internet) и расшифровать его на выходе, когда он достигнет сети компании. Этот зашифрованный трафик передается по туннелю между двумя сетями: даже если злоумышленник видит трафик, он не сможет расшифровать и изменить его незаметно для принимающей стороны. Сети, построенные с использованием криптографических протоколов, получили название ***защищенных VPN***.

Основной причиной использования компаниями защищенных VPN является то, что они могут передавать конфиденциальную информацию чрез Internet без угрозы ее разглашения или изменения. Все, что передается по защищенной VPN, зашифровано так, что даже при перехвате этой информации ее нельзя будет прочитать даже с использованием самого дорогостоящего современного оборудования.

Доверенная и защищенная VPN не зависят от применяемых технических средств и могут существовать одновременно. Очевидно, что защищенные и доверенные VPN обладают совершенно разными свойствами. Защищенные VPN обеспечивают защиту информации, но не гарантируют доступность канала передачи информации. Доверенные VPN предоставляют гарантию, например, качества обслуживания, но не обеспечивают защиты передаваемой информации.

Немного позже появился новый тип доверенных VPN, использующих на этот раз в качестве среды передачи Internet, а не каналы, арендованные у телефонных компаний. Эти доверенные VPN все еще не обеспечивали безопасность передаваемых данных, но позволяли пользователям легко создавать сетевые сегменты внутри глобальных сетей. Кроме того, сегменты, созданные на базе доверенных VPN, могли контролироваться из одной точки, что упрощало их администрирование. Для них СП уже гарантировали качество обслуживания.

Защищенная VPN может быть частью доверенной VPN. Тогда образуется третий тип VPN, который лишь недавно появился на рынке – ***смешанная VPN***. Защищенная часть смешанной VPN должна контролироваться пользователем (путем настройки VPN-оборудования в его части сети) или тем же СП, который предоставляет доверенную часть смешанной VPN. Иногда вся смешанная VPN

защищается как защищенная VPN, но чаще защищается лишь часть смешанной VPN.

Случаи применения смешанных VPN в настоящее время еще только определяются. Типична ситуация, когда компания уже имеет доверенную VPN, в некоторых частях которой требуется особо защитить информацию.

Защищенная VPN может администрироваться ее пользователем или СП, предоставляющим услуги пользователю. Доверенные VPN и доверенные части смешанной VPN всегда администрируются СП. VPN, которые администрируются СП, называются ***предоставляемые провайдером VPN***. Конечно, пользователь может указать, как развернуть VPN, но инсталляция и поддержка предоставляемой провайдером VPN всегда осуществляется кем-то другим, но не пользователем.

Теперь рассмотрим основные требования к VPN и технологии их построения.

Существует одно очень важное общее требование ко всем типам VPN: *администратор VPN должен знать рамки своей VPN*. VPN любого типа существенно отличается от обычной сети. Таким образом, администратор VPN должен всегда знать, какой тип трафика должен присутствовать в его сети и какой не должен.

Требования к защищенной VPN:

1. *Весь трафик защищенной VPN должен быть зашифрован и аутентифицирован*. Многие протоколы, используемые для создания защищенных VPN, разрешают аутентификацию, но не могут шифровать данные. Хотя такие сети намного безопаснее, чем сети, где не используется аутентификация, они не являются VPN, так как не обеспечивают конфиденциальность передаваемых данных.
2. *Способы защиты в VPN должны быть согласованы между всеми участниками VPN*. Защищенная VPN имеет один или несколько туннелей, каждый из которых имеет две конечные точки. Администраторы конечных точек туннеля должны договориться о способах защиты туннеля.
3. *Никто за пределами VPN не может изменить характеристики VPN*. Для атакующего должно быть невозможно изменить ха-

рактеристики какой-либо части VPN, например, изменить протокол шифрования на более слабый или воздействовать на выбор ключей.

Технологии построения защищенных VPN:

1. *Протокол IPSec с поддержкой шифрования* как в туннельном, так и в транспортном режимах. Защищенные соединения могут быть установлены вручную или с помощью протокола IKE, при использовании цифровых сертификатов или заранее распределенных ключей. Протокол IPSec описан во многих документах RFC, включая 2401, 2406, 2407, 2408 и 2409.
2. *Протокол IPSec внутри L2TP* (как описано в RFC 3193) широко применяется при создании клиент-серверных VPN с удаленным доступом.

Обе эти технологии стандартизированы в IETF, и каждая из них реализована в совместимых между собой продуктах различных фирм.

Требования к доверенной VPN:

1. *Никто кроме доверенного СП VPN не может влиять на создание или модификацию путей в VPN.* Особое свойство доверенной VPN — то, что пользователь может доверить СП создание и контроль VPN. Никто кроме доверенных лиц не может изменить что-либо в VPN. Заметим, что некоторые VPN поддерживаются сразу несколькими СП. В этом случае пользователь доверяет группе СП.
2. *Никто кроме доверенного СП VPN не может изменять, удалять или вставлять свои данные в каналах VPN.* Доверенная VPN — это не просто набор каналов. Это также и потоки данных, которые циркулируют по каналам. Хотя каналы совместно используются одновременно несколькими пользователями одного СП, сам канал передачи данных принадлежат какой-либо определенной VPN, и никто, кроме СП, не может воздействовать на данные в этом канале. Изменения, внесенные некоторой третьей стороной, могут повлиять на характеристики самого канала, например, на объем трафика в канале.

Технологии построения доверенных VPN:

RFC 3031 описывает архитектуру MPLS, на основе которой разработаны следующие две технологии:

1. *MPLS с ограниченным распространением информации о маршрутизации в BGP*, что описано в draft-ietf-ppvpn-rfc2547bis и других соответствующих проектах предложений.
2. *Транспортировка фреймов уровня 2 с помощью MPLS*, что описано в draft-martini-l2circuittrans-mpls и других соответствующих проектах предложений.

Ни одна из этих двух технологий не была стандартизирована в IETF, но предполагается, что обе станут стандартами в будущем. Пока СП не отдают явного предпочтения какой-либо из них.

Технологии построения смешанных VPN:

1. *Любая технология построения защищенной VPN базируется на любой поддерживаемой технологии построения доверенной VPN.*

Необходимо отметить, что смешанная VPN защищена только в тех частях, где есть защищенные VPN. Это означает, что добавление защищенной VPN к доверенной VPN не увеличивает защищенность всей доверенной VPN, а только той ее части, что непосредственно защищена. Защищенная VPN наследует такие преимущества доверенной VPN, как гарантию качества обслуживания.

Требования к смешанным VPN:

1. *Границы адресов защищенной VPN внутри доверенной VPN должны быть четко определены.* В смешанной VPN защищенная VPN может являться подмножеством доверенной VPN, по аналогии, например, с тем, как один отдел в компании имеет собственную защищенную VPN внутри корпоративной доверенной VPN. Для любой пары адресов в смешанной VPN администратор должен точно знать, является ли трафик между этими адресами частью защищенной VPN.

Технологии построения смешанных VPN:

1. *Любая технология построения защищенной VPN базируется на любой технологии построения доверенной VPN.*

Необходимо отметить, что смешанная VPN защищена только в тех частях, где есть защищенные VPN. Это означает, что добавление защищенной VPN к доверенной VPN не увеличивает защищен-

ность всей доверенной VPN, а только той ее части, которая непосредственно защищена. Защищенная VPN наследует такие преимущества доверенной VPN, как гарантию качества обслуживания.

Требования к предоставляемым провайдером VPN:

1. *Свойства и границы адресов предоставляемой провайдером VPN должны быть четко определены.* Так как администратор VPN не может эмпирическим путем определить, что предоставляется СП, а что нет, СП должен предоставить список всех свойств и границ адресов и гарантировать, что они не изменятся в течение всего существования VPN. Это особенно важно для предоставляемых провайдером защищенных VPN, где реализация требования пользователя по защите должна быть четко соблюдена СП.

4.7. Рекомендации специалистов

Рекомендации по выбору средств построения корпоративных VPN целесообразно разделить на три группы в соответствии с организационно-правовой формой компании и уровнем секретности информации, которая будет обрабатываться в пределах проектируемой VPN.

- Государственные предприятия и организации, работающие с информацией, представляющей государственную тайну.
- Государственные учреждения, не работающие с государственной тайной.
- Коммерческие российские компании, желающие ограничить доступ к конфиденциальной (служебной, деловой, технической, экономической) информации, не составляющей государственной тайны.

В соответствии с положениями законодательства РФ для предприятий первой и второй группы на сегодня нет другой альтернативы, кроме как изначально ориентироваться на отечественных производителей VPN-продуктов, имеющих соответствующие лицензии и сертификаты Гостехкомиссии и ФАПСИ. Однако необходимо иметь в виду, что работа с информацией, представляющей государственную тайну, сопряжена с необходимостью выполнения доста-

точно большого объема различных организационно-технических мероприятий для удовлетворения большого количества разнообразных требований.

Так, VPN-продукты "ШИП" можно рекомендовать использовать в тех случаях, когда имеющиеся партнеры по производству/бизнесу уже работают с этим продуктом, а компания имеет надежные каналы связи для поддержки работоспособности ключевой системы.

Известные на рынке продукты ЗАСТАВА целесообразно использовать в тех случаях, когда компания имеет хорошие каналы связи с удаленными подразделениями и ей необходимо одновременно обеспечить наличие как защищенных, так и открытых соединений в Internet. Кроме того, ЗАСТАВА представляет собой оптимальное решение также и в тех случаях, когда компания предпочитает иметь масштабируемое решение по созданию собственной ключевой инфраструктуры, способной работать с изменяющимся количеством абонентов.

Наибольшей свободой выбора обладают компании третьей группы, которые сегодня могут использовать любые VPN-продукты, в том числе и западного производства. Здесь на первый план выходят такие параметры, как стоимость, функциональность, качество, производительность, криптостойкость, трудоемкость обслуживания, совместимость с уже имеющимся парком оборудования и т.д. Информация в табл. 8, подготовленная на базе открытых публикаций производителей, дает некоторое представление об этих параметрах.

Сравнение широко распространенных зарубежных продуктов, предназначенных для создания VPN, по расширенному набору параметров приведено в приложении I (источник — http://www.citforum.ru/nets/).

Если попытаться дать общую рекомендацию, то оптимальным решением с точки зрения обеспечения информационной безопасности является построение VPN на базе МЭ. Хорошим кандидатом на эту роль является многофункциональный продукт CheckPoint FW-1/VPN-1 или Cisco PIX Firewall, обладающий максимальной производительностью. Из отечественных МЭ можно порекомендовать продукт "ФПСУ-IP" компании "Амикон", DataGuard компании "Сигнал-Ком", а также комплекс МЭ ЗАСТАВА с модулем постро-

ния VPN. Довольно привлекательным решением выглядит построение корпоративной VPN на базе ЗАСТАВЫ с криптомодулем ВЕСТА, обладающим хорошей масштабируемостью, функциональностью и высокой криптостойкостью.

Таблица 8. **Сравнительные параметры некоторых VPN-продуктов**

Параметр	Windows NT/2000	Cisco IOS 12.x	CheckPoint FW-1	КК "ШИП"	ЗАСТАВА 2.5
1	2	3	4	5	6
Протокол, реализующий виртуальные туннели	PPTP/IPSec	L2TP/IPSec	IPSec	SKIP	SKIP
Способ реализации	Программный	Программный	Программный	Программно-аппаратный	Программный
Поддерживаемые аппаратные платформы	Intel	Cisco	Intel, Sun-SPARC, HP и др.	Intel	Intel, Sun-SPARC
Поддерживаемые ОС	-	IOS 12.x	Windows 95/98/NT/2000; Solaris; Linux, HP-UX и др.	FreeBSD	Windows 95/98/NT; Solaris
Аутентификация и поддержка целостности пакетов	Нет/Да	Да	Да	Да	Да
Поддержка внешн. Устройств усиленной аутентификации пользователей	Да	Нет	Да	Да	Да
Возможность центрального администрирования VPN	Да	Да	Да	Нет	Да
Используемые алгоритмы шифрования	DES; 3DES	DES; 3DES	DES; 3DES; CAST; IDEA и др.	ГОСТ 28147-89	ГОСТ 28147-89; ВЕСТА-2М; DES; 3DES
Максим. криптостойкость (длина ключа, бит)	168	168	168	256	256
Количество одновременно используемых криптоалгоритмов				1	256

Окончание табл.8

1	2	3	4	5	6
Наличие открытого криптоинтерфейса	Да	Нет	Нет	Нет	Да
Ведение журнала аудита	Да	Да	Да	Да	Да
Максимальная производительность (АП — аппаратная платформа)	зависит от АП	250 МБайт/с	зависит от АП	8 МБайт/с	зависит от АП
Наличие клиентских; серверных; шлюзовых частей	Да Да Нет	Да Нет Да	Да Да Да	Да Нет Да	Да Да Да
Средства построения собственной ключевой системы	Нет	Нет	Да	Да	Да
Возможность каскадирования туннелей	Да	Да	Да	Нет	Нет
Наличие сертификата Гостехкомиссии	Нет	Да, на отдельные изделия	Да, на партии изделий	Нет	Да, на производство
Наличие сертификата ФАПСИ (в т.ч. на криптомодули)	Нет	Нет	Нет	Да	Да
Поддержка внешних систем распределения ключей и сертификатов (PKI)	Да	Да	Да	Нет	Да
Поддержка внешних средств защиты от НСД				Аккорд	Аккорд; Dallas Lock; Secur ID

Контрольные вопросы по разделу 4

1. Какие требования предъявляются к продуктам построения VPN? Поясните их.
2. Расскажите о вариантах реализации VPN, их преимуществах и недостатках. Приведите примеры продуктов.
3. Какие функции в VPN выполняют шлюзы и клиенты?
4. Какие сетевые средства реализуют протоколы создания VPN?
5. Сравните достоинства и недостатки средств создания VPN различных категорий.

6. Расскажите о построении VPN на базе сетевой ОС. Приведите примеры.
7. Расскажите о построении VPN на базе маршрутизаторов. Приведите примеры.
8. Расскажите о построении VPN на базе МЭ. Приведите примеры.
9. Дайте определение МЭ и расскажите об их назначении, компонентах, типах и схемах подключения в сети.
10. Расскажите о построении VPN на базе ПО. Приведите примеры.
11. Расскажите о построении VPN на базе аппаратных средств. Приведите примеры.
12. Какие виды VPN Вам известны и какие задачи они решают?
13. Расскажите об Intranet VPN. Приведите схему построения.
14. Расскажите о Client/server VPN. Нарисуйте схему построения.
15. Расскажите об Extranet VPN. Схематично представьте способ построения.
16. Расскажите о VPN с удаленным доступом и их вариантах.
17. Расскажите о документе, посвященным видам VPN и технологиям их построения, выпущенном VPN-консорциумом.
18. Каковы рекомендации специалистов по выбору средств для построения VPN и по каким основным параметрам их лучше всего сравнивать?

5. РОССИЙСКИЕ ПРОДУКТЫ ДЛЯ СОЗДАНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

5.1. Аппаратно-программный комплекс защиты информации "Континент-К"

Аппаратно-программный комплекс (АПК) "Континент-К" сертифицирован в Гостехкомиссии по 3 классу защищенности (сертификат № 352 от 28.08.2000) для МЭ и сертифицирован в ФАПСИ (сертификат соответствия ФАПСИ СФ/124-0489 от 17.08.2001 г.) на соответствие требованиям к средствам криптографической защиты конфиденциальной информации. Криптографическое ядро (СКЗИ "КриптоПро CSP") и используемое ПО абонентского пункта АПК "Континент-К" (ПО АП) сертифицированы ФАПСИ (сертификаты соответствия ФАПСИ СФ/114-0441 от 11.03.2000 г. и СФ/124-0460 от 20.04.2001 г.).

АПК "Континент-К" предназначен для построения VPN на основе глобальных сетей общего пользования, использующих протоколы семейства TCP/IP (например, Internet), и обеспечивает:

- эффективную защиту конфиденциальной информации, передаваемой по сетям общего пользования;
- полную "прозрачность" для конечных пользователей;
- защиту информационных систем от атак со стороны сетей общего пользования;
- безопасный доступ к ресурсам сетей общего пользования.

В качестве составных частей VPN могут выступать ЛВС организации, их сегменты и отдельные компьютеры (в том числе переносные или домашние компьютеры руководителей и сотрудников).

Аппаратно-программный комплекс "Континент-К" отличает:

- эффективная и надежная защита информации в гетерогенных сетях;
- отсутствие вмешательства в существующие технологии обработки информации, полная прозрачность для приложений и пользователей;
- централизованное управление настройками системы и оперативный мониторинг ее состояния;
- совмещение в одном устройстве функций межсетевого экрана и криптографического маршрутизатора;
- возможность разграничивать доступ от нескольких внутренних защищаемых сегментов;
- защита мобильных и удаленных пользователей даже в случае динамического распределения IP-адресов;
- удобный графический интерфейс программы управления;
- простота в настройке и обслуживании;
- наличие положительного заключения ФАПСИ и сертификата ГТК.

АПК "Континент-К" обладает широким спектром возможностей.

- Надежная криптографическая защита передаваемых данных по ГОСТ 28147-89.
- Маршрутизация сетевого трафика (статическая).
- Фильтрация сетевого трафика.
- Обеспечение доступа мобильных и удаленных пользователей.
- Обеспечение высокой пропускной способности.
- Низкие накладные расходы.
- Низкая стоимость эксплуатации корпоративной сети за счет использования сетей общего пользования вместо собственных или арендуемых линий связи.
- Возможность сжатия передаваемой информации.
- Скрытие внутренней структуры защищаемой сети.
- Создание информационных подсистем с разделением доступа на физическом уровне.
- Поддержка возможности удаленного управления коммутационным оборудованием.

- Высокая надежность комплекса (в т.ч. за счет "горячего", т.е. аппаратного резервирования).
- Поддержка до 15 внутренних интерфейсов.
- Неограниченная масштабируемость комплекса (регистрация до 500 пользователей на каждом сервере доступа; возможность объединения в сеть до 5000 VPN устройств).
- Простота установки и настройки.
- Централизованное управление сетью.
- Удобство администрирования.
- Возможность ролевого управления комплексом.
- Контроль за действиями администратора.
- Ведение системных журналов.
- Необслуживаемый режим работы.
- Оповещение администратора (в реальном режиме времени) о событиях, требующих оперативного вмешательства.
- Поддержка динамического распределения адресов при доступе удаленных пользователей.
- Абсолютная прозрачность для всех приложений.
- Поддержка мультимедиа-сервисов.
- Возможность организации доступа к ресурсам сетей общего пользования из защищаемых сетей.

В состав комплекса входят: центр управления сетью (ЦУС); криптошлюз (КШ); программа управления сетью (ПУ); абонентский пункт (АП); сервер доступа (СД) и программа управления сервером доступа (ПУ СД).

Криптографический шлюз (КШ), представляющий собой специализированное программно-аппаратное устройство, функционирующее под управлением защищенной ОС FreeBSD, обеспечивает криптографическую защиту информации при ее передаче по открытым каналам сетей общего пользования и защиту внутренних сегментов сети от проникновения извне. Криптошлюз обеспечивает:

- прием и передачу пакетов по протоколам семейства TCP/IP (статическая маршрутизация);

- шифрование передаваемых и принимаемых IP-пакетов по алгоритму ГОСТ 28147-89 в режиме гаммирования с обратной связью;
- сжатие защищаемых данных;
- защиту данных от искажения по алгоритму ГОСТ 28147-89, режим имитовставки;
- фильтрацию IP-пакетов в соответствии с заданными правилами фильтрации на основе IP-адресов отправителя и получателя, допустимых значений полей заголовка, используемых портов UDP/TCP и флагов TCP/IP-пакета;
- скрытие внутренней структуры защищаемого сегмента сети (NAT);
- криптографическую аутентификацию удаленных абонентов;
- периодическое оповещение ЦУС о своей активности;
- регистрацию событий, связанных с работой КШ;
- оповещение администратора (в реальном режиме времени) о событиях, требующих оперативного вмешательства;
- идентификацию и аутентификацию администратора при запуске КШ (средствами сертифицированного в ФАПСИ электронного замка "Соболь");
- контроль целостности программного обеспечения КШ до загрузки операционной системы (средствами ЭЗ "Соболь").

Центр управления сетью (ЦУС) осуществляет управление работой всех КШ, входящих в состав системы защиты. ЦУС осуществляет контроль за состоянием всех зарегистрированных на нем КШ, проводит рассылку ключевой информации, предоставляет администратору функции удаленного управления КШ, обеспечивает получение и хранение содержимого системных журналов КШ, а также ведение журнала событий НСД. ЦУС обеспечивает:

- аутентификацию КШ и консолей управления;
- контроль текущего состояния всех КШ системы;
- хранение информации о состоянии системы защиты (сети КШ);
- централизованное управление криптографическими ключами и настройками каждого КШ сети;
- взаимодействие с программой управления;

- регистрацию событий по управлению и изменению параметров КШ;
- резервное копирование служебных данных на компьютер управления;
- детализацию информации о попытках несанкционированного доступа;
- получение журналов регистрации от всех имеющихся КШ и их хранение.

Программа управления предназначена для централизованного управления всеми КШ, работающими под управлением одного ЦУС. Эта программа позволяет:

- отображать информацию о текущем состоянии всех имеющихся КШ;
- добавлять в систему новые КШ, изменять сведения о существующем КШ или удалять его;
- централизованно управлять настройками КШ;
- управлять правилами маршрутизации КШ;
- управлять ключами шифрования;
- анализировать содержание журналов регистрации КШ.

Абонентский пункт (АП) — ПО, устанавливаемое на любой компьютер и позволяющее удаленному пользователю связываться по защищенному каналу с сетью, защищенной АПК "Континент-К". АП, функционирующий под управлением ОС Windows 95/98/NT/2000, позволяет осуществить:

- удаленный доступ к ресурсам защищаемой сети по защищенному каналу;
- идентификацию и аутентификацию пользователя с использованием цифровых сертификатов;
- функционирование при условии динамического распределения IP-адресов.

В зависимости от конфигурации АП может либо запрещать все незащищенные соединения (например, с сетью Internet), либо разрешать их, что позволяет строить гибкую политику сетевой безопасности.

5.2. Программные продукты компании "ЭЛВИС+"

Программные продукты семейства ЗАСТАВА реализуют технологию защищенных виртуальных сетей, выделяя собственные виртуальные защищенные каналы в общедоступных линиях связи и открытых сетях типа Internet. Продукты сетевой защиты ЗАСТАВА, основанные на стандартах IPSec, обеспечивают криптографически стойкую защиту трафика между географически разнесенными ЛВС филиалов и штаб-квартиры предприятия, а также отдельными удаленными компьютерами работников, находящихся вне его пределов в любой точке мира, где есть телефонная связь или Internet.

VPN-продукты ЗАСТАВА совместимы с индустриальным протоколом SKIP v.2 и с продуктами всех производителей, поддерживающих этот стандарт: SUN Microsystems, CheckPoint и т.д. VPN ЗАСТАВА дополнен протоколом IKE.

Полнота сетевой системы защиты, создаваемой с использованием VPN-продуктов ЗАСТАВА, обеспечивается следующей функциональностью.

- VPN-продукты ЗАСТАВА закрывают отдельные компьютеры, серверы и целые сегменты сети, образуя жесткий периметр VPN и решая весь спектр задач сетевой безопасности, включая аутентификацию пользователей.
- Продукты централизованного управления позволяют управлять VPN, реализуя гибкую корпоративную политику сетевой безопасности по отношению к каждому сетевому ресурсу, пользователю и даже приложению.
- Входящий в состав продуктового ряда межсетевой экран ЗАСТАВА обеспечивает защиту КС от атак извне, контролируя трафик в точках взаимодействия закрытого периметра VPN с открытыми сетями типа Internet, а также обеспечивает сегментирование внутренних сетей.
- Система регистрации фиксирует попытки взлома защищенного периметра VPN.
- Открытые интерфейсы VPN ЗАСТАВА позволяют наращивать функциональность системы без дополнительных затрат.

В состав программных продуктов семейства ЗАСТАВА входит ряд решений.

1. ЗАСТАВА-Клиент — обеспечивают защиту пользовательских рабочих станций от несанкционированного доступа из внешних сетей, а также организацию защищенных соединений с отдельными компьютерами и/или с компьютерами из сегментов ЛВС, защищенных программными продуктами семейства ЗАСТАВА и/или SKIP-продуктами других производителей. ЗАСТАВА-Клиент поставляется как программный пакет, который устанавливается на компьютере пользователя. Перенастройки работающего на этом компьютере программного обеспечения не требуется. Продукт поставляется в двух модификациях: ЗАСТАВА-Персональный Клиент (ЗПК) и ЗАСТАВА-Корпоративный Клиент (ЗКК). При использовании продукта ЗПК политика информационной безопасности задается самим пользователем с помощью набора конфигурационных правил посредством интерфейса командной строки или графического интерфейса пользователя. ЗКК не имеет интерфейса пользователя, что позволяет пользователям эксплуатировать продукт без специальной подготовки. Конфигурирование продукта происходит удаленно администратором безопасности. На удаленные компьютеры конфигурация загружается с помощью дискеты или смарт-карты.

2. ЗАСТАВА-Сервер (ЗС) обеспечивает защиту серверов от НСД из внешних сетей, а также организацию защищенных соединений с отдельными компьютерами и/или с компьютерами из сегментов ЛВС, защищенных программными продуктами семейства ЗАСТАВА и/или SKIP-продуктами других производителей. ЗС поставляется как программный пакет, который устанавливается на компьютере, выполняющем функции сервера. Перенастройки работающего на сервере ПО не требуется. Политика информационной безопасности задается пользователем с помощью набора конфигурационных правил — локально или удаленно посредством интерфейса командной строки или графического интерфейса пользователя.

3. ЗАСТАВА-Офис (ЗО) обеспечивает коллективную защиту сегмента ЛВС от НСД из внешних сетей, а также организацию защищенных соединений с отдельными компьютерами и/или с компьютерами из сегментов ЛВС, защищенных программными продуктами семейства ЗАСТАВА и/или SKIP-продуктами других производителей. ЗО поставляется как программный пакет, который устанавлива-

ется на компьютере, выполняющем функции сетевого шлюза (Gateway) между защищаемым сегментом сети и внешними локальными (LAN) или глобальными (WAN) сетями. Политика информационной безопасности задается самим пользователем с помощью набора конфигурационных правил — локально или удаленно посредством интерфейса командной строки или графического интерфейса пользователя.

ЗАСТАВА работает на платформах Windows 95/NT и Solaris Intel/SPARC (табл. 9).

Таблица 9. **Поддерживаемые платформы**

Продукт	Win 95/98	Win NT	Solaris Intel	Solaris Sparc
ЗАСТАВА-Корпоративный Клиент	+	+		
ЗАСТАВА-Персональный Клиент	+	+	+	+
ЗАСТАВА-Сервер		+	+	+
ЗАСТАВА-Офис		+	+	+
Сервер сертификатов ЗАСТАВА		+		

Скорость обработки на различных аппаратных платформах и увеличение длины IP-пакета при использовании различных алгоритмов для продуктов ЗАСТАВА представлены в табл. 10.

Таблица 10. **Технические характеристики**

	Алгоритм (разработчик)		
	DES	ГОСТ (Анкад)	ВЕСТА (ЛАН Крипто)
Pentium II/300, скорость обработки, Мбит/с	8	6	13
SPARC Ultra 450, скорость обработки, Мбит/с	38	17	61
Увеличение длины IP-пакета, байт	64	88	85

Функциональные характеристики VPN-продуктов ЗАСТАВА (кроме МЭ ЗАСТАВА, но включая сервер сертификатов — СС) приведены в табл. 11.

Таблица 11. **Функциональные характеристики VPN-продуктов ЗАСТАВА**

Характеристики	ЗКК	ЗПК	ЗС	ЗО	СС
Поддержка IPsec (SKIP v.2)	Y	Y	Y	Y	-
Ipsec compliance: RFC1825-29, 1851	Y	Y	Y	Y	-
ручное управление ключами IPsec	Y	Y	Y	Y	-
CDP	Y	Y	Y	Y	Y
LDAP	N	N	N	N	Y
Open CryptoAPI™	Y	Y	Y	Y	-
X509 v1-v3 (Diffie-Hellman)	Y	Y	Y	Y	Y
UDH (Unsigned Diffie-Hellman)	Y	Y	Y	Y	Y
Одновременное использование различных алгоритмов защиты и различные длины ключей для различных IP соединений	Y	Y	Y	Y	-
Одновременная поддержка защищенных и открытых IP-соединений	Y	Y	Y	Y	-
Поддержка защищенных соединений с мобильными компьютерами, не имеющими постоянного IP адреса (nomadic)	N	N	Y	Y	-
Туннелирование трафика	N	N	N	Y	-
Аутентификация пользователя/администратора с использованием постоянного пароля	Y	Y	Y	Y	Y
Аутентификация пользователя/администратора через PKCS#11 интерфейс с использованием смарт-карт, токенов и дискет	Y	Y	Y	Y	N
Поддержка SecurID	Y	Y	Y	Y	N
Различная политика безопасности на разных сетевых интерфейсах	N	N	Y	Y	-
Локальная политика безопасности (ЛПБ) управляется администратором и не может быть изменена локальным пользователем	Y	N	N	N	-
ЛПБ определяется конечным пользователем через графический интерфейс пользователя (ГИП)	N	Y	Y	Y	-
ЛПБ полностью хранится на внешнем носителе или дискете	Y	Y	Y	Y	-
Удаленное или локальное конфигурирование администратором безопасности через ГИП	Y	Y	Y	Y	-
Удаленное или локальное конфигурирование администратором безопасности через интерфейс командной строки (UNIX)	N	N	Y	Y	-
Защита канала, по которму осуществляется удаленное конфигурирование (UNIX)	-	Y	Y	Y	-
Функции локального регистрирования (Windows)	Y	Y	Y	Y	-
Функции локальной сигнализации (Windows)	Y	Y	Y	Y	-
Installation wizard (Windows)	Y	Y	Y	Y	Y
SVR4 package installation (UNIX)	-	Y	Y	Y	-
Ethernet и FastEthernet	Y	Y	Y	Y	Y
PPP и SLIP	Y	Y	Y	Y	Y

5.3. VPN-решения компании "Инфотекс"

Компания "Инфотекс" создает программные продукты для организации VPN, которые позволяют повысить эффективность управления бизнес-процессами и использовать новейшие достижения информационных технологий на рабочем месте и вне офиса.

Вся линия продуктов ViPNet имеет сертификаты соответствия:

- Сертификат Гостехкомиссии при Президенте РФ №545 от 17.12.01;
- Сертификат Гостехкомиссии при Президенте РФ №546 от 17.12.01;
- Сертификат ФАПСИ на СКЗИ "Домен-К" по классу защищенности КС1 №СФ/114-0470 от 01.07.01;
- Сертификат ФАПСИ на СКЗИ "Домен-К" по классу защищенности КС2 №СФ/124-0471 от 01.07.01.

В основе решений ViPNet – пакет программ, являющийся универсальным программным средством для создания VPN любой конфигурации, интегрированных с системой распределенных персональных и межсетевых экранов.

ViPNet включает в себя ряд подсистем.

- Распределенную систему межсетевых и персональных сетевых экранов, защищающую информационные ресурсы и пользователей как от внешних, так и внутренних сетевых атак.
- Распределенную систему межсетевого и персонального шифрования трафика любых приложений и операционной системы, гарантирующую целостность и конфиденциальность информации, как на внешних, так и внутренних коммуникациях, и обеспечивающую разграничение доступа к техническим и информационным ресурсам.
- Систему ЭЦП и шифрования информации на прикладном уровне, обеспечивающую достоверность и юридическую значимость документов и совершаемых действий.
- Систему прозрачного для программных приложений шифрования данных при сохранении указанных данных в процессе работы этих приложений на сетевых и локальных жестких дисках, других носителях. Система обеспечивает целостность и недоступность информации для несанкционированного использования в процессе ее хранения.

- Систему контроля и управления связями, правами и полномочиями защищенных объектов корпоративной сети, обеспечивающую автоматизированное управление политиками безопасности в корпоративной сети.
- Комбинированную систему управления ключами, включающую подсистему асимметричного распределения ключей (PKI), обеспечивающую информационную независимость пользователей в рамках заданных политик безопасности от центральной администрации, и подсистему распределения симметричных ключей, гарантирующую высокую надежность и безопасность всех элементов централизованного управления средствами ViPNet, в том числе защиту подсистемы ИОК.
- Систему, обеспечивающую защищенное взаимодействие между разными виртуальными частными сетями ViPNet путем взаимного согласования между администрациями сетей допустимых межобъектных связей и политик безопасности.

Технология ViPNet обеспечивает следующие функции.

- Быстрое развертывание корпоративных защищенных решений на базе имеющихся у корпорации ЛВС, доступных ресурсов глобальных (включая Internet) и ведомственных телекоммуникационных сетей, телефонных и выделенных каналов связи, средств стационарной, спутниковой и мобильной радиосвязи и др. При этом в полной мере может использоваться уже имеющееся у корпорации оборудование (компьютеры, серверы, маршрутизаторы, коммутаторы, МЭ и т.д.).
- Создание внутри распределенной КС информационно–независимых виртуальных защищенных контуров, включающих как отдельные компьютеры, так и сегменты сетей, для обеспечения функционирования в единой телекоммуникационной среде различных по конфиденциальности или назначению информационных задач. Такие контуры создаются только исходя из логики требуемых (разрешенных) информационных связей, независимо от приложений, сетевой операционной системы, без каких-либо настроек сетевого оборудования. При этом достигается еще одно очень важное свойство таких виртуальных сетей – независимость режимов безопасности, установленных в VPN, от сетевых администраторов,

управляющих различными физическими сегментами большой корпоративной сети, от ошибочных или преднамеренных действий с их стороны, представляющих одну из наиболее вероятных и опасных угроз на сети.

- Защиту, как ЛВС в целом, их сегментов, так и отдельных компьютеров и другого оборудования от несанкционированного доступа и различных атак, как из внешних, так и из внутренних сетей.
- Поддержку защищенной работы мобильных и удаленных пользователей корпоративной сети. Организацию контролируемого и безопасного для корпоративной сети подключения внешних пользователей для защищенного обмена информацией с ресурсами корпоративной сети.
- Организацию безопасного для ЛВС подключения отдельных рабочих станций этих сетей к открытым ресурсам сети Internet и исключение риска атаки из Internet на всю ЛВС через подключенные к открытым ресурсам компьютеры ЛВС.
- Защиту (конфиденциальность, подлинность и целостность) любого вида трафика, передаваемого между любыми компонентами сети, будь то рабочая станция (мобильная, удаленная, локальная), информационные серверы доступа, сетевые устройства или узлы. При этом становится недоступной для перехвата из сети, в том числе для участников VPN, и любая парольная информация различных приложений, баз данных, почтовых серверов и др., что существенно повышает безопасность этих прикладных систем.
- Защиту управляющего трафика для систем и средств удаленного управления объектами сети: маршрутизаторами, межсетевыми экранами, серверами и пр., а также самих средств удаленного управления от возможных атак из глобальной или корпоративной сети.
- Контроль доступа к любому узлу (рабочая станция, сервер, маршрутизатор и т.д.) и сегменту сети (ЛВС, сегмент ЛВС, группа сегментов сети и т.д.), включая фильтрацию трафика, правила которой могут быть определены для каждого узла отдельно, как с помощью набора стандартных настроек, так и с помощью индивидуальной настройки.
- Защиту от НСД к информационным ресурсам корпоративной сети, хранимым на рабочих станциях (мобильных, удаленных и ло-

кальных), серверах (WWW, FTP, SMTP, SQL, файл-серверах и т.д.) и других хранилищах группового доступа.

- Организацию безопасной работы участников VPN с совместным информационным групповым и/или корпоративным информационным ресурсом.
- Аутентификацию пользователей и сетевых объектов VPN на основе использования как системы симметричных ключей, так и ИОК и сертификатов стандарта X.509.
- Оперативное управление распределенной VPN-сетью (включая систему распределенных сетевых экранов) и политикой информационной безопасности на сети из одного центра с возможностью делегирования части полномочий локальным администраторам.
- Исключение использования недекларированных возможностей операционных систем и приложений для совершения информационных атак, кражи секретных ключей и сетевых паролей.

Технология ViPNet представляет собой сертифицированный программный комплекс, позволяющий организовать виртуальную сеть, защищенную от НСД по классу 1В для автоматизированных систем и 3 классу для МЭ.

В качестве криптографического ядра системы используется "Домен-К" – сертифицированная ФАПСИ разработка ОАО "Инфотекс". Уникальное сочетание симметричных процедур распределения ключей и технологий ИОК, ЭЦП, автоматических процедур ключевого взаимодействия обеспечивает высокий уровень безопасности в системе.

Полностью безопасная работа пользователей и применения информационных и технических ресурсов обеспечивается при установке средств защиты на каждый компьютер, участвующий в VPN. Информация, которой данный компьютер обменивается с другими компьютерами, становится недоступной для любых других компьютеров, не участвующих в данном соединении. Информация, которая расположена на самом компьютере, недоступна с любого компьютера, не участвующего в VPN. Доступ с компьютеров, участвующих в VPN, определяется наличием соответствующих связей, настройкой фильтров и полностью контролируется администраторами безопасности.

При взаимодействии между компьютерами, включенными в VPN-сеть, обеспечивается установление между такими компьютерами защищенных соединений. При этом в реальном масштабе времени осуществляется шифрование всего IP-трафика между компьютерами по алгоритму, рекомендованному ГОСТ 28147-89, а также, при необходимости, по другим алгоритмам (DES, 3DES, RC6). Одновременно производится инкапсуляция всех типов IP-пакетов в единый тип, что полностью скрывает структуру информационного обмена. При работе через межсетевые экраны других производителей, осуществляющих преобразование адресов (функция NAT), инкапсуляция всех типов пакетов производится в единый тип UDP – формата, что соответствует предложениям IETF (Internet Engineering Task Force) по обеспечению и стандартизации совместной работы VPN и МЭ. Это обеспечивает совместимость технологии ViPNet не только с собственной системой распределенных сетевых экранов, но и с сетевыми экранами других производителей, придерживающихся рекомендаций IETF.

Если в ЛВС возможно выделение участков сети, где организационными мерами исключен доступ посторонних лиц, то эти группы компьютеров могут защищаться совместно. В этом случае не требуется установка клиентских программных средств ViPNet на каждый компьютер и возможно ограничиться установкой компонента сети под названием ViPNet Coordinator на шлюзовой компьютер данного участка сети.

Компьютеры виртуальной сети могут располагаться внутри ЛВС любого типа, поддерживающих IP-протокол, находиться за другими типами сетевых экранов, иметь реальные или виртуальные адреса, подключаться через общедоступные сети путем выделенных или коммутируемых соединений.

Часто при соединении с другими сетями, использующими внутреннюю адресную структуру, возникает проблема конфликта IP-адресов. Технология ViPNet с использованием специальных механизмов предоставляет возможность не перестраивать в этом случае имеющуюся адресную структуру. Каждый из ее объектов автоматически формирует для других объектов уникальный виртуальный адрес, который и может быть использован приложением.

Основой всех программ для виртуальной сети является ViPNet-драйвер, взаимодействующий непосредственно с драйвером сетевого интерфейса, что обеспечивает независимость программы от операционной системы и ее приложений. Драйвер контролирует весь IP-трафик, поступающий и исходящий из компьютера, и выполняет его фильтрацию по многочисленным параметрам и при необходимости – шифрование и инкапсуляцию.

Программный комплекс ViPNet включает в свой состав следующие основные компоненты: ViPNet [Администратор], ViPNet [Координатор], ViPNet [Клиент].

ViPNet [Администратор] создает логическую инфраструктуру виртуальной сети, определяет политики безопасности в ней, осуществляет мониторинг и управление объектами сети. Он также формирует симметричную ключевую информацию и первичную парольную информацию для объектов сети, выпускает сертификаты открытых ключей для объектов сети.

ViPNet [Координатор]:

- выполняет маршрутизацию почтовых и управляющих защищенных сообщений при взаимодействии объектов сети между собой и ViPNet [Администратором];
- в реальном времени осуществляет регистрацию и предоставление информации о состоянии объектов сети, их местоположении, значении их IP-адресов и др.;
- обеспечивает работу защищенных компьютеров ЛВС в VPN от имени одного адреса (функция proxy);
- осуществляет туннелирование пакетов от обслуживаемой ViPNet [Координатором] группы незащищенных компьютеров ЛВС для передачи трафика от них к другим объектам; VPN в зашифрованном виде по открытым каналам Internet/intranet;
- фильтрует трафик от источников, не входящих в состав VPN, в соответствии с заданной политикой безопасности (функция МЭ);
- обеспечивает возможность работы защищенных по технологии ViPNet компьютеров ЛВС через МЭ и прокси-серверы других производителей.

ViPNet [Клиент] обеспечивает защиту информации при ее передаче в сеть, а также защиту от доступа к ресурсам компьютера и атак на него из локальных и глобальных сетей. При этом ViPNet [Клиент] может быть установлен как на рабочую станцию (мобильную, удаленную, локальную), так и на всевозможные типы серверов (баз данных, файл-серверов, WWW, FTP, SMTP, SQL и пр.) с целью обеспечения безопасных режимов их использования. В комплексе ViPNet реализованы разнообразные прикладные системы для работы на клиентском месте, например, деловая почта с автопроцессингом и защищенные службы реального времени.

Для установки ViPNet [Администратор] необходим IBM-совместимый компьютер с операционной системой Windows 95/98/Me/NT/2000/XP и не менее 100 Мбайт свободного места на жестком диске. Характеристики компьютера определяются размерностью сети.

Для установки ViPNet [Координатора] необходим IBM-совместимый компьютер с операционной системой Windows NT/2000/XP или Linux, а также не менее 100 Мбайт свободного места на жестком диске. Характеристики компьютера определяются размерностью сети и производительностью каналов связи.

Для установки ViPNet [Клиента] необходим IBM-совместимый компьютер с ОС Windows 95/98/ME/NT/2000/XP с модемом или сетевой картой и не менее 20 Мбайт свободного места на жестком диске.

Основным программным модулем для построения виртуальной сети является *ViPNet-драйвер*. Функциями ViPNet-драйвера является обработка входящих и исходящих IP-пакетов.

Ускоритель криптопреобразований *криптоакселератор ViPNet [TURBO 100]* предназначен для разгрузки центрального процессора при операциях шифрования и дешифрования. Плата криптоакселератора совместима с продуктами ViPNet, работающими под ОС Linux, и может использоваться для закрытия потоков данных со скоростями 100 Мбит/с.

Программный комплекс ViPNet является легко масштабируемой системой. Наращивание системы может осуществляться по мере возникающих у корпорации потребностей путем увеличения по-

ставщиком продукта требуемого числа лицензий на количество объектов, которое может быть зарегистрировано в центре управления данной сети. Количество объектов, которое может быть зарегистрировано в одной сети, практически не ограничено (до 65000 координаторов, до 65000 абонентских узлов на одном координаторе).

ПО функционирует в операционных средах Windows 95/98/ME/NT/2000/XP, Linux.

Производительность работы драйвера защиты трафика в зависимости от ОС и мощности компьютера — от 6 до 32 Мбит/с и практически не ограничивает работу компьютеров даже в 100-мегабитных сетях.

Параметры работы VipNet представлены в табл. 12.

Таблица 12. **Характеристики работы VipNet**

Параметр	Значение
Пропускная способность	ОС Windows NT Канал 10 Мбит Pentium III/ 450 — 9.5 Мбит/с Канал 100 Мбит Pentium III/ 450 — 20 Мбит/с Pentium III/700 — 28 Мбит/с
	ОС Linux (без ViPNet [Turbo 100]) Канал 10 Мбит Pentium166 — 7 Мбит/с Канал 100 Мбит Pentium III/ 700 – 40Мбит
	ОС Linux (с ViPNet [Turbo 100]) Канал 100 Мбит Pentium III/ 700 – 92Мбит
Накладные расходы на поддержание туннеля	30 – 80 байт
Увеличение размеров пакета	40 – 80 байт
Максимальное количество сетевых интерфейсов	32
Снижение трафика	LAN 5 – 10 %
Максимальное число клиентов в одной VPN-сети	Не ограничено

5.4. Семейство продуктов "Net-PRO" компании "Сигнал-КОМ"

Семейство программных продуктов "Net-PRO" разработки компании "Сигнал-КОМ" ориентировано на создание VPN, базирующихся на IP-сетях общего пользования, и может быть использовано как средство коллективной и индивидуальной защиты в сетях Internet/Intranet. "Net-PRO" работает совершенно прозрачно для пользователя, не требуя модификации приложений и прикладных служб. Построение VPN на базе семейства продуктов "Net-PRO" позволяет обеспечить защиту потоков данных в различных вариантах:

- в пределах КС;
- при взаимодействии объединенных ЛВС;
- при взаимодействии с удаленными ресурсами в сетях общего пользования;
- при организации безопасной работы удаленного компьютера с ЛВС и др.

Основной целью, которую ставили перед собой разработчики программного продукта "Net-PRO", являлось создание комплекса средств, обеспечивающих достаточную гибкость при решении широкого круга задач информационной безопасности в сетях различной конфигурации. Это определило разбиение продукта на три функциональных модуля:

- Net-PRO VPN Server — МЭ, реализующий функции SOCKS-сервера;
- Net-PRO VPN Client — клиентский модуль, поддерживающий протокол SOCKS;
- Net-PRO PC Firewall — локальный МЭ.

Модули "Net-PRO" работают под управлением Windows 95/NT, однако применение SOCKS-посредников позволяет защищать ресурсы, функционирующие и на любых других платформах.

Шифрование в семействе продуктов "Net-PRO" обеспечивается за счет использования расширенного протокола SSL, свободного от экспортных ограничений, касающихся длины криптографических ключей, и дополненного отечественными алгоритмами шифрования (ГОСТ 28147-89). Аутентификация основывается либо на паролях, либо на цифровых идентификаторах — сертификатах в формате

X.509. Продукты семейства "Net-PRO" поддерживаются УЦ "Notary-PRO" разработки "Сигнал-КОМ", либо любыми другими УЦ, удовлетворяющими стандарту X.509.

Управление доступом к ресурсам осуществляется на основе аутентифицирующей информации, предоставляемой пользователем, а также с помощью набора правил, формируемых администратором SOCKS-сервера (или серверов, если их несколько) на основе знания топологии виртуальной сети.

В отличие от традиционных МЭ при использовании "Net-PRO" идентифицируются конкретные лица, а не IP-адреса машин, которые эти лица используют для выхода в сеть.

1. Net-PRO VPN Server. Центральное место в семействе продуктов "Net-PRO" занимает модуль "Net-PRO VPN Server", выступающий в роли МЭ в шлюзе ЛВС. Он выполняет фильтрацию приложений и процедуры аутентификации и шифрования потока данных. Net-PRO VPN Server позволяет безопасно объединять через сети общего пользования (в том числе, Internet) ЛВС предприятий и их филиалов, соединять центральный офис компании с удаленными (мобильными) сотрудниками, партнерами по бизнесу и клиентами. При этом обеспечивается шифрование данных, аутентификация и полный контроль доступа к сетевым ресурсам.

Net-PRO VPN Server оснащен средствами борьбы со спуфингом, позволяя контролировать соответствие физического происхождения пакета и его IP-адреса (спуфинг, spoofing – распространенный хакерский прием, заключающийся в том, что злоумышленник пытается извне получить НСД к сети, подделывая содержимое своего пакета под пакет с более высокими привилегиями доступа, например, выдавая его за пакет из вашей ЛВС).

2. *Net-PRO VPN Client* является соксификатором (SOCKS-клиентом) – программой-посредником, заставляющим приложения пользователей работать по протоколу SOCKS, причем, без модификации самих приложений. Он внедряется между пользовательскими приложениями и стеком коммуникационных протоколов, перехватывая коммуникационные вызовы, формируемые приложениями, и перенаправляя их (в случае надобности) на SOCKS-сервер

"Net-PRO". При этом попутно осуществляется аутентификация и шифрование данных по протоколу SSL.

Net-PRO VPN Client устанавливается на компьютерах ЛВС, защищаемой с помощью Net-PRO VPN Server, или на удаленном компьютере, доступ с которого в защищаемую сеть осуществляется через сеть общего пользования (например, Internet) в режиме прямого или коммутируемого подключения.

Работа клиентского модуля совершенно прозрачна для приложений и не требует их модификации. Все настройки (коммуникационные и криптографические) производятся в программе конфигурирования модуля "Net-PRO" с помощью удобного графического интерфейса.

3. Net-PRO PC Firewall — индивидуальное средство защиты компьютера. Клиентский модуль Net-PRO PC Firewall занимает особое положение в семействе продуктов "Net-PRO", играя роль индивидуального средства защиты, поддерживающего прямое (без представительства proxy-сервера) защищенное взаимодействие с аналогичными клиентскими модулями.

Net-PRO PC Firewall устанавливается на отдельных компьютерах, обеспечивая защиту передаваемых между ними потоков данных (аутентификацию и шифрование), независимо от того, находятся эти компьютеры в пределах одной ЛВС или взаимодействуют через глобальную сеть общего пользования. Фактически, Net-PRO PC Firewall выполняет роль локального МЭ, ограждающего рабочую станцию пользователя от нежелательных вторжений.

В VPN, защищаемых сервером "Net-PRO", дополнительная установка на компьютеры модуля Net-PRO PC Firewall повышает уровень безопасности VPN, обеспечивая "поверх" установленных защищенных SOCKS-соединений сквозную аутентификацию и защиту данных между компьютерами в разных ЛВС.

Рассмотрим принцип работы системы. Удаленные пользователи могут подключаться к Internet любым способом: по коммутируемой или выделенной линии. При попытке установить соединение с сервером, находящимся в ЛВС предприятия, модуль Net-PRO VPN Client начинает взаимодействовать с SOCKS-сервером (Net-PRO VPN Server). По завершении первого этапа взаимодействия пользо-

ватель будет аутентифицирован, а проверка правил доступа покажет, имеет ли он право соединяться с конкретным приложением на конкретном сервере; все дальнейшее взаимодействие будет происходить по защищенному шифрованием каналу.

Помимо защиты ЛВС от НСД на SOCKS-сервер "Net-PRO" может возлагаться контроль доступа сотрудников предприятия к открытым ресурсам Internet (Telnet, WWW, SMTP, POP и др.). Доступ является полностью авторизованным, при этом идентифицируются конкретные лица, а не компьютеры, с которых они выходят в сеть. Правила доступа могут запрещать или разрешать соединения с конкретными ресурсами Internet в зависимости от полномочий или потребностей конкретного сотрудника (или группы сотрудников). Действие правил доступа может зависеть и от других параметров, например, от метода аутентификации или времени суток. Дополняют функции контроля развитые средства мониторинга и журнал событий.

Для организации надежного контроля доступа к ресурсам ЛВС предприятия, серверы приложений могут быть выделены в отдельный сегмент. Следует отметить, что использование Net-PRO VPN Server позволяет полностью скрывать топологию ЛВС. Серверы предприятия могут не иметь зарегистрированных сетевых адресов и доменных имен: разрешение имен производится на SOCKS-сервере.

С помощью "Net-PRO" на базе сети общего пользования можно построить VPN, обеспечивающую безопасное взаимодействие ЛВС предприятия и его филиалов. Для этого в точке сопряжения каждой ЛВС с Internet устанавливается SOCKS-сервер "Net-PRO", а на рабочих станциях в ЛВС — какой-либо из SOCKS-посредников:

- Net-PRO VPN Client разработки "Сигнал-КОМ";
- соксификатор любой другой фирмы-производителя;
- приложение со встроенной поддержкой протокола SOCKS.

При такой конфигурации VPN сотрудники предприятия и филиала получают доступ ко всем серверам предприятия и филиала так, как если бы они находились в одной ЛВС. При этом два SOCKS-сервера "Net-PRO", взаимодействуя между собой, с помощью шифрования создают защищенный виртуальный канал. Разу-

меется, все, что говорилось в предыдущем примере относительно контроля доступа, остается верным и в этом случае.

Наконец, вариант организации VPN на базе только локальных экранов Net-PRO PC Firewall. В такой конфигурации обеспечивается защита сетей TCP/IP, включающих сервера и рабочие станции, функционирующие под управлением Windows NT/95. Данная конфигурация не требует наличия proxy-серверов, так как защищенные аутентифицированные соединения устанавливаются непосредственно между конечными точками сети, оснащенными модулем Net-PRO PC Firewall.

5.5. Продукты МО ПНИЭИ "ШИП" и "Игла-2"

Концепция создания шифратора "ШИП" отличается тем, что в данном случае шифратор является так называемым "черным ящиком" [9]. Это означает, что шифратор представляет собой функционально завершенное устройство, которое выполняет только строго назначенные ему функции и не может использоваться для решения прикладных задач, как обычный компьютер. "ШИП" — это магистральный шифратор, который ставится на выходе ЛВС и защищает весь ее трафик. "Игла-2" является в большей степени клиентским шифратором (как "ЗАСТАВА-клиент"), однако может выполнять функции шифратора сети при специальных его настройках и использоваться для защиты сети там, где параметры скорости соединений не так важны.

Шифраторы обеспечивают:

- защиту (шифрование и проверку целостности с использованием имитовставки) данных, передаваемых между узлами сети, согласно ГОСТ 28147-89;
- одностороннюю аутентификацию узлов защищенной сети на основе имитовставки согласно ГОСТ 28147-89;
- управление ключевой системой защищенной сети из одного или нескольких центров управления;
- контроль целостности передаваемой информации;
- защиту доступа к ЛВС и сокрытие IP-адресов подсети;
- создание защищенных подсетей в сетях общего пользования;

- передачу контрольной информации в центр управления безопасностью защищенной IP-сети;
- фильтрацию IP, ICMP, SKIP-пакетов и TCP-соединений на этапе маршрутизации и при приеме/передаче в канал связи;
- поддержку и преобразование различных сетевых протоколов;
- защиту от НСД ресурсов самого шифратора.

Управление ключами в системе "ШИП" предполагает:

- формирование и распространение по сети справочников соответствия, определяющих, какие именно абоненты ЛВС имеют доступ в VPN;
- периодическую (плановую) смену ключей шифрования;
- сбор и хранение информации обо всех нештатных событиях в сети, возникающих при аутентификации узлов, передаче зашифрованной информации, ограничении доступа абонентов ЛВС;
- оповещение криптоустройств о компрометации ключей.

Для шифратора "Игла-2" каждого абонента приходится заводить вручную. Средств удаленного управления такими шифраторами пока не существует. Данный факт говорит о том, что применение шифратора "Игла-2" в больших распределенных корпоративных системах затруднительно ввиду отсутствия системы централизованного управления.

Организация VPN. В целом условия применения данных шифраторов не отличаются от продуктов "ЗАСТАВА". Роль клиентской части для шифратора "ШИП" в данном случае играет "Игла-2". Однако "Игла-2" может самостоятельно выступать в качестве криптомаршрутизатора.

Аналогично, данные устройства могут применяться для создания распределенных VPN-сетей с разделением потоков между абонентами данной системы. Отличительными особенностями шифраторов можно назвать возможности резервирования центров управления ключевой системой и разбиения сети на региональные подсети (каждая подсеть при этом будет управляться своим центром управления). Кроме того, выполнены достаточно жесткие требования к защите программного обеспечения шифраторов от несанкционированного искажения, изменения, к защите ключевых данных, а также

к защите от внешних и внутренних сетевых атак. К недостаткам устройств можно отнести достаточно неудобную (по сравнению с другими шифраторами) систему управления, а также отсутствие динамической маршрутизации в криптоустройствах, что создает дополнительные проблемы в больших распределенных сетях, где в каждом шифраторе необходимо прописать маршруты до каждого шифратора, участвующего в обмене информацией. То же самое относится и к "Игле-2".

5.6. Аппаратно-программный комплекс "ФПСУ-IP" компании "Амикон"

Комплексы межсетевого экранирования и организации VPN "ФПСУ-IP" (Фильтр Пакетов Сетевого Уровня для протоколов TCP/IP) сертифицированы по 3 классу защищенности от НСД к информации (сертификат Гостехкомиссии № 233 от 29.04.99).

Продукт "ФПСУ-IP" позиционируется как МЭ уровня TCP/UDP. С его помощью можно организовать криптографически защищенные межсетевые соединения на уровне протокола IP со сжатием графика [9].

"ФПСУ-IP" реализован по принципу ложного ARP-сервера, который устанавливается в физический разрыв между двумя сегментами сети. Он перехватывает ARP-запросы сетевых устройств, предоставляя в качестве ответа MAC-адрес принявшего данный запрос интерфейса. Приходящие на него IP пакеты подвергаются фильтрации (с полной пересборкой пакетов), и, если задано, дополнительно обрабатываются для организации VPN (компрессия данных и/или дополнительное кодирование с нелинейным преобразованием исходных данных) и затем транслируются на другой интерфейс или сбрасываются в соответствии с результатами обработки. Такое построение позволяет обеспечивать внедрение "ФПСУ-IP" в существующие сети практически без проведения реконфигурирования последних, что также ставилось в виде задачи перед разработкой комплекса. Кроме того, такой МЭ является полностью прозрачным для клиентов сети, которые в процессе штатного использования комплекса даже не будут знать о его существовании. Применение соб-

ственной операционной среды для МЭ экрана делает его более безопасным, производительным и неприхотливым к условиям эксплуатации.

Защита операционной среды и рабочей информации в "ФПСУ-IP" от НСД осуществляется с помощью системы собственной разработки, где используются платы расширения BIOS "Аккорд" производства ОКБ САПР. Эта система позволяет разграничивать уровни доступа обслуживающего персонала к системе и защищает программное обеспечение на жестком диске с помощью ключа, находящегося на электронном идентификаторе Touch Memory.

"ФПСУ-IP" реализует следующие основные функциональные возможности:

- фильтрация сетевых пакетов уровня IP и TCP в соответствии с задаваемыми администраторами правилами на основе IP-адресов отправителя и получателя, инкапсулированных фреймов, времени и даты передачи пакета, разрешенных портов абонентов (для TCP/UDP-пакетов), а также пар адресов абонентов, для которых разрешено соединение;
- трансляция сетевых адресов отправителя и получателя в межсетевых туннелях, скрывающая внутренние адреса субъекта и объекта информационного взаимодействия (NAT);
- создание множества VPN (создание защищенных областей идентифицированных компьютеров, объединенных между собой туннелями со строгой двухсторонней аутентификацией). Через один "ФПСУ-IP" может быть создано до 1024 VPN в каждую сторону, имея в виду наличие двух портов и возможность каскадных схем использования "ФПСУ-IP" (что невозможно выполнить с применением других реализаций).
- возможность VPN-поддержки каналов управления удаленными пограничными маршрутизаторами (находящихся на входах в демилитаризованные зоны, прикрываемые "ФПСУ-IP") по протоколам SNMP и Telnet, что не требует применения дополнительных средств для защиты систем управления (HP OpenView, CA Unicenter и др.) важнейшими сетевыми ресурсами организации;

- осуществление при туннелировании данных безусловной строгой двухсторонней аутентификации и трансляции сетевых адресов (NAT), что обеспечивает практически гарантированную защиту от любых внешних информационных атак на VPN;
- применение эффективных (на уровне ARJ) механизмов "проходного" сжатия данных, за счет чего повышаются скорости обмена информацией по любым используемым каналам связи глобальных сетей (WAN) и уменьшаются затраты организации на аренду ресурсов WAN;
- строгая защита передаваемых данных на уровне IP, в том числе от навязывания ранее переданных;
- сокрытие факта использования защитных свойств комплекса. При нарушении правил фильтрации и сброса пакета на межсетевом экране клиент получает ICMP-сообщение о том, что маршрут не найден (опционально);
- регистрация в специальном защищенном хранилище статистической информации о функционировании комплекса (все действия по управлению, фильтрации данных и суточный биллинг), при этом доступ к данным осуществляется только в режиме Read Only;
- визуальное отображение на экране монитора попыток нарушения правил фильтрации;
- собственная операционная функционально замкнутая среда, что обеспечивает защиту от доступа к конфигурационной и другой рабочей информации и автоматический контроль целостности исполняемых модулей, исключая их несанкционированную модификацию и внедрение разрушающих программных воздействий; кроме того, при использовании специальной эталонной программы контроля и выдачи значений хэш-функций всех исполнимых модулей подсистем инсталлированного комплекса с целью сравнения их с априорно известными;
- обеспечение защиты от несанкционированного доступа к информации и ресурсам комплекса посредством идентификации администратора по некопируемому уникальному идентификатору и содержимому памяти электронной таблетки Touch Memory, а также по паролю условно-постоянного действия;

- разделение прав на доступ к работе комплекса для различных классов администраторов.

"ФПСУ-IP" имеет симметричную ключевую систему, как, например "ШИП", первоначально загружаемую вручную локально. Каждое устройство "ФПСУ-IP" может хранить до четырех комплектов собственных ключей одновременно, а также все необходимые данные парновыборочной связи не более, чем для 32 групп (в каждой группе может быть до 9 999 комплектов ключей). Все взаимодействующие друг с другом устройства ФПСУ-IP переходят на новые комплекты ключей автоматически сразу же после изменения номера комплекта на одном из них.

Если для других средств организации VPN, выполненных на основе типовых алгоритмов (например, протокол SKIP) характерно достаточно существенное снижение скорости передачи потоков данных за счет введения избыточности в каждый передаваемый пакет, то при применении комплекса "ФПСУ-IP" обеспечивается минимальная избыточность передаваемой информации, что обеспечивает даже прирост скорости передачи IP-потоков.

"ФПСУ-IP" имеет высокие скоростные характеристики: при сжатии, шифровании трафика на процессоре Pentium-200 можно добиться скорости до 11,7 Мбит/с (например, "ШИП" в таких же условиях дает скорость 5 Мбит/с, "ЗАСТАВА" — 4,5 Мбит/с, "Континент" — 10,2 Мбит/с).

Поддерживаемые протоколы в IP-среде — ARP, ICMP, Telnet, SNMP и другие стандартные протоколы на базе TCP/UDP (всего 255 протоколов, согласно RFC 1700).

Межсетевое экранирование (фильтрация IP потоков): по адресам; по протоколам; по TCP/UDP портам; по дате/времени; по служебной и управляющей информации; по логическим группам взаимодействующих абонентов (правил фильтрации) и пересечениям интерфейсов доступа, приписанных для этих групп; по интерфейсам приема/передачи; сокрытие факта использования защитных свойств комплекса; сокрытие топологии защищаемой сети

VPN – экранирование, реализующее:

- противодействие всем возможным атакам из внешних информационных сетей и каналов связи;

- строгую двухстороннюю аутентификацию VPN-данных (удаленных абонентов/подсетей);
- блочное сжатие IP-потоков с применением данных аутентификации;
- периодическую повторную аутентификацию установленных соединений;
- автоматическую синхронизацию аутентификационных данных взаимодействующих комплексов;
- объединение комплексов в группы, допускающее различные комбинации (варианты) вложений (255 групп до 2500 комплексов в каждой группе).

Компрессия/восстановление данных при использовании ФПСУ-туннелей: оригинальная реализация высокоскоростного механизма сжатия "на проходе" с использованием разнородных алгоритмов (двухпроходный компрессор), обеспечивающего высокие коэффициенты сжатия (на уровне стандартных архиваторов).

Аутентификация — строгая двухсторонняя аутентификация VPN-данных согласно Рекомендации X.509 (реализация АМИКОН© при участии ИнфоКрипт©).

Проходное пакетное шифрование — возможность встраивания сертифицированных криптографических средств защиты информации (открытый криптографический интерфейс)

Система управления/мониторинга, обеспечивающая:

- локальное управление/конфигурирование;
- централизованное защищенное дистанционное управление и мониторинг состояний комплексов с использованием АРМ собственной разработки;
- взаимодействие со стандартными средствами централизованного мониторинга состояний с SNMP-агентом, размещенным в составе АРМ ЦДУК.

Система аудита/регистрации, поддерживающая:

- применение MIB-подобного хранилища для регистрации всех значимых событий и ведения статистики работы с возможностями импорта статистической информации в файлы DBF-формата для генерации отчетов;

- аудит действий обслуживающего персонала (как локальных, так и удаленных);
- ведение статистики работы абонентов с автоматическим формированием ежесуточных данных о количестве принятой и переданной информации (биллинг).

Среди недостатков "ФПСУ-IP" можно отметить следующие:

- нерабочее состояние комплекса при его настройке (в это время сетевой трафик через него не проходит);
- отсутствие возможности использовать DNS, что затрудняет анализ статистической информации;
- отсутствие на сегодня системы централизованного управления шифраторами;
- работа только с двумя сетевыми платами;
- поддержка только Ethernet-протокола.

Достоинством продукта "ФПСУ-IP" является его довольно низкая цена.

5.7. Сравнение российских продуктов

Приведем сравнительную таблицу (табл. 13) рассмотренных выше российских продуктов для создания VPN [8].

Таблица 13. **Сравнительные характеристики российских VPN-продуктов**

	ШИП	Застава	ФПСУ-IP	VipNet	Континент–К	Криптон IP
1	2	3	4	5	6	7
Общие сведения						
Производитель, поставщик	МО ПНИЭИ	Элвис+	Амикон	Инфо-Текс	Информ-защита	Анкад
Используемые ОС	FreeBSD	Win NT/95/98 Sparc/Intel Solaris	Собственная ОС	Win NT/95/98/ ME/2000 Linux	Win NT (Service Pack 5.0 и выше)	MS-DOS 5.0 и выше

Продолжение табл.13

1	2	3	4	5	6	7
Сертификация Гостехкомиссией при Президенте РФ или ФАПСИ	Сертификат ФАПСИ	Класс 3 №145 от 14.01.98 (под Solaris) Серийное производство	Класс 3 №233 от 14.04.99 Сертифицировано серийное производство	Сертификат ГТК по кл. 1В для АС и класс 3 для МЭ. Заявлен на сертификацию в ФАПСИ	Сертификат ГТК №352 от 28.08.00 по 3 классу для МЭ	Принят на сертификацию ФАПСИ
Использование отечественных криптографических стандартов для организации VPN-сервисов	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89
Максимальное количество сетевых интерфейсов	5	5	2	32	16	Н/д
Функции управления доступом (фильтрация данных и трансляция адресов)						
Фильтрация пакетов служебных протоколов (для диагностики и управления работой сетевых устройств)	Да	Да	Да	Да	Да	Нет
Фильтрация с учетом входного и выходного интерфейса (для проверки подлинности адресов)	Да	Да	Да	Да	Да	Да
Фильтрация с учетом любых значимых полей сетевых пакетов	Да	Да	Да	Да	Да	Н/д

Продолжение табл.13

1	2	3	4	5	6	7
Фильтрация на транспортном уровне запросов на установления виртуальных соединений с учетом транспортных адресов	Да (TCP/UDP)	Да (TCP/UDP)	Да (TCP/UDP)	Да (TCP/UDP)	Да (TCP/UDP)	Н/д
Фильтрация на прикладном уровне запросов к прикладным сервисам	Нет	Нет	Нет	Нет	Нет	Нет
Фильтрация с учетом даты/времени	Нет	Нет	Да	Нет	Нет	Н/д
Трансляция номеров портов/сетевых адресов	-/+	-/+	+/+	-/+	-/+	Н/д
Возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети	Да	Да	Да	Да	Да	Да
Возможность скрытия межсетевого экрана	Нет	Нет	Да	Нет	Нет	Нет
Идентификация и аутентификация сетевого трафика						
Возможность аутентификации трафика	Да (хэш-функции ГОСТ Р34.11-94)	Да (хэш-функции по алгоритму MD5)	Да (хэш-функции ГОСТ Р34.11-94)	Нет	ГОСТ 28147-89 в режиме имитовставки	Да (односторонняя аутентификация с имитовставкой)

Продолжение табл.13

1	2	3	4	5	6	7
Администрирование						
Проведение идентификации и аутентификации администратора МЭ по идентификатору (коду)	Средствами FreeBSD	Средствами Solaris	ТМ Аккорд	Пароль	Средствами ЭЗ Соболь	Нет
Проведение идентификации и аутентификации запросов на доступ удаленных администраторов	Средствами FreeBSD + конфигурацией ПО	Средствами Solaris + конфигурацией ПО	Строгая двусторонняя аутентификация при защите запросов	По паролю	Специальный административный ключ на Touch Memory	Нет
Возможность централизованного управления	Да (telnet)	Да (telnet + графическая оболочка)	Да (АРМ ЦУБ)	Да	Да	Нет
Регистрация действий администратора ИЖ по изменению правил фильтрации	Да	Да	Да	Н/д	Да	Нет
Графический интерфейс удаленного управления (GUI)	Нет (только текстовый)	Есть (Java)	АРМ ЦУБ, АРМ ЦКС (контроль связи)	Н/д	Специальное ПО	Нет
ОС, поддерживающие GUI	-	Любой Java browser	DOS	Н/д	Win NT 4.0 (Service Pack от 4) или Win'9x	-
Сигнализация в центре управления о событиях на удаленных МЭ	Да	Да	Да	Н/д	Да	Нет

Продолжение табл.13

1	2	3	4	5	6	7
Фильтрация на транспортном уровне запросов на установления виртуальных соединений с учетом транспортных адресов	Да (TCP/UDP)	Да (TCP/UDP)	Да (TCP/UDP)	Да (TCP/UDP)	Да (TCP/UDP)	Н/д
Фильтрация на прикладном уровне запросов к прикладным сервисам	Нет	Нет	Нет	Нет	Нет	Нет
Фильтрация с учетом даты/времени	Нет	Нет	Да	Нет	Нет	Н/д
Трансляция номеров портов/сетевых адресов	-/+	-/+	+/+	-/+	-/+	Н/д
Возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети	Да	Да	Да	Да	Да	Да
Возможность скрытия межсетевого экрана	Нет	Нет	Да	Нет	Нет	Нет
Идентификация и аутентификация сетевого трафика						
Возможность аутентификации трафика	Да (хэш-функции ГОСТ Р34.11-94)	Да (хэш-функции по алгоритму MD5)	Да (хэш-функции ГОСТ Р34.11-94)	Нет	ГОСТ 28147-89 в режиме имитовставки	Да (односторонняя аутентификация с имитовставкой)

Продолжение табл.13

1	2	3	4	5	6	7
Администрирование						
Проведение идентификации и аутентификации администратора МЭ по идентификатору (коду)	Средствами FreeBSD	Средствами Solaris	ТМ Аккорд	Пароль	Средствами ЭЗ Соболь	Нет
Проведение идентификации и аутентификации запросов на доступ удаленных администраторов	Средствами FreeBSD + конфигурацией ПО	Средствами Solaris + конфигурацией ПО	Строгая двусторонняя аутентификация при защите запросов	По паролю	Специальный административный ключ на Touch Memory	Нет
Возможность централизованного управления	Да (telnet)	Да (telnet + графическая оболочка)	Да (АРМ ЦУБ)	Да	Да	Нет
Регистрация действий администратора ИЖ по изменению правил фильтрации	Да	Да	Да	Н/д	Да	Нет
Графический интерфейс удаленного управления (GUI)	Нет (только текстовый)	Есть (Java)	АРМ ЦУБ, АРМ ЦКС (контроль связи)	Н/д	Специальное ПО	Нет
ОС, поддерживающие GUI	-	Любой Java browser	DOS	Н/д	Win NT 4.0 (Service Pack от 4) или Win'9x	-
Сигнализация в центре управления о событиях на удаленных МЭ	Да	Да	Да	Н/д	Да	Нет

Продолжение табл.13

1	2	3	4	5	6	7
Протоколирование событий/ формирование отчетов						
Учет использования	Да	Да	Да	Н/д	Н/д	Да
Сортировка/фильтрация сообщений	+/+	+/+	+/+	Н/д	Н/д	-/-
Формат журнала регистрации	Syslog	Syslog	Хранилище, подобное MIB	Н/д	Н/д	Текстовый
Форматы экспорта журнала регистрации	Текст	Текст	DBF-формат	Н/д	Н/д	Текст
Параметры VPN						
Применение отечественных алгоритмов (ГОСТ) для построения VPN	Да	Да	Да	Да/Нет (зависит от настроек)	Да	Да
Базовый протокол	SKIP	SKIP	Собственный	Собственный	Собственный	Собственный
Накладные расходы на поддержку туннелей	112 на IP-пакет	112 на IP-пакет	18-20 на IP-пакет	30-80 на IP-пакет	26-36 на IP-пакет	Н/д
Возможность сжатия трафика	Да	Нет	Да	Нет	Да	Н/д
Наличие клиентских частей	Да (Windows NT)	Да (Solaris Windows 95/98/NT)	Нет	Да	Да (Windows 95/98/NT)	Нет
Количество одновременно поддерживаемых независимых туннелей	Н/д	1400	До 1024 на каждом сетевом интерфейсе	Windows – 50, Linux – 300	не более 500 на каждый КШ	Н/д

Продолжение табл.13

1	2	3	4	5	6	7
Возможность вложенности VPN-туннелей друг в друга (каскадирование)	Да	Да	Да	Н/д	Н/д	Н/д
Возможность VPN-поддержки каналов управления пограничными маршрутизаторами	Нет	Да	Да	Нет	Нет	Нет
Возможность VPN-взаимодействия с VPN других организаций	Да (при использовании ими SKIP)	Да (при использовании ими SKIP)	Нет (если не ФПСУ-IP)	Нет (если не VipNet)	Нет (если не "Континент")	Нет (если не "Криптон")
Собственная безопасность						
Защита целостности среды	Нет	Нет	Да - по классу 1а	Нет	Нет	Н/д
Защита целостности ПО	Да - контрольные суммы	Да - контрольные суммы	Да - по классу 1а	Нет	Да - ЭЗ Соболь	Да – ЭЦП
Разграничение полномочий обслуживающего персонала	Да - средства FreeBSD	Нет	Да - с помощью ТМ	Да - по паролю	Нет	Нет
Защита используемой ключевой информации	Да (главные ключи грузятся с дискеты)	Да (средствами ОС Solaris)	Да (собственными средствами)	Да (собственными средствами)	Да (на диске в зашифр. виде, ключ хранения – в ЭЗ Соболь)	Да (загрузка ключей с дискеты, смарт-карты)
Аутентификация программных модулей/ дополнений	Нет	Нет	Да (хэш-функции)	Нет	Нет	Н/д

Окончание табл. 13

Характеристики производительности (пропускная способность), Мбит/с						
В режиме шифрования	8 (Pentium 200)	8 (Pentium 200)	11 (Pentium 200)	9.5 (Pentium III/450)	17,4 (Celeron/500)	1,2-1,8 (Intel 486)
Дополнительные возможности						
Open CryptoAPI[tm]	Нет	Да	Нет	Нет	Нет	Нет
Стоимостные характеристики, долл.						
Цена	Н/д	2500-3000	1000-1500	Н/д	Н/д	350

Контрольные вопросы по разделу 5

1. Каковы назначение, особенности, состав и возможности аппаратно-программного комплекса защиты информации "Континент-К"?
2. Какие программные продукты компании "ЭЛВИС+" используются для построения VPN и как именно? Какой основной протокол управления ключами применяется в этих продуктах?
3. Расскажите об VPN-решениях компании "Инфотекс". Каковы их особенности и функциональные возможности? В чем заключается технологий ViPNet?
4. Какие функции по созданию VPN и как именно реализованы в семействе продуктов "Net-PRO" компании "Сигнал-КОМ"? На основе какого протокола осуществляется шифрование?
5. Рассмотрите назначение и возможности продуктов МО ПНИЭИ "ШИП" и "Игла-2" с точки зрения построения VPN.
6. Какие составляющие аппаратно-программного комплекса "ФПСУ-IP" компании "Амикон" и с какими особенностями используются для построения VPN? Что реализует VPN—экранирование?
7. По каким основным показателям удобнее всего сравнивать продукты для создания VPN?
8. Сравните рассмотренные в данном разделе известные российские VPN-продукты по основным показателям и сделайте вывод, в каких случаях эффективнее всего их применение.

Заключение

Основная проблема современных сетей VPN [4, 5, 11] — отсутствие устоявшихся стандартов аутентификации и обмена шифрованной информацией. Эти стандарты все еще находятся в процессе разработки и потому не реализованы в продуктах различных изготовителей. Проблема влечет за собой замедление распространения VPN. Поскольку различные компании не могут пользоваться продукцией одного изготовителя, затрудняется объединение сетей компаний-партнеров в extranet.

Еще один аспект, связанный с сертификацией, — пока средства построения VPN сертифицируются по классу межсетевых экранов. Назначение и функциональные возможности МЭ и VPN существенно отличаются. Поэтому очевидна потребность в разработке соответствующего отдельного руководящего документа, который бы позволил корректно и наиболее полно сертифицировать средства построения VPN как средства из самостоятельного класса, предназначенного для обеспечения информационной безопасности при передаче по открытым каналам связи.

Продукты построения VPN могут оказаться узким местом в сети. Это происходит из-за того, что для обеспечения множества соединений и шифрования информации, передаваемой по этим соединениям, требуется высокая производительность оборудования или ПО.

Еще одно уязвимое место VPN — отсутствие единых, надежных способов управления такими сетями.

И, наконец, отсутствие (или слабое развитие) механизмов обеспечения качества услуг в сетях типа Internet – это очень большая проблема для сетей VPN, поскольку многие работающие в VPN приложения требуют гарантированной доставки информации за ограниченное время.

Средства VPN не всемогущи. Они не являются полноценными средствами обнаружения и блокирования атак. Они могут предотвратить ряд несанкционированных действий, но далеко не все возможности, которые могут использовать хакеры для проникновения в КС. Они не могут обнаружить вирусы и атаки типа "отказ в обслуживании" (это делают антивирусные системы и средства обна-

ружения вторжений), они не могут фильтровать данные по различным признакам (это делают МЭ) и т.д. На это можно возразить, что подобные опасности не страшны, так как VPN не примет незашифрованный трафик и отвергнет его. Однако на практике это не так. Во-первых, в большинстве случаев средство построения VPN используется для защиты лишь части трафика, например, направленного в удаленный филиал. Остальной трафик (например, к публичным Web-серверам) проходит через VPN-устройство без обработки. А во-вторых, серьезная проблема — атаки изнутри. По статистике около 75 % финансовых потерь наносится в результате подобных агрессий. Также статистика утверждает, что до 80 % всех инцидентов, связанных с информационной безопасностью, происходит по вине авторизованных пользователей, имеющих санкционированный доступ в КС. Из чего следует вывод, что атака или вирус будут зашифрованы наравне с безобидным трафиком. Атаки типа "отказ в обслуживании" (DoS- или DDoS-атаки) также является существенным препятствием для VPN-агентов.

Чего ждать в будущем? Безусловно, будет выработан и утвержден единый стандарт построения виртуальных сетей. Скорее всего, основой этого стандарта будет уже зарекомендовавший себя протокол IPSec. Изготовители сконцентрируются на повышении производительности своих продуктов и на создании удобных средств управления VPN.

Рынок VPN-продуктов постоянно расширяется, поскольку интерес к этой технологии в последнее время усиливается. Вместе с тем, информационная безопасность КС и применение криптографии для защиты информации при передаче по открытым каналам связи являются достаточно "тонкими" областями знаний, поэтому даже малейшая ошибка при проектировании корпоративной VPN может привести к фатальным для компании результатам. По этой причине необходимо быть особенно осмотрительным как при выборе VPN-продуктов, так и при проектировании самой VPN.

Скорее всего, развитие средств построения VPN будет идти в направлении VPN на базе маршрутизаторов, так как данное решение сочетает в себе достаточно высокую производительность, интеграцию VPN и маршрутизации в одном устройстве. Однако будут

развиваться и недорогие решения на базе сетевых ОС для небольших организаций.

Создание интегрированных VPN как одной из составляющих при проведении комплексных мероприятий по обеспечению защиты сетей позволит передавать голос, данные, видеоизображения и другую информацию с гарантированным качеством обслуживания на единой технологической платформе, прозрачной для внедрения любых новых платформонезависимых услуг и приложений. Другими словами, создание VPN является следующим, закономерным шагом в эволюции корпоративных сетей по пути к их совершенствованию и наиболее эффективному использованию современных достижений информационных и сетевых технологий.

Приложение 1. Сравнение зарубежных продуктов для создания виртуальных частных сетей

Компания	Продукт	Тип	Интерфейсы (макс. число, тип)	Обработка протоколов	Сжатие IP-пакетов
1	2	3	4	5	6
3Com	PathBuilder S500 Tunnel Switch Family	Маршр. Коммутатор, уст-во VPN, МЭ	2 10/100-Мбит/с, 8 ГС	Через IP	—
	SuperStack II NETBuilder SI	Маршр. Коммутатор, уст-во VPN, МЭ	2 10/100-Мбит/с, 2 или 4 ГС, ISDN	Через IP	—
	OfficeConnect NETBuilder	Маршр. Коммутатор, уст-во VPN, МЭ	1 10-Мбит/с, 1 или 2 ГС	Через IP	—
	NETBuilder II	Маршр. Коммутатор, уст-во VPN, МЭ	Множество 10/100-Мбит/с и ГС	Через IP	—
Altiga Networks	VPN Concentrator Series, C10	Выделенное уст-во VPN (концентратор)	3 10/100-Мбит/с	Через IP	—
	VPN Concentrator Series, C20	Выделенное уст-во VPN (концентратор)	3 10/100-Мбит/с	Через IP	—
	VPN Concentrator Series, C50	Выделенное уст-во VPN (концентратор)	3 10/100-Мбит/с	Через IP	—
Ascend	Pipeline 50/75	Маршрутизатор со ср-ми VPN, МЭ	1 10-Мбит/с, 1 ISDN		—
	Pipeline 85	Маршрутизатор со ср-ми VPN, МЭ	4 10-Мбит/с, 1 ISDN		—
	Pipeline 220	Маршрутизатор со ср-ми VPN, МЭ	2 10-Мбит/с, 1 ГС, 1 ISDN	IPX, AppleTalk	—
Assured Digital	ADI-4500	Выделенное уст-во VPN	2 10/100-Мбит/с		—
	ADI-1000	Выделенное уст-во VPN	2 10-Мбит/с		—
Axent Technologies	Raptor Firewall/ VPN Server	Средства VPN с МЭ	Лимитируются ОС хост-компьютера		—

Таблица П1

Управление	Функциональные возможности						Цена, долл.
	Сквозная передача	т/т ЗА	т/т ИПЗ	Поддержка ПТ	Поддерж. алгоритмы аутентиф.	Поддерж. алгоритмы шифрования	
7	8	9	10	11	12	13	14
Консоль, telnet, HP OpenView	+	+/+	+/+	PPTP, L2TP	MD5, SHA-1	DES, Triple-DES, RC5, HMAC MD5, HMAC SHA-1, PAP, CHAP, MS-CHAP	30 295
Консоль, telnet, HP OpenView	+	+/+	+/+	PPTP, L2TP	MD5, SHA-1		7295
Консоль, telnet, HP OpenView	+	+/+	+/+	PPTP, L2TP	MD5, SHA-1		5095
Консоль, telnet, HP OpenView	+	+/+	+/+	PPTP, L2TP	MD5, SHA-1		23 795
Java, консоль, telnet	+	-/-	-/+	PPTP, L2TP	MD5, HMAC MD5, SHA-1, HMAC SHA-1, Null	DES-56, DES-168, Null, RC4	20 000
Java, консоль, telnet	+	-/-	-/+	PPTP, L2TP		DES-56, DES-168, Null, RC4	30 000
Java, консоль, telnet	+	-/-	-/+	PPTP, L2TP		DES-56, DES-168, Null, RC4	60 000
GUI через SecureConnect Manager	+	+/+	+/+	PPTP, L2TP	MD5, SHA-1, Null	DES, DES-40, Triple-DES, Null	1520 (P50), 1720 (P75)
GUI через SecureConnect Manager	+	+/+	+/+	—	MD5, SHA-1, Null	DES, DES-40, Triple-DES, Null	1920
GUI через SecureConnect Manager	+	+/+	+/+	—	MD5, SHA-1, Null	DES, DES-40, Triple-DES, Null	5990
GUI ОС NT, командная строка	—	+/+	+/+	Патентованных	MD5, SHA-1, Null	DES, Triple-DES, Null	20 985
GUI ОС NT, командная строка	—	+/+	+/+	—	MD5, SHA-1, Null	DES, Triple-DES, Null	3585
GUI ОС NT и Solaris	+	+/+	+/+	—	MD5, SHA-1, Null	DES, Triple-DES, Null, RC2	5000 (только ПО)

1	2	3	4	5	6
Check Point Software	VPN-1 Gateway Solution с ускорителем VPN-1 Accelerator Card	МЭ со ср-ми VPN	Лимитируются ОС хост-компьютера		—
Cisco	Cisco 1720 VPN Router	Маршрутизатор со ср-ми VPN	1 10-Мбит/с, 5 последовательных		—
	Прогр. обеспеч. IPSec for Cisco IOS	Маршрутизатор со ср-ми VPN	Лимитируются ОС хост-компьютера	Через IP	+
Compaq	AltaVista Tunnel 98	Программные средства VPN	Лимитируются ОС хост-компьютера		+
Compatible Systems	IntraPort 2+	Выделенное уст-во VPN	2 100-Мбит/с	IPX, Apple-Talk	+
Cybernetica	Privador SVPN System	Выделенное уст-во VPN	2 10/100-Мбит/с		—
Data Fellows	F-Secure VPN+ 4.0	Программные ср-ва VPN, МЭ, маршрутизатор (под NT 4.0)	Лимитируются ОС хост-компьютера		—
Elock Technologies	e-Lock VPN	Программные средства VPN	Лимитируются ОС хост-компьютера		+
FreeGate	OneGate 150 с Branch and Remote VPN	Устр-во доступа в Internet со ср-ми маршрутизации, VPN, МЭ	2 10-Мбит/с, 1 ISDN		+
	OneGate 1000 с Branch and Remote VPN	Устр-во доступа в Internet со ср-ми маршрутизации, VPN, МЭ	2 10-Мбит/с, 1 ISDN, 1 ГС		—
Fortress Technologies	NetFortress VPN-10	Оборудование VPN	2 10/100-Мбит/с		—
IBM	IBM eNetwork Firewall 3.3	МЭ со ср-ми VPN	Лимитируются ОС хост-компьютера		+

Продолжение табл.П1

7	8	9	10	11	12	13	14
GUI ОС NT, Solaris, HP-UX и AIX, запросы LDAP, команд. строка	+	-/+	-/+	—	MD5, SHA-1, CBC-DES MAC	DES, Triple-DES, DES-40, Null, CAST, CAST 40	14 980 (с VPN-1),
Командная строка, консоль, telnet	—	+/+	+/+	Патентованных	MD5, SHA-1	DES, Triple-DES	2990
Командная строка с GUI на базе Java	+	+/+	+/+	L2TP, L2F	MD5, SHA-1	DES, Triple-DES, Null	8000 (только ПО)
GUI Win32 и Motif	+	-/-	-/-	L2TP, L2F	MD5	RC4	3695 (только ПО)
GUI ОС NT/98/95 и Mac., команд. ст-ка telnet	+	+/+	-/+	Патентованных	MD5	DES, Triple-DES	13 990
GUI Win32	—	-/-	-/+	—	MD5, SHA-1	DES, Triple-DES, Idea	~9000
GUI HTTP и ОС NT/95; требуется доп. соединение	+	+/+	+/+	—	MD5, SHA-1	DES, Triple-DES, Blowfish, CAST	4990 (только ПО)
GUI на рабочей станции	+	+/+	+/+	—	MD-5, SHA-1, Null	DES, Triple-DES, Null	3000
На основе HTTP; поддержка SSL	—	-/+	-/+	—	MD5, SHA-1	DES, Triple-DES, Null, RC2, RC4	5385
На основе HTTP; поддержка SSL	—	-/+	-/+	PPTP	MD5, SHA-1	DES, Triple-DES, Null, RC2, RC4	12 085
GUI операционных систем NT/98/95	—	+/+	-/+	PPTP	MD5, SHA-1	DES, Triple-DES, Idea	11 990
На базе Java	+	-/+	-/+	Патентованных	MD5, SHA-1	DES, Triple-DES	5000 (только ПО)

1	2	3	4	5	6
IBM, подразделение сетевого оборудования	IBM 2210 Nways Multiprotocol Router (Ethernet)	Маршр. с интегр. МЭ, ср-ва VPN	2 10-Мбит/с, 12 ГС, ISDN	Без IP через L2TP	—
	IBM 2210 Nways Multiprotocol Router (Token Ring)	Маршр. с интегр. МЭ, ср-ва VPN	2 4/16-Мбит/с, 12 ГС, ISDN	Без IP через L2TP	+
	IBM 2212 Access Utility (Ethernet)	Ср-во доступа с интегр. МЭ, ср-ва VPN	9 10/100-Мбит/с, 20 ГС, ISDN	Без IP через L2TP	+
	IBM 2212 Access Utility (Token Ring)	Ср-во доступа с интегр. МЭ,ср-ва VPN	9 4/16-Мбит/с, 20 ГС, ISDN	Без IP через L2TP	+
	IBM 2216 Nways Multiaccess Connector (Ethernet)	Коннектор для множ. Доступа с интегр. МЭ и ср-ми VPN	12 10-Мбит/с, 8 100-Мбит/с, 64 ГС, ISDN	Без IP через L2TP	+
	IBM 2216 Nways Multiaccess Connector (Token Ring)	Коннектор для множ. Доступа с интегр. МЭ и ср-ми VPN	12 4/16-Мбит/с, 64 ГС, ISDN	Без IP через L2TP	+
Intel	LanRover VPN Gateway 6.6	Оборудование VPN с МЭ и функциями маршрутизации	2 100-Мбит/с		+
Internet Devices	Fort Knox Policy Router, Professional Series	Средство маршрутизации на базе правил	3 10/100-Мбит/с3 10/100-Мбит/с		—
Internet Dynamics	Conclave 1.52	МЭ с интегр. ср-ми VPN, удал. доступа и обнаружения вирусов	Лимитируются ОС хост-компьютера (Windows NT)	Сквозная передача	—
Lucent Technologies	VPN Gateway 2.0 с ускорителем шифрования данных	Шлюз VPN с МЭ	4 10/100-Мбит/с	Сквозная передача IPX	+
	PortMaster 3 с ускорителем шифрования данных	Маршр. со ср-ми удаленного доступа (доп.)	1 10-Мбит/с, 2 ГС		+

Продолжение табл.П1

7	8	9	10	11	12	13	14
На базе Web (Java); на платф. NT, AIX и HP-UX	+	+/+	+/+	Патенто-ванных	MD5, SHA-1	DES, Triple-DES, DES-40	2850
На базе Web (Java); на платф. NT, AIX и HP-UX	+	+/+	+/+	PPTP, L2TP, L2F	MD5, SHA-1	DES, Triple-DES, DES-40	2850
На базе Web (Java); на платф. NT, AIX и HP-UX	+	+/+	+/+	PPTP, L2TP, L2F	MD5, SHA-1	DES, Triple-DES, DES-40	10 200
На базе Web (Java); на платф. NT, AIX и HP-UX	+	+/+	+/+	PPTP, L2TP, L2F	MD5, SHA-1	DES, Triple-DES, DES-40	10 200
На базе Web (Java); на платф. NT, AIX и HP-UX	+	+/+	+/+	PPTP, L2TP, L2F	MD5, SHA-1	DES, Triple-DES, DES-40	39 500
На базе Web (Java); на платф. NT, AIX и HP-UX	+	+/+	+/+	PPTP, L2TP, L2F	MD5, SHA-1	DES, Triple-DES, DES-40	39 500
GUI ОС NT/98/95	+	-/+	-/+	PPTP, L2TP, L2F	MD5, SHA-1, Null	DES-56, Triple-DES-168, Triple-DES-112, DES-40, Null	18 500
На базе HTTP (Java); использует SSL	+	-/+	-/+	Патенто-ванных	MD5, SHA-1	DES, Triple-DES, RC4	11 990
Встроенный GUI на платф. NT/98/95	+	-/+	-/+	—	MD5	DES, Triple-DES, RC2, RC4	4480 (только ПО)
На базе Java, интеграция с Navigator 4.05; платф. NT/98/95 и Solaris	+	-/+	-/+	—	HMAC MD5, HMAC SHA-1, Null	DES, Triple-DES, RC4, Null	25 980
На базе Java, командная строка	+	-/+	-/+	—	SHA-1, HMAC SHA-1, MD5, HMAC MD5, Null	DES, Triple-DES	13 590

1	2	3	4	5	6
Microsoft	Windows NT Server 4.0 SP4 Routing and Remote Access Service	Маршр. со ср-ми VPN, реализов. На уровне ОС	Лимитируются ОС хост-компьютера	Сквозная передача	—
NetScreen Technologies	NetScreen-10	МЭ с интегр. ср-ми VPN	3 10-Мбит/с	IPX	—
	NetScreen-100	МЭ с интегр. ср-ми VPN	3 10/100-Мбит/с		—
Norman Data Defense Systems	Norman Security Server	Шлюз VPN с МЭ	Лимитируются ОС хост-компьютера	Сквозная передача	+
Nortel Networks	Contivity Extra-net Switch 1500, версия 2.0	Шифрующий маршру-тизатор с МЭ	2 100-Мбит/с	Сквозная передача	+
Novell	BorderManager Firewall Services 3 cIPro System 3.30	Программные средства VPN на базе каталогов	Лимитируются ОС хост-компьютера		—
RAD-GUARD	Personal Ravlin 3.0.2	Выделенное уст-во VPN	2 или 4 10/100-Мбит/с	Сквозная передача	—
RedCreek Communica-tions	Ravlin 3200 3.0.2	Выделенное уст-во VPN	2 10-Мбит/с		—
	Ravlin 10/5100 3.0.2	Выделенное уст-во VPN	2 10-Мбит/с	Сквозная передача	—
Secure Computing	Sidewinder	МЭ со ср-ми VPN	8 10/100-Мбит/с		—
Sonic Systems	SonicWALL PRO	МЭ со ср-ми VPN	3 10/100-Мбит/с, 1 ГС		—
Technologic	Intercep-tor/InstaGate	МЭ со ср-ми VPN	5 10/100-Мбит/с, 1 ГС		—

Продолжение табл.П1

7	8	9	10	11	12	13	14
GUI ОС NT, командная строка	+	-/-	-/-	L2TP, MPPE	—	Null, RC4-40, RC4-128	1618 (только ПО)
На базе Web, командная строка	+	-/+	-/+	PPTP	MD5, SHA-1, Null	DES, Triple-DES, Null	7990
На базе Web, командная строка	+	-/+	-/+	PPTP	MD5, SHA-1, Null	DES, Triple-DES, Null	13 990
Встроенный GUI на платформе NT 4.0	+	-/-	-/-	PPTP	—	Blowfish	4 000 (только ПО)
На базе HTTP (доп. — с поддержкой Java)	—	-/+	-/+	—	MD5, SHA-1 (не все комбинации применимы к ESP)	DES, Triple-DES, DES-40	14 000
GUI ОС NT/98/95	+	-/+	-/+	L2TP, L2F, PPTP	HMAC MD5, MD5 с ключами, HMAC SHA-1, SHA-1 с ключами	DES, Triple-DES, RC2, RC5	1990 (только ПО)
GUI, автономное или на базе HP OpenView	+	+/+	+/+	PPTP	MD5, SHA-1, DES MAC, Triple-DES MAC	DES, Triple-DES, Null	15 000
GUI ОС NT/98/95	+	+/+	+/+	—	MD5, SHA-1	DES, Triple-DES, Null	2500
GUI ОС NT/98/95	+	+/+	+/+	Патентованных	MD5, SHA-1	DES, Triple-DES, Null	3600
Командная строка, GUI X Window	+	+/+	+/+	Патентованных	MD5, SHA-1	DES, Triple-DES, RC4	19 800
На базе HTTP	+	-/+	-/+	—	MD5, SHA-1, Null	DES, Triple-DES, Null, ARC4	5990
Secure HTTP (SSL) и Java	+	-/+	-/+	PPTP	MD5	DES, Triple-DES, RC2, RC4, Safer	7990

1	2	3	4	5	6
TimeStep	TimeStep Permit Gateway 4520	Выделенное уст-во VPN	2 10-Мбит/с		—
	TimeStep Permit Gateway 7520	Выделенное уст-во VPN	2 100-Мбит/с		—
	TimeStep Permit Gateway 2520	Выделенное уст-во VPN	2 4,5-Мбит/с		—
VPNet Technologies	VPNware VSU-1100, версия 2.51	Выделенное уст-во VPN	2 10/100-Мбит/с		+
	VPNware VSU-10	Выделенное уст-во VPN	2 10-Мбит/с	Сквозн. передача или блокировка; блок. трафика вне VPN	+
	VPNware VSU-1010	Выделенное уст-во VPN	2 10-Мбит/с	Сквозн. передача или блокировка; блок. трафика вне VPN	+
WatchGuard Technologies	WatchGuard LiveSecurity System	МЭ со ср-ми VPN	До 3 10/100-Мбит/с	Сквозн. передача или блокировка; блок. трафика вне VPN	—

Примечания:
ГС — глобальная сеть;
т/т ЗА — транспорт/туннелирование заголовков аутентификации;
т/т ИПЗ — транспорт/туннелирование инкапсулированного протокола защиты;
ПТ — протоколы туннелирования (кроеме IPSec, который поддерживают все продукты, кроме AltaVista Tunnel 98 (Compaq), Routing and Remote Service (Microsoft) и Norman Security Server (Norman Data Defense Systems)).

Окончание табл.П1

7	8	9	10	11	12	13	14
GUI ОС NT/98/95	+	-/+	-/+	PPTP	MD5, SHA-1, Null	DES, Triple-DES, Null, CAST, Blowfish, Idea, RC5	16 985
GUI ОС NT/98/95	+	-/+	-/+	—	MD5, SHA-1, Null		27 985
GUI ОС NT/98/95	+	-/+	-/+	—	MD5, SHA-1, Null		13 985
На базе Web; взаим. со шлюз. через SSL	+	+/+	+/+	—	MD5 (с ключ. и HMAC), HMAC SHA-1, Null	DES, Triple-DES, Null, RC5	37 985
На базе Web; взаимодействие со шлюзом через SSL	+	+/+	+/+	—		DES, Triple-DES, Null, RC5	7585
На базе Web; взаимодействие со шлюзом через SSL	+	+/+	+/+	—		DES, Triple-DES, Null, RC5	11 985
GUI ОС NT/98/95	+	-/+	-/+	PPTP	MD5, SHA-1, Null	DES, Triple-DES, Null	9980

Приложение 2. Документы по основным протоколам для виртуальных частных сетей

[источник информации — VPN Consortium — http://www.vpnc.org]

Протокол IPSec

RFC 2401 Proposed standard	Security Architecture for the Internet Protocol
RFC 2411 Informational RFC	IP Security Document Roadmap
RFC 2521 Experimental RFC	ICMP Security Failures Messages
RFC 2709 Informational RFC	Security Model with Tunnel-mode IPsec for NAT Domains
RFC 2764 Informational RFC	Framework for IP Based Virtual Private Networks
draft-ietf-nat-rsip-framework	Realm Specific IP: Framework
draft-ietf-nat-rsip-protocol	Realm Specific IP: Protocol Specification
draft-ietf-nat-rsip-ipsec	RSIP Support for End-to-end IPSEC
draft-ietf-ipsec-sctp Finished WG last call, waiting for AD review	On the Use of SCTP with IPsec
draft-ietf-ipsec-properties	Security Properties of the IPsec Protocol Suite
draft-ward-bgp-ipsec	Securing BGPv4 using IPsec
draft-ietf-ips-security	Securing Block Storage Protocols over IP
draft-sankar-lmp-sec	LMP Security Mechanism
draft-dupont-ipsec-mipv6	How to make IPsec more mobile IPv6 friendly
draft-ietf-send-psreq	IPv6 Neighbor Discovery trust models and threats
draft-ietf-ipsp-ipsecpib	IPSec Policy Information Base
draft-ietf-ipsp-msme	Multidimensional Security Policy Management and Enhancements for IP Security Policy
draft-ietf-ppvpn-ce-based	Framework for Provider Provisioned CE-based Virtual Private Networks using IPsec
draft-wang-cevpn-group	VPN Group Support for CE-based IPsec VPN
draft-wang-cevpn-routing	Routing Support in CE-based IPsec VPNs
draft-ietf-ipsec-monitor-mib	IPSec Monitoring MIB
draft-ietf-ipsec-isakmp-di-mon-mib	ISAKMP DOI-Independent Monitoring MIB
draft-ietf-ipsec-doi-tc-mib	IPSec DOI Textual Conventions MIB
draft-ietf-ipsec-ike-monitor-mib	IKE Monitoring MIB
draft-jenkins-ipsec-tun-mon-mib	IPsec Tunnel Monitoring MIB

Заголовки ESP и AH

RFC 2406 Proposed standard -- being updated by draft-ietf-ipsec-esp-v3	Encapsulating Security Payload (ESP)
draft-ietf-ipsec-esn-addendum	Extended Sequence Number Addendum to IPsec DOI for ISAKMP
RFC 2402 Proposed standards -- being updated by draft-ietf-ipsec-rfc2402bis	IP Authentication Header

Обмен ключами

RFC 2407 Proposed standard	Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 Proposed standard	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 Proposed standard	Internet Key Exchange (IKE)
RFC 2412 Informational RFC	OAKLEY Key Determination Protocol
RFC 2367 Informational RFC	PF_KEY Key Management API, Version 2
RFC 2522 Experimental RFC	Photuris: Session-Key Management Protocol
RFC 2523 Experimental RFC	Photuris: Extended Schemes and Attributes
RFC 3129 Informational RFC	Requirements for Kerberized Internet Negotiation of Keys
draft-ietf-ipsec-sonofike-rqts	Son-of-IKE Requirements
draft-ietf-ipsec-jfk	Just Fast Keying (JFK)
draft-ietf-ipsec-ikev2	Internet Key Exchange (IKE) Protocol, version 2
draft-ietf-ipsec-ikev2-rationale	Design Rationale for IKEv2
draft-ietf-ipsec-soi-features	Features of Proposed Successors to IKE
draft-spencer-ipsec-ike-implementation	IKE Implementation Issues
draft-ietf-ipsec-isakmp-gss-auth	GSS-API Authentication Mode for IKE
draft-nourse-scep	Cisco Simple Certificate Enrollment Protocol (SCEP)
draft-orman-public-key-lengths	Determining Strengths For Public Keys Used For Exchanging Symmetric Keys
draft-ietf-msec-gdoi	Group Domain of Interpretation
draft-arkko-map-doi	MAP Security Domain of Interpretation for ISAKMP
draft-ietf-ipsec-udp-encaps-main	UDP Encapsulation of IPsec Packets
draft-ietf-ipsec-nat-reqts	IPsec-NAT Compatibility Requirements
draft-ietf-ipsec-nat-t-ike	Negotiation of NAT-Traversal in the IKE
draft-richardson-ipsec-opportunistic	Method for doing opportunistic encryption with IKE
draft-ietf-kink-kink	Kerberized Internet Negotiation of Keys (KINK)
draft-ietf-ipsec-ike-lifetime	Responder Lifetime Notify Message for IKE
draft-keromytis-ike-id	'suggested ID' extension for IKE
draft-richardson-ipsec-ikeping	n echo request/reply mechanism for ISAKMP
draft-ietf-ipsec-revised-identity	Revised Use of Identity in Successors to IKE
draft-ietf-ipsec-pki-profile	Internet IP Security PKI Profile of ISAKMP and PKIX
draft-richardson-ipsec-rr	Method for storing IPsec keying material in DNS

Криптографические алгоритмы

RFC 2405 Proposed standard	ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2451 Proposed standard	ESP CBC-Mode Cipher Algorithms
RFC 2104 Informational RFC	HMAC: Keyed-Hashing for Message Authentication
RFC 2202 Informational RFC	Test Cases for HMAC-MD5 and HMAC-SHA-1
RFC 2403 Proposed standard	Use of HMAC-MD5-96 within ESP and AH
RFC 2404 Proposed standard	Use of HMAC-SHA-1-96 within ESP and AH
RFC 2857 Proposed standard	Use of HMAC-RIPEMD-160-96 within ESP and AH
RFC 2410 Proposed standard	NULL Encryption Algorithm and Its Use With IPsec
RFC 1828 Proposed standard	IP Authentication using Keyed MD5 (may be moved to Historic)
RFC 1829 Proposed standard	ESP DES-CBC Transform (may be moved to Historic)
RFC 2085 Proposed standard	HMAC-MD5 IP Authentication with Replay Prevention
RFC 3173 Proposed standard	IP Payload Compression Protocol (IPComp)
RFC 2394 Informational RFC	IP Payload Compression Using DEFLATE
RFC 2395 Informational RFC	JP Payload Compression Using LZS
RFC 3051 Informational RFC	IP Payload Compression Using ITU-T V.44 Packet Method
draft-ietf-ipsec-ike-modp-groups Finished WG last call, waiting for AD review	More MODP Diffie-Hellman groups for IKE
draft-ietf-ipsec-ciph-aes-cbc	AES Cipher Algorithm and Its Use With IPsec
draft-ietf-ipsec-ciph-aes-ctr	Using AES Counter Mode With IPsec ESP
draft-ietf-ipsec-ciph-aes-xcbc-mac Finished WG last call, waiting for AD review	AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
draft-ietf-ipsec-ciph-sha-256	HMAC-SHA-256-96 Algorithm and Its Use With IPsec
draft-ietf-ipsec-ciph-camellia	Camellia Cipher Algorithm and Its Use With IPsec

Удаленный доступ

RFC 2661 Proposed standard	Layer Two Tunneling Protocol (L2TP)
RFC 2888 Informational RFC	Secure Remote Access with L2TP
RFC 3193 Proposed standard	Securing L2TP using IPsec
draft-ietf-ipsra-pic	PIC, A Pre-IKE Credential Provisioning Protocol
draft-ietf-ipsra-reqmts	Requirements for IPsec Remote Access Scenarios
draft-ietf-ipsec-dhcp	Dynamic configuration of IPSEC VPN host using DHCP
draft-dukes-ike-mode-cfg	ISAKMP Configuration Method
draft-beaulieu-ike-xauth	Extended Authentication within IKE (XAUTH)

MPLS

RFC 3031 Full standard	Multiprotocol Label Switching Architecture
RFC 3032 Full standard	MPLS Label Stack Encoding
RFC 3036 Full standard	Label Distribution Protocol (LDP) Specification

RFC 3037 Informational RFC	LDP Applicability
draft-behringer-mpls-security	Analysis of the Security of the MPLS Architecture
RFC 2547 Informational RFC -- being updated by draft-ietf-ppvpn-rfc2547bis, intended for standards track	BGP/MPLS VPNs
draft-ietf-ppvpn-ipsec-2547	Use of PE-PE IPsec in RFC2547 VPNs
draft-ietf-ppvpn-gre-ip-2547	Use of PE-PE GRE or IP in RFC2547 VPNs
draft-rosen-ppvpn-2547bis-protocol	Protocol Actions for RFC2547bis
draft-ietf-ppvpn-as2547	Applicability Statement for VPNs Based on rfc2547bis
draft-ietf-ppvpn-requirements	Service requirements for Layer 3 Provider Provisioned Virtual Private Networks
draft-ietf-ppvpn-framework	Framework for Layer 3 Provider Provisioned Virtual Private Networks
draft-ietf-ppvpn-bgpvpn-auto	Using BGP as an Auto-Discovery Mechanism for Network-based VPNs
draft-ietf-ppvpn-l3vpn-auth	CE-to-CE Authentication for Layer 3 VPNs
draft-ietf-pwe3-arch	PWE3 Architecture
draft-ietf-pwe3-control-protocol	Transport of Layer 2 Frames Over MPLS
draft-ietf-pwe3-ethernet-encap	Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks
draft-ietf-l2tpext-pwe3-ethernet	Transport of Ethernet Frames over L2TPv3
draft-ietf-pwe3-frame-relay	Frame Relay over Pseudo-Wires
draft-ietf-pwe3-protocol-layer	Protocol Layering in PWE3
draft-ietf-pwe3-framework	Framework for Pseudo Wire Emulation Edge-to-Edge
draft-bryant-pwe3-terms	PWE3 Common Terminology
draft-stein-pwe3-controlword	PWE3 Control Word

Виртуальные маршрутизаторы

draft-ietf-ppvpn-as-vr	Applicability Statement for Virtual Router-based Layer 3 PPVPN approaches
draft-ietfppvpn-vpn-vr	Network based IP VPN Architecture using Virtual Routers
draft-ietf-ppvpn-vr-mib	Virtual Router Management Information Base Using SMIv2

СПИСОК ЛИТЕРАТУРЫ

1. Аписелла М. Горизонты сетей VPN // Computerworld. – 2001.— № 13.
2. Городецкий Я., Клочков А. Глобальный доступ в частные сети // Сетевой. – 2000.— № 11.
3. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. — СПб.: BHV, 2000.
4. Лукацкий А.В. VPN — старые песни о главном // Компьютер-Пресс.— 2001. — № 5.
5. Лукацкий А.В. Неизвестная VPN // Компьютер-Пресс. — 2001. — № 10.
6. Панасенко С.П. Виртуальные частые сети и другие способы защиты информации // Мир ПК. — 2002.— № 4.
7. Петренко С. VPN-технологии защищенного обмена конфиденциальной информацией // Информационная безопасность (Приложение к "Компьютер-ИНФО"). — 2000. — № 35 (219).
8. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. — ДМК. — 2000.
9. Романов М. Средства защиты информации //Сетевой.– 2000. – № 9.
10. Сальватор С. Виртуальные частные сети: новые предложения? // Сетевой. — 2000. — № 11.
11. Сериков И. Виртуальные частные сети // PC Magazine/RE – 1999. — № 7.
12. Турская Е. VPN как средство "неотложной помощи" // Сетевой. — 2000. — № 11.
13. Menezes A.J., vanOorschot P.C., Vanstone S.A. Handbook of Applied Cryptography // CRC Press, 1996. – 816 p.
14. Architecture for Public Key Infrastructure. The Open Group Guide. Doc. Num. G801. — http://www.opengroup.org/publications.
15. Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи".