ДЕНИСОВА Т.Б.

Построение виртуальной частной сети

Методические указания
к выполнению курсового и дипломного проекта

Рекомендовано УМО по образованию в области телекоммуникаций в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности “Защищенные системы связи”

Самара, 2006

УДК 004.732
Построение виртуальной частной сети. Методическое пособие для курсового и дипломного проектирования.
ПГАТИ. – Самара, 2006, 100 с.
27 рис., 24 табл.

Рассматриваются схемы организации виртуальной частной сети (VPN), характеристики VPN-продуктов, характеристики VPN-услуги, модели надежности и безопасности VPN-услуги, оценка надежности и безопасности VPN-услуги, протоколы VPN.

Для студентов, обучающихся по специальности “Защищенные системы связи”

Рецензенты:
д.ф.-м.н., проф. СамГУ – Астафьев В.И.,
к.т.н., доц. ПГАТИ – Зайкин В.П.

СОДЕРЖАНИЕ

1. Виртуальная частная сеть (VPN)

1.1 Определение, цели и задачи VPN.

Под термином “виртуальная частная сеть” (Virtual Private Network - VPN) понимают широкий круг технологий, обеспечивающих безопасную и качественную связь в пределах контролируемой группы пользователей по открытой глобальной сети.

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.

VPN можно применять для решения трех 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 корпоративной сетью отдельных мобильных пользователей или работающих дома сотрудников (удаленный доступ).

В качестве среды для создания виртуальных частных сетей выступают сети пакетной коммутации: X.25, FR, ATM, IP (Internet). Наиболее популярны технологии VPN, рассчитанные на использование в среде Internet.

1.2 Качество обслуживания в VPN.

Параметрами качества обслуживания в VPN являются характеристики транспортного обслуживания: задержка, вариация задержки и доля потерянных пакетов при транспортировке по сети. Эти параметры оговариваются в соглашении о качестве обслуживания, которое заключается между провайдером сети и клиентом. Для обеспечения качества обслуживания необходимы дополнительные технологические механизмы, встроенные в протоколы и оборудование сети.

Технология FR имеет встроенные возможности для поддержки дифференцированного качества обслуживания для разных виртуальных каналов. Гарантируемыми параметрами качества являются средняя согласованная пропускная способность и максимальная пульсация трафика. Если клиенту нужно передавать разные виды трафика с разным качеством обслуживания, то он просто заказывает несколько виртуальных каналов соответствующего качества.

Технология ATM имеет более тонкие процедуры поддержания параметров качества обслуживания, чем технология FR. ATM предоставляет трафику реального времени гарантии по задержкам передаваемых пакетов.

Internet пока не может дать пользователям гарантий дифференцированного обслуживания.

В частных IP-сетях провайдер имеет набор механизмов для дифференцированного обслуживания своих клиентов. К таким механизмам относятся приоритетное обслуживание (обслуживание очередей WFQ), резервирование полосы пропускания (протокол резервирования ресурсов RSVP), поддержка виртуальных каналов (протокол коммутации меток MPLS).

1.3 Защита данных в VPN.

Для того чтобы виртуальные частные сети использовались как полноценный транспорт для передачи трафика, необходимы не только гарантии на качество передачи, но и гарантии в безопасности передаваемых данных. Многие специалисты прежде всего связывают термин “виртуальные частные сети” именно с безопасностью данных.

При подключении корпоративной сети к любой открытой сети возникает два вида угроз:

1. несанкционированный доступ к внутренним ресурсам корпоративной сети, полученный злоумышленником в результате логического входа в эту сеть,
2. несанкционированный доступ к корпоративным данным в процессе их передачи по открытой сети.

Для того чтобы виртуальная частная сеть по уровню безопасности приблизилась к истинной частной сети, в которой эти угрозы практически отсутствуют, VPN должна включать средства для отображения угроз как первого, так второго типов. К средствам VPN относится широкий круг устройств безопасности: многофункциональные брандмауэры, маршрутизаторы со встроенными возможностями фильтрации пакетов, proxy-серверы, аппаратные и программные шифраторы передаваемого трафика.

2. Организация VPN

2.1 VPN устройства

Виртуальные частные сети отличаются друг от друга многими характеристиками: набором функциональных возможностей VPN-устройств, точками размещения VPN-устройств, типом платформы, на которой работают эти устройства, применяемыми протоколами шифрования и аутентификации. Существует несколько типов VPN-устройств:

- *отдельное аппаратное устройство* VPN на основе специализированной ОС реального времени, имеющее два или более сетевых интерфейса и аппаратную криптографическую поддержку,
- *отдельное программное решение,* которое дополняет стандартную операционную систему функциями VPN,
- *расширение брандмауэра* за счет дополнительных функций защищенного канала,
- *средства VPN, встроенные в маршрутизатор* или коммутатор.

Устройства VPN могут играть в виртуальных частных сетях роль шлюза или клиента.

Шлюз VPN – это сетевое устройство, подключенное к нескольким сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов позади него. Размещение шлюза должно быть аналогично размещению брандмауэра, т.е. таким образом, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. 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. Шлюз VPN может быть реализован всеми перечисленными выше способами, т.е. в виде отдельного аппаратного устройства, отдельного программного решения, а также в виде брандмауэра или маршрутизатора, дополненных функциями VPN.

Клиент VPN – это программный или аппаратно-программный комплекс, обычно на базе персонального компьютера. Его сетевое транспортное обеспечение модифицировано для выполнения шифрования и аутентификации трафика, которым устройство обменивается со шлюзами VPN и/или другими клиентамиVPN. Обычно реализация VPN-клиента представляет собой программное решение.

Для создания виртуальной частной сети предприятия нужны как VPN-шлюзы, так и VPN-клиенты. Шлюзы целесообразно использовать для защиты локальных сетей предприятия, а VPN-клиенты – для удаленных и мобильных пользователей, которым требуется устанавливать соединения с корпоративной сетью через Интернет.

2.2 Расположение VPN устройств в сети

При создании защищенных каналов виртуальных частных сетей 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:

- 1 схема (пользовательская) — все средства VPN размещаются в сети предприятия;
- 2 схема (провайдерская) — все средства VPN размещаются в сети провайдера;

- 3 схема (смешанная) — часть средств VPN размещены в сети провайдера, а часть — в сети предприятия.

2.2.1 Пользовательская схема

Предприятие самостоятельно защищает данные, передаваемые по публичной сети, размещая VPN-шлюзы и VPN-клиенты в своей сети и на своей территории (рис. 2.1). Такую схему иногда называют пользовательской. Оборудование VPN физически находится в помещении предприятия. Предприятие берет на себя полностью задачу обеспечения безопасности, а у провайдера только получает гарантированную (или негарантированную) пропускную способность. Локальные сети 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 корпоративной сети, расположенной позади него.

При образовании защищенных каналов между шлюзами различных локальных сетей 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 локальной сети 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).

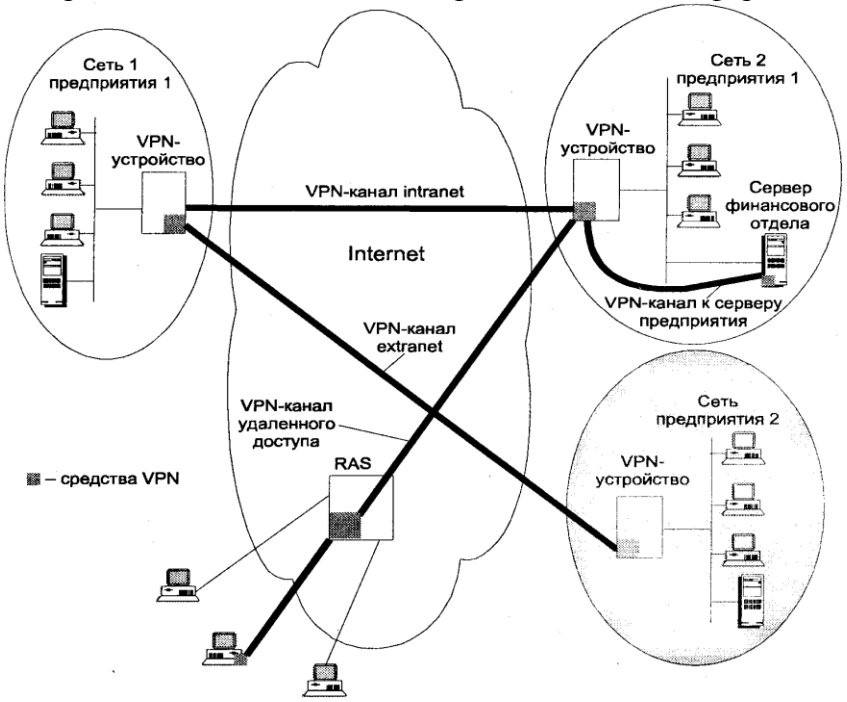

Рис.2.1. Организация VPNс помощью средств предприятия.

В целом схема, при которой все оборудование VPN размещается на территории предприятия, с точки зрения администратора предприятия обладает рядом как достоинств, так и недостатков.

Достоинства:

- прежде всего, это полный контроль администратора предприятия над ситуацией по защите корпоративной сети: 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 программное обеспечение 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.

2.2.2 Провайдерская схема

В данном случае виртуальная частная сеть организуется исключительно с помощью средств провайдера, поэтому такая схема и называется провайдерской (рис. 2.2). Провайдер устанавливает в своей сети некоторое количество VPN-шлюзов, образующих защищенные каналы внутри публичной сети для тех своих клиентов, которые пожелали воспользоваться услугами VPN. Это хорошо масштабируемое и экономичное решение, управляемое централизованно администратором сети провайдера.

Для компьютеров корпоративной сети (как объединенных в локальные сети, так и автономных) защищенный канал прозрачен. Программное обеспечение этих конечных узлов остается без изменений, а также отпадает необходимость приобретения, конфигурирования и поддержки собственного VPN-шлюза. Реализация провайдерского варианта VPN по-прежнему требует участия администратора корпоративной сети, хотя и в гораздо меньшем объеме по сравнению с предыдущим вариантом. Как минимум, администратор должен предоставить провайдеру перечень адресов, входящих в состав интрасети и экстрасети предприятия, а возможно, и данные для аутентификации пользователей и оборудования корпоративной сети.

Гибкость этой схемы состоит в легкости подключения новых пользователей к существующим защищенным каналам, независимо от места их расположения. Особенно это полезно при подсоединении к экстрасети — вместо индивидуального конфигурирования VPN-средств на каждом конце канала вносятся изменения только в VPN-шлюзы провайдера данного предприятия и провайдера предприятия-партнера. При этом необходимо, чтобы оба провайдера использовали совместимые средства VPN.

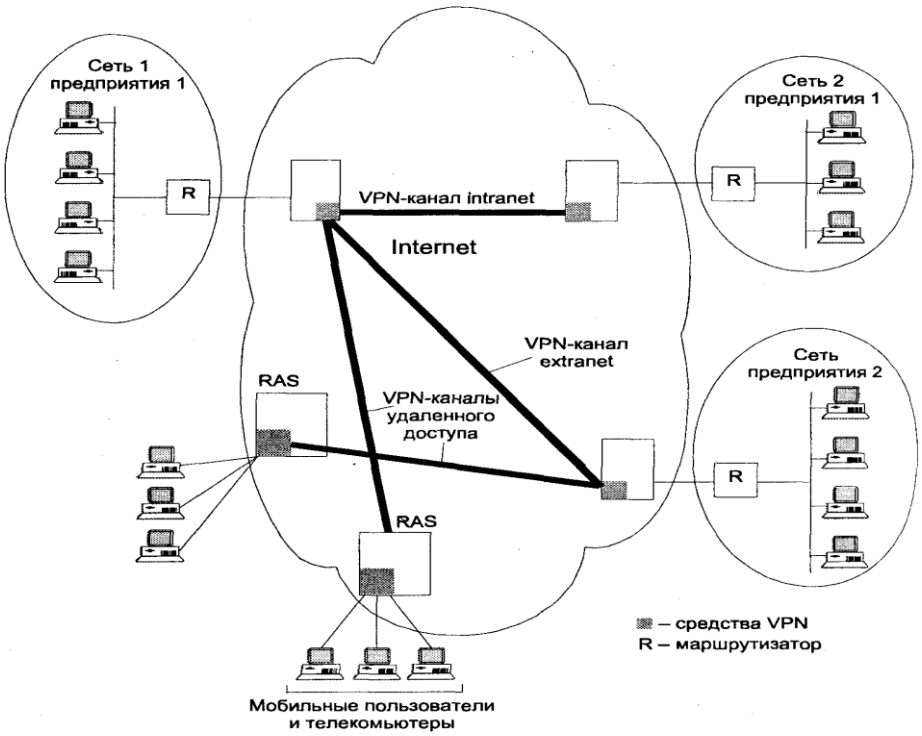

Рис. 2.2. Организация VPN средствами провайдера

Вариант, когда все заботы по поддержанию защищенного канала берет на себя провайдер публичной сети, оставляет тем не менее сомнения в надежности защиты: во-первых, незащищенными оказываются каналы доступа к публичной сети, во-вторых, потребитель услуг чувствует себя в полной зависимости от добросовестности провайдера. И тем не менее, специалисты прогнозируют, что именно вторая схема в ближайшем будущем станет основной в построении защищенных каналов.

Приведенная на рис. 2.2 схема требует уточнения, что Internet — это не однородное облако, никому не принадлежащее, а совокупность сетей, находящихся под административным контролем большого количества предприятий и организаций. Если услуги VPN предоставляет провайдер, владеющий некоторой магистральной частью Internet, то схема расположения VPN-оборудования может быть уточнена. На рис. 2.3 показаны IP-сети провайдера А, которые являются неотъемлемыми частями Internet и в то же время полностью контролируются данным провайдером.

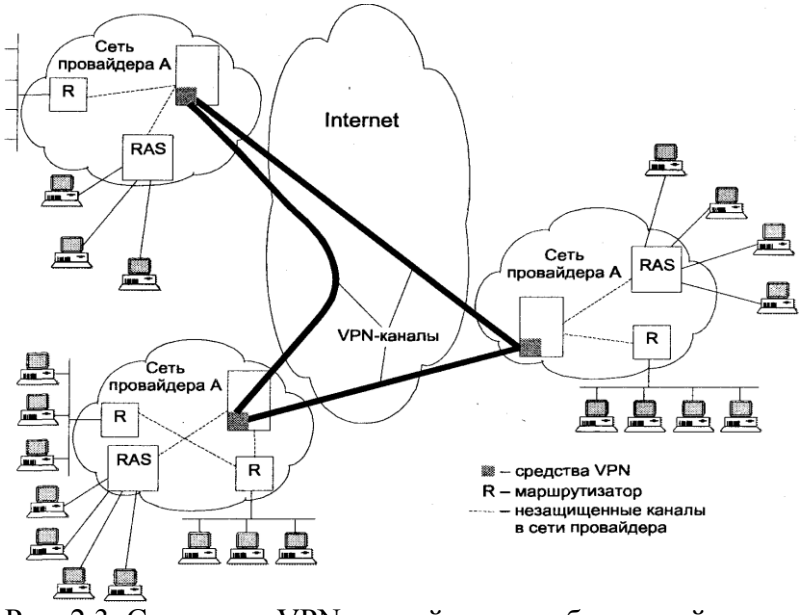

Рис. 2.3. Структура VPN провайдера с собственной магистралью

В пределах своей сети провайдер обычно гарантирует безопасность передаваемых данных своим клиентам без использования средств VPN, и только в точках соединения своих сетей с публичной частью Internet устанавливает VPN-шлюзы. Поэтому, когда трафик клиентов интрасети и экстрасети проходит только через магистраль одного провайдера, то он обслуживается, как правило, без создания защищенных каналов VPN. И только в том случае, когда необходимо либо соединить сети одного провайдера через публичный Internet, либо создать экстрасеть для предприятий, подключенных к разным провайдерам, используется технология VPN.
Можно отметить следующие достоинства и недостатки провайдерской схемы построения VPN.
Достоинства для пользователя:

- не нужно покупать и обслуживать дорогое и сложное VPN-оборудование.

Недостатки для пользователя:

- пользователь должен доверить провайдеру секретную информацию (пароли, ключи).

Участок пути между помещением пользователя и оборудованием провайдера, включающий канал доступа к глобальной сети и промежуточные каналы между провайдером доступа и VPN-провайдером, не защищен.
Достоинства для провайдера:

- провайдеру легче обеспечить высокую готовность VPN, используя оборудование провайдерского класса;
- провайдеру легче диагностировать и устранять проблемы, не командируя сотрудников на предприятия заказчика;
- провайдер может тесно интегрировать VPN-услуги с его возможностями по поддержанию дифференцированного качества обслуживания для приложений пользователя;
- закрепление за собой клиентов из-за недостаточного уровня стандартизации услуг VPN в настоящее время.

Учитывая, что каждая из рассмотренных схем имеет свои достоинства и недостатки, можно ожидать, что в ближайшем будущем станут применяться обе

2.2.3 Смешанная схема

Виртуальная частная сеть может быть организована и на основе смешанного варианта — VPN-устройства размещаются как в сети провайдера, так и в корпоративной сети. Это происходит в тех случаях, когда предприятие для создания VPN пользуется услугами одного провайдера, но имеет некоторое количество сетей и удаленных пользователей, подключенных к Internet через сети других провайдеров. В таком случае приходится устанавливать в сетях и компьютерах удаленных пользователей предприятия, обращающихся к услугам других провайдеров, собственные средства VPN (рис. 2.4).

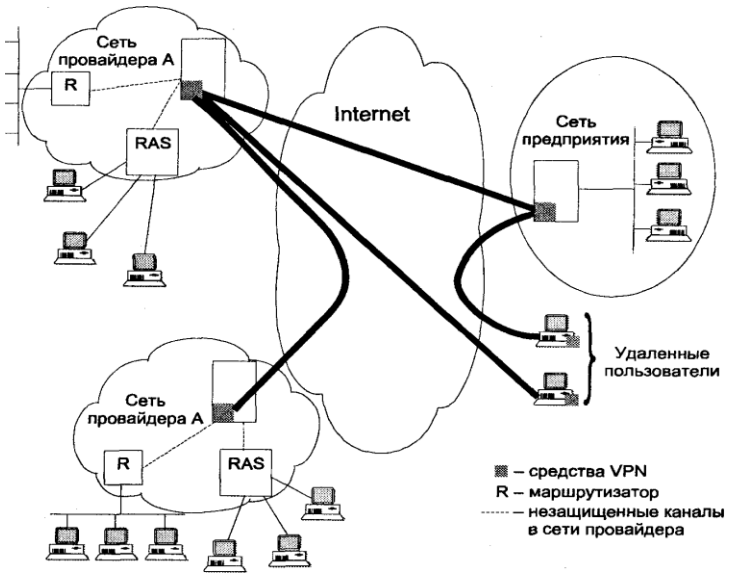

Рис. 2.4. Организация VPN с использованием средств провайдера и предприятия

Этот вариант, как компромиссный, обладает достоинствами и недостатками предыдущих вариантов.

3. Решения для построения VPN

3.1 Решения отечественных компаний

3.1.1.Аппаратно-программный комплекс КРИПТОН-IP КОМПАНИИ «АНКАД» для VPN

Типичная схема подключения локальной компьютерной сети к глобальной сети Internet с использованием криптографического маршрутизатора (КМ) КРИПТОН-IP показана на рис. 3.1.

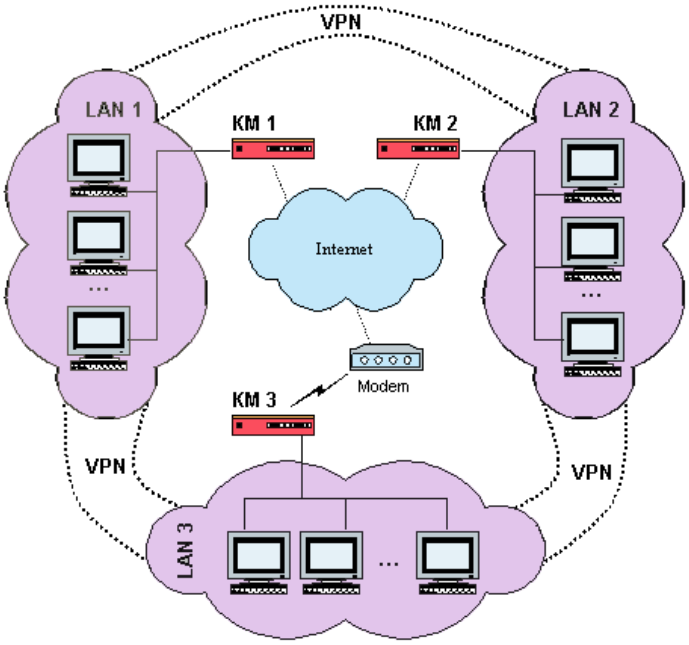

Рис.3.1 Решение компании «АНКАД» для VPN

КМ производит шифрование информации, вычисление имитовставок по алгоритму ГОСТ 28147-89 и выполняет функции статического фильтра пакетов данных и обеспечивает контроль прохождения всего IP-трафика.

Наиболее эффективно использовать КМ в качестве шифратора на проходе, установленного в разрыве между ЛВС и маршрутизатором доступа, функции которого может выполнять и сам КМ при наличии статической IP-адресации в сети.

Все криптомаршрутизаторы ВЧС авторизуются: каждый имеет уникальный ключ, известный другим КМ. Поскольку КМ обрабатывает и пропускает в локальную сеть только пакеты, приходящие от авторизованных КМ, то локальные сети оказываются защищенными от вторжения извне.

Таблица 3.1. Основные характеристики КМ КРИПТОН-IP

Название продукта (тип)	Интерфейсы	Производительность	Криптопротоколы	Алгоритмы шифрования/Алгоритмы аутентификации
КМ	Адаптеры LAN Ethernet, нуль-модемный кабель, PPP-устройства (модемы)	1,2-1,8 Мбит/с (Intel 486)	Собственный, IP, Ipsec	ГОСТ 28147-89, MD5

3.1.2 Решение ViPNet Custom российской компании «Инфотекс»

Решение ViPNet Custom предназначено для объединения в единую защищенную виртуальную сеть произвольного числа рабочих станций, мобильных пользователей и локальных сетей.

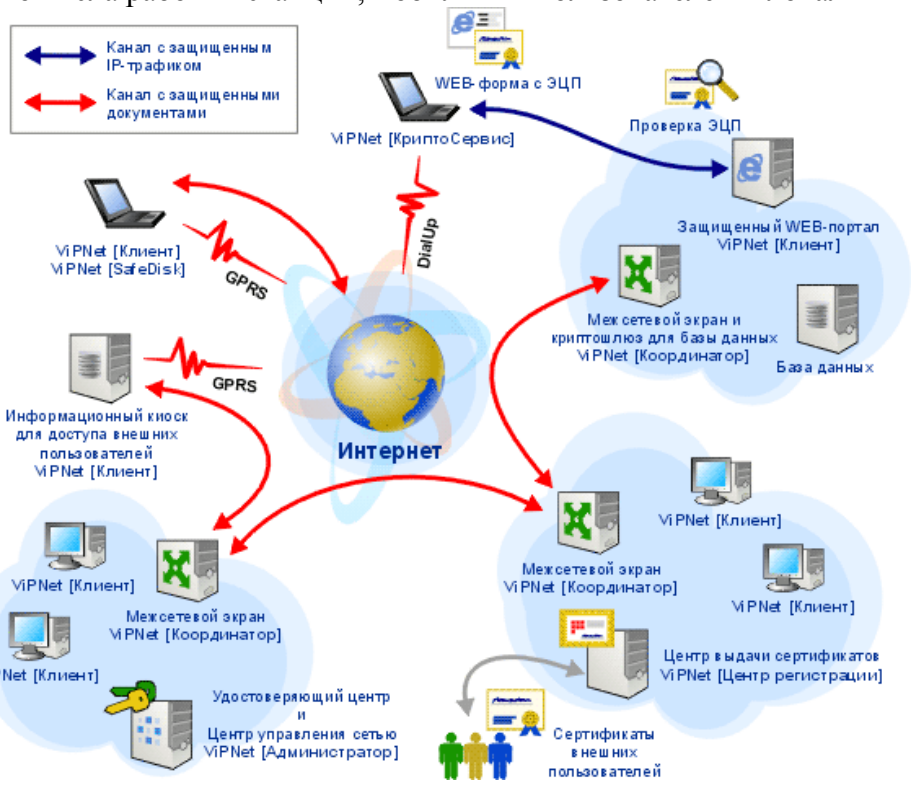

Рис. 3.2 Решение ViPNet Custom компании «Инфотекс»

Решение ViPNet CUSTOM может содержать следующие программные компоненты, которые могут быть выбраны заказчиком системы по его желанию:

ViPNet [Администратор] - отвечает за развертывание и администрирование защищенной сети, включая функции Удостоверяющего Центра. Создает инфраструктуру сети, осуществляет мониторинг и управление объектами сети. Он так же формирует первичную ключевую и парольную информацию для объектов сети, сертифицирует ключевую информацию, сформированную объектами сети;

Включает в себя программы : Центр Управления Сетью и Ключевой Центр.

Создание объектов сети ViPNet, связей между ними, формирование симметричной ключевой информации, формирование первичных ключевых дистрибутивов, дистанционное обновление и смену ключевой информации, централизованное формирование электронной цифровой подписи (ЭЦП) и выдачу цифровых сертификатов на открытые ключи ЭЦП, сформированные на местах, осуществляет ПО ViPNet[Администратор] в составе ПО [Центр управления сетью] (ЦУС) и ПО [Ключевой и удостоверяющий центр] (КЦ). Центры управления различных виртуальных сетей могут взаимодействовать между собой для организации защищенного межсетевого взаимодействия между узлами своих сетей.

ViPNet [Координатор] - реализует все серверные функции в рамках защищенной сети: криптомаршрутизатор, криптошлюз, межсетевой экран, сервер защищенной почты и многое другое. Выполняет маршрутизацию защищенных пакетов при взаимодействии объектов сети между собой, регистрацию и предоставление информации о состоянии объектов сети, работу защищенных компьютеров локальной сети в VPN от имени одного адреса, туннелирование пакетов от заданных незащищенных компьютеров локальной сети, фильтрацию открытых пакетов

в соответствии с заданной политикой безопасности, осуществляет возможность работы защищенных компьютеров локальной сети через сетевые экраны других производителей.

ViPNet [Клиент] - **м**одуль, реализующий все клиентские функции в рамках защищенной сети: клиентское шифрование, персональный сетевой экран, контроль сетевой активности приложений, встроенная система обнаружения атак (IDS), развитая система аудита, клиент защищенной почтовой службы и многое другое. Обеспечивает защиту информации при ее передаче по открытым каналам сетей общего пользования, а так же защиту от доступа к ресурсам компьютера из сетей общего пользования.

ViPNet [ЦентрРегистрации] - выполняет роль "филиала" Удостоверяющего Центра - ViPNet [Администратора]**,** который можно установить в удаленной локальной сети и обеспечить процедуру выдачи и сертификации ЭЦП внешних пользователей - физических и юридических лиц.

Программа Центр Регистрации предназначена для регистрации внешних пользователей и получения для них в УКЦ цифровых сертификатов. Право работать в данной программе определяется программой Центра управления путем регистрации узла в задаче ЦР и формирования соответствующего справочника доступа. В системе может присутствовать произвольное количество ЦР.

В Центре Регистрации при предъявлении документов внешним пользователем, подтверждающих его полномочия, создается запрос на сертификат, производится отправка его в УКЦ и осуществляется ввод в действие изданного в УКЦ сертификата. В Центре Сертификации сертификат будет либо удовлетворен, либо отклонен. Только запрос на сертификат со статусом "удовлетворен" становится сертификатом подписи, и этот сертификат может быть введен в действие. После введения в действие сертификата, внешний пользователь сможет пользоваться им (подписывать документы) на любом узле с установленным ПО ViPNet.

Таблица 3.2. Основные характеристики ViPNet Custom

Название продукта (тип)	Интерфейсы	Производительность	Криптопротоколы	Алгоритмы шифрования/Алгоритмы аутентификации
VipNet Клиент	COM-интерфейс, Управление конфигурацией сети, есть встроенное IDS, драйвер Программа “Контроль приложений”	Канал 100Мбит, пропусканная способность составляет 60-70 Мбит/с	Собственный	ГОСТ 28147-89(зависит от настроек), DES, 3DES,RC6, AES/-
ПО VipNet Координатор	COM-порт, драйвер Программа “Контроль приложений”	Канал 10Мбит Pentium III/ 450 - 9.5Мбит/с Канал 100Мбит Pentium III/ 450 - 20Мбит/с Pentium III/700 - 28Мбит/с	Собственный, стек протоколов TCP/IP(туннелирование), IP/241	ГОСТ 28147-89(зависит от настроек), DES, 3DES, AES/-
ЦУ сетью ПО VipNet Администратор	API-интерфейс, внутренний мониторинг и управление объектами сети	С применением аппаратного крипто-акселератора ViPNet Turbo 100 60-70 Мбит/с	Собственный, IKE	ГОСТ 28147-89(зависит от настроек), DES, 3DES, AES, RC6/MD5
ПО ViPNet [Центр регистрации]	COM-интерфейс	не ниже 28Мбит/с(не ниже Pentium III), ОЗУ - не менее 128 Мбайт	Собственный	ГОСТ 28147-89(зависит от настроек), DES, 3DES,RC6/-

3.1.3 Решения «Микротест» на базе сертифицированных VPN-продуктов компании «Инфотекс»

В связи с тем, что программный комплекс «ViPNet» обеспечивает не только защиту трафика, передаваемого между компьютерами, но также защищает сами компьютеры от сетевых атак за счет интегрированных персональных межсетевых экранов, компания «Микротест» использует данный продукт для создания клиентских VPN.
СОСТАВ КОМПЛЕКСА:
ViPNet [Администратор]: Центр Управления Сетью, Ключевой Центр,
ViPNet [Координатор],
ViPNet [Клиент].

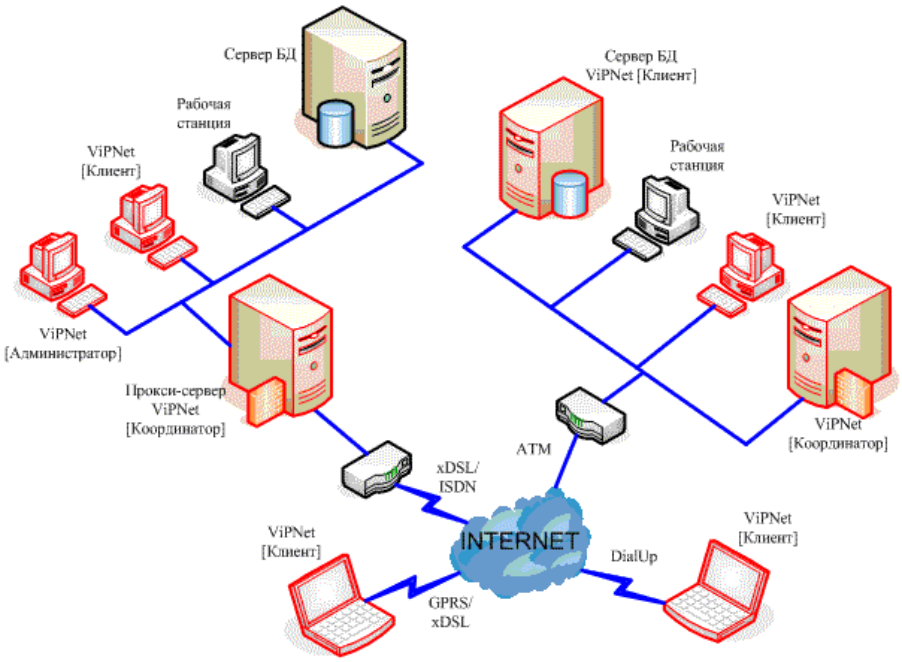

Рис. 3.3. Решение «МИКРОТЕСТ» на базе продуктов компании «Инфотекс»

ViPNet [Администратор] включает в себя программы: Центр Управления Сетью и Ключевой Центр.
Центр Управления Сетью является регистрационным центром и предназначен для конфигурации и управления виртуальной сетью.Ключевой Центр предназначен для обеспечения ключевой информацией всех участников VPN и выполнения функций удостоверяющего центра. При этом первичные клиентские ключевые наборы могут быть записаны на дискеты, смарт-карты, touch memory, e-token и прочее для передачи участникам VPN. Последующее обновление ключевой информации осуществляется автоматически по защищенным каналам VPN.
ViPNet[Координатор] – модуль, осуществляющий в зависимости от настроек следующие функции:

- *Сервер-туннель*. Модуль позволяет организовать защиту (шифрование) трафика между локальными сетями или группами компьютеров этих сетей для передачи его по открытой глобальной сети. При этом весь IP-трафик туннелируется в защищенное соединение между ViPNet [Координаторами] по UDP-протоколу. Модуль также позволяет обеспечить защищенное управление маршрутизаторами сети (Cisco и др.) за счет использования технологии обратного туннеля.
- *Межсетевой экран*. Модуль обеспечивает фильтрацию IP-трафика от всех источников вне VPN и источников, трафик от которых туннелируется в соответствии с заданной

политикой. Также модуль является мультиинтерфейсным межсетевым экраном для разделения локальной сети на несколько сегментов с разными уровнями безопасности.

- *Proxy-сервер* защищенных соединений. Модуль обеспечивает работу абонентских пунктов защищенной сети от имени одного адреса.
- *Сервер "открытый Интернет"*. Модуль, который устанавливается в точке присоединения локальной сети к Интернет и обеспечивает фильтрацию и туннелирование открытого трафика при доставке его к компьютеру локальной сети с установленной на нем компонентой ViPNet [Клиент].
- *Почтовый сервер*. Модуль обеспечивает маршрутизацию почтовых конвертов, а также управляющих сообщений Центра Управления Сетью при взаимодействии объектов сети между собой.
- *Сервер IP-адресов*. Модуль обеспечивает работу с динамическими IP-адресами.

Функциональность ViPNet [Координатора] определяется Центром управления сетью.

ViPNet [Клиент] – модуль, используемый как для обеспечения защиты удаленного доступа к сети офиса так и построения VPN между компьютерами внутри сети офиса, реализует на рабочем месте следующие функции:

- *Персональный сетевой экран* - возможность защитить компьютер от НСД как из глобальной, так и из локальной сети. Сетевой экран позволяет системному администратору или пользователю (при наличии соответствующих полномочий):

1) Управлять доступом к данным компьютера.
2) Обеспечивать соединения с другими узлами только по инициативе пользователя.
3) Контролировать активность сетевых приложений на данном компьютере.
4) Определять адреса злоумышленников, пытающихся получить доступ к компьютеру.
5) Установление VPN-соединений. Эта функция дает возможность устанавливать защищенные соединения с VipNet [Координаторами] и другими компьютерами, оснащенными ViPNet [Клиентом]. Возможность установления защищенных соединений между компьютерами, оснащенными ViPNet [Клиентом] позволяет:

1. Организовать схему защищенного использования всевозможных Web-приложений с доступом к Web-платформе, на которой установлен ViPNet [Клиент], только определенному списку участников VPN.
2. Защитить и дополнительно авторизовать все соединения между локальными, мобильными и удаленными пользователями, оснащенными ViPNet [Клиентом], и корпоративными серверами приложений, баз данных, SQL-серверами, также оснащенными ViPNet [Клиентом]. Благодаря этому становится защищенным внедрение всевозможных ERP-систем, финансово-учетных систем, работающих в реальном времени, систем типа "Клиент-Банк", "Интернет-Банк", CRM-систем и прочих систем, где с одной стороны накапливается конфиденциальная информация, требующая соблюдения правил информационной безопасности и управления доступом, а с другой стороны необходима коллективная работа с приложениями на сети разных категорий пользователей.
3. Использовать недорогие и общедоступные сетевые ресурсы открытой сети для передачи конфиденциальной информации.

- *Услуги защищенных служб реального времени*. Модуль предназначен для защиты циркулярного обмена сообщениями, проведения конференций, аудио- и видео-переговоров и позволяет:

1. Обмениваться сообщениями или организовывать циркулярный обмен сообщениями, в процессе которого организатор такого обмена видит все сообщения, в то же время участники обмена сообщений друг друга не видят. При этом ведутся и могут быть сохранены протоколы всех сообщений.
2. Проводить защищенные конференции.
3. Проводить защищенные аудио- (Voice over IP) и видео-переговоры (конференции). Технология ViPNet поддерживает любые стандартные программные и аппаратные средства для проведения аудио- и видео-конференций, основанные на IP-технологиях.

- *Сервис защищенных почтовых услуг (деловая почта)*. Модуль предоставляет услуги защищенной “деловой почты” с возможностями аутентификации отправителя и получателя, а также обеспечивает контроль за прохождением и использованием документов.

Таблица 3.3. Основные характеристики ViPNet

Название продукта (тип)	Интерфейсы/Управление	Производительность	Криптопротоколы	Алгоритмы шифрования/ Алгоритмы аутентификации
ViPNet [Администратор]: Центр Управления Сетью, Ключевой Центр.	API-интерфейс, внутренний мониторинг и управление объектами сети	С применением аппаратного крипто-акселератора ViPNet Turbo 100 60-70 Мбит/с	Собственный, IKE	ГОСТ 28147-89(зависит от настроек), DES, 3DES,RC6, AES
ViPNet [Координатор]	COM-порт, драйвер Программа “Контроль приложений”	С применением аппаратного крипто-акселератора ViPNet Turbo 100 60-70 Мбит/с	Собственный	ГОСТ 28147-89(зависит от настроек), DES, 3DES,RC6, AES
ViPNet [Клиент]	COM-интерфейс, Управление конфигурацией сети	С применением аппаратного крипто-акселератора ViPNet Turbo 100 60-70 Мбит/с	Собственный	ГОСТ 28147-89(зависит от настроек), DES, 3DES,RC6, AES

3.2 Решения зарубежных компаний

3.2.1. Межсетевые экраны Juniper Networks (NetScreen)

Межсетевые экраны Juniper Networks (NetScreen) – семейство специализированных продуктов, объединяющих функции межсетевого экрана (firewall), концентратора виртуальных частных сетей (VPN), маршрутизатора и средства управления трафиком (bandwidth manager). Во всех продуктах NetScreen реализуются аппаратно на базе высокоскоростных заказных микросхем (ASIC). Гарантированная пропускная способность устройств до 12Гбит/с.

Обеспечивая максимальную производительность, высокую отказоустойчивость и масштабируемость, межсетевые экраны Juniper Networks (NetScreen) позволяют защитить высокоскоростные магистральные сети, не создавая препятствий, что является неотъемлемым требованием для телекоммуникационных компаний и операторов связи.

Решение компании Juniper Networks представлено на рис. 3.4.

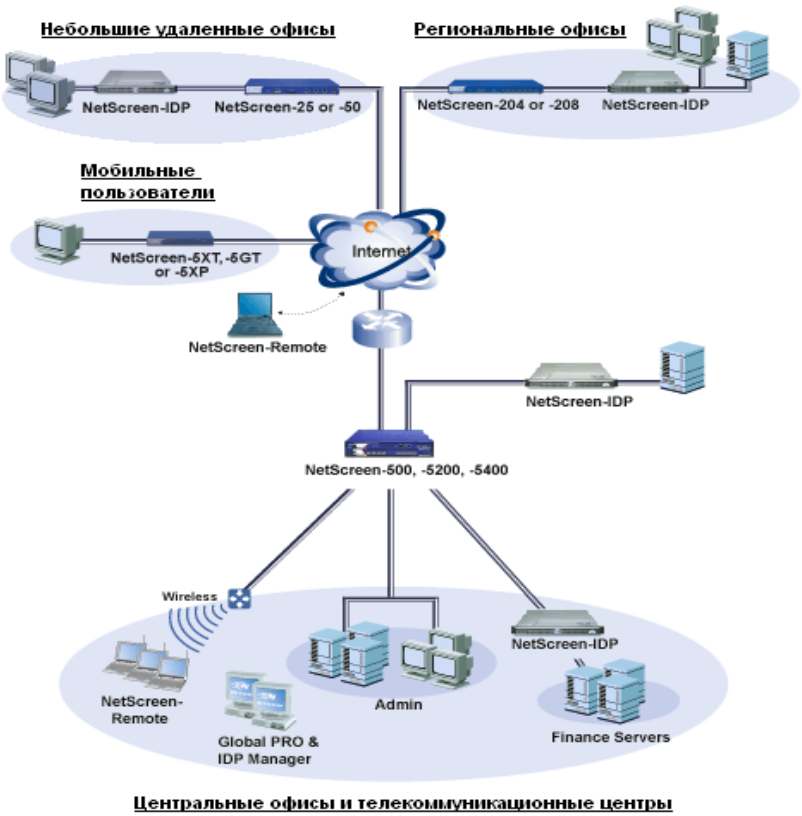

Рисунок 3.4 – Архитектура решений Juniper Networks(NetScreen)

Центральные офисы и телекоммуникационные центры

NetScreen-500 – модульная система, предусматривающая подключение до 4 портов Gigabit Ethernet или 8 портов FastEthernet и пропускную способность 700Мбит/с, предназначена для использования в центрах обработки данных, центральных корпоративных узлах доступа к Интернет, сетях операторов связи.

NetScreen-5000 – модульная высокопроизводительная система, предусматривающая подключение до 24 портов Gigabit Ethernet или 72 портов FastEthernet и пропускную способность 12Gbps. Предназначена для использования в крупных центрах обработки данных, сетях операторов связи, предоставля.щих услуги по защите информации.

NetScreen-IDP – системы обнаружения и предотвращения вторжений (IDP) – семейство специализированных продуктов, особенностью которых является использование комплексного метода обнаружения вторжений на 2-7 уровнях модели OSI (включающего анализ поведения протоколов, характера трафика, обнаружение предопределенных последовательностей, распознавание атак типа backdoor, IP spoof, Syn-flood и др.), точность которого позволяет осуществляеть немедленную терминацию атак в реальном времени. Семейство продуктов NetScreen-IDP включает три одинаковые по функциональности модели (IDP-50, IDP-200, IDP-600, IDP-1100), различающиеся величиной пропускной способности и ассортиментом интерфейсов. NetScreen-IDP включается непосредственно в линию связи и может работать в режиме моста (без IP адресов на интерфейсах) и маршрутизатора. Устройство может быть использовано и в качестве пассивного детектора атак (сниффера).

Комплексный метод включает в себя ряд технологий обнаружения атак, основными из которых являются: обнаружение предопределенных последовательностей (Signature Detection), анализ поведения протоколов, Backdoor Detection, Network Honeypot.

Региональные офисы

NetScreen-204 и NetScreen-208 отличаются количеством портов Ethernet 10/100 (четыре и восемь соответственно). Это наиболее универсальные устройства безопасности, имеющиеся на рынке и легко интегрируемые в многие приложения, включая средние и крупные корпоративные сети, е-бизнес приложения, центры обработки данных, инфраструктуру операторов связи и интернет-

провайдеров. Устройства обеспечивают производительность 550 Mbps и 400 Mbps (устройства 208 и 204 соответственно) при выполнении функций межсетевого экрана. Даже для таких ресурсоемких приложений как применение алгоритмов шифрования 3DES и AES, устройства обеспечивают скорость 200 Mbps.

Небольшие удаленные офисы

NetScreen-50 и NetScreen-25 обеспечивают интегрированное решение для малого и среднего бизнеса и для удаленных офисов. Имеют 4 порта Ethernet 10/100. Устройства обеспечивают гибкое решение для задач, где требуются несколько демилитаризованных зон (DMZ), беспроводная локальная сеть, или несколько независимых сегментов сети. NetScreen 50 высокопроизводительное устройство обеспечивает 170 Mbps при выполнении функций межсетевого экрана и 50 Mbps для 3DES, с поддержкой 8,000 сессий и 100 VPN туннелей (100Mbps, 20Mbps при 3DES VPN, 4000 сессий и 25 VPN туннелей для NetScreen-25).

Мобильные пользователи

NetScreen-5XT, NetScreen-5XP и Netscreen-5GT Устройства являются устройствами начального уровня, но основаны на таких же технологиях межсетевых экранов, виртуальных частных сетей и управления трафиком, что и устройства верхнего ряда. Это дает возможность использовать данные устройства в удаленных офисах, магазинах и для удаленных пользователей, подключенных по высокоскоростному доступу. Модели выпускаются в двух версиях: версия на 10 пользователей и неограниченная по количеству пользователей Elite- версия. NetScreen-5XT имеет более высокую производительность, встроенный коммутатор на 4 порта 10/100, дополнительную память и резервный доступ по коммутируемой линии.

Программные продукты для мобильных пользователей: NetScreen-Remote VPN Client и NetScreen-Remote Security Client, - соответственно VPN клиент и VPN клиент с персональным межсетевым экраном.

Таблица 3.4. Основные характеристики VPN продуктов Juniper Networks

<table>
<tr><th>Продукт</th><th>Интерфейсы</th><th>Управление</th><th>Производительность</th><th>Протоколы туннелирования</th><th>Алгоритмы шифрования / Алгоритмы аутентификации</th></tr>
<tr><td>NetScreen-5400</td><td>24 Mini-GBIC или 6 Mini-GBIC + 72 10/100</td><td rowspan="15">WebUI (HTTP/ HTTPS-SSL); CLI (консоль, SSH или Telnet)</td><td>24/30G FW–1,000,000
15/12G AES VPN–25,000</td><td rowspan="15">IPSec, L2TP, L2TP-over-IPSec</td><td rowspan="15">3DES, DES и AES / SHA-1, MD5</td></tr>
<tr><td>NetScreen-5200</td><td>8 Mini-GBIC или 2 Mini-GBIC + 24 10/100</td><td>8/10G FW–1,000,000
4/5G AES VPN–25,000</td></tr>
<tr><td>NetScreen-500 Advanced</td><td rowspan="2">свыше 8 10/100 или 8 Mini-GBIC или 4 GBIC</td><td>700M FW–250,000
250M 3DES VPN–5,000+10000 Dial-Up</td></tr>
<tr><td>NetScreen-500 Baseline</td><td>700M FW–128,000
250M 3DES VPN–1,000</td></tr>
<tr><td>NetScreen-208 Advanced</td><td rowspan="2">8 10/100</td><td>550M FW–128,000
200M 3DES VPN–1,000</td></tr>
<tr><td>NetScreen-208 Baseline</td><td>550M FW–64,000
200M 3DES VPN–500</td></tr>
<tr><td>NetScreen-204 Advanced</td><td rowspan="2">4 10/100</td><td>400M FW–128,000
200M 3DES VPN–1,000</td></tr>
<tr><td>NetScreen-204 Baseline</td><td>400M FW–64,000
200M 3DES VPN–500</td></tr>
<tr><td>NetScreen-50 Advanced</td><td rowspan="2">4 10/100</td><td>170M FW–64,000
45M 3DES VPN–500</td></tr>
<tr><td>NetScreen-50 Baseline</td><td>170M FW–48,000
45M 3DES VPN–150</td></tr>
<tr><td>NetScreen-25 Advanced</td><td rowspan="2">4 10/100</td><td>100M FW–32,000
20M 3DES VPN–125</td></tr>
<tr><td>NetScreen-25</td><td>100M FW–24,000</td></tr>
</table>

Baseline			20M 3DES VPN–50		
NetScreen-5GTP/5GT	1 10/100 Untrust, 4 10/100 Trust		75M FW–2,000 20M 3DES VPN–10		
NetScreen-5XT/Elite	1 10/100 Untrust, 4 10/100 Trust		70M FW–2,000 20M 3DES VPN–10		

3.2.2. Решение компании Lucent Technologies(Lucent Secure VPN)

Lucent Technologies имеет в своем арсенале линию Lucent Secure VPN, продукты и системы управления которой образуют наиболее функциональную структуру для построения виртуальных частных сетей (ВЧС) для предприятий.

Решение компании Lucent Technologies представлено на рисунке 3.5.

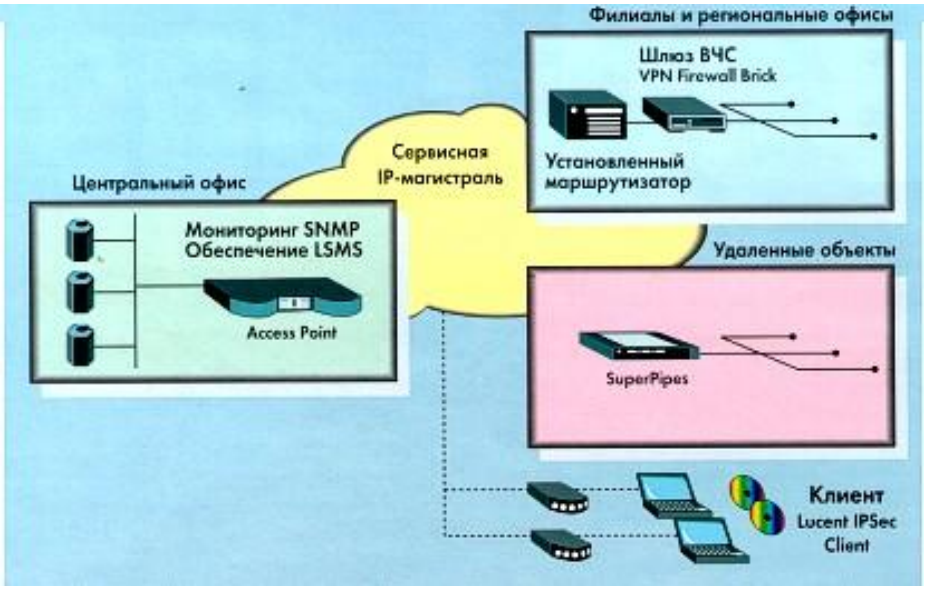

Рисунок 3.5. – Принципиальная схема построения VPN

Центральный офис

Фундаментом линии Lucent Secure VPN является интегрированная платформа централизованного управления правилами – сервер управления безопасностью LSMS (Lucent Security Management Server). Сервер LSMS взаимодействует с серверами аутентификации пользователей RADIUS и SecurID. Он также отвечает за обработку открытых ключей и цифровых сертификатов X.509. Сервер LSMS предусматривает широкие возможности аудита, регистрации и аварийной сигнализации (alarm). Усиление защиты достигается за счет Lucent RealSecure™, встроенной системы обнаружения атак. Сервер LSMS надежно зарекомендовал себя как средство централизованного обеспечения для предприятий, создающих крупномасштабные ВЧС удаленного доступа. Один сервер LSMS способен управлять сотнями шлюзов ВЧС и маршрутизаторов Pipeline и SuperPipe, тысячами клиентов IPSec Client – возможно одновременное управление 24000 туннелей ВЧС.

Приложение управления правилами Access Point QVPN Builder, работающее под управлением системы LSMS, специально оптимизировано для обеспечения параметров корпоративных ВЧС, связывающих отдельные объекты. Централизованное управление профилями ВЧС, правилами межсетевых экранов и правилами качества обслуживания QoS позволяет разворачивать ВЧС быстро и экономично. Реализованные Lucent функции конфигурирования ВЧС и управления правилами, основанные на интеграции LSMS и QVPN Builder, занимают лидирующие позиции в отрасли.

Другой класс оборудования, представленный в линии Lucent Secure VPN — это маршрутизаторы Access Point и Pipeline/SuperPipe. Их отличительная особенность — единая сервисная платформа, построенная с учетом требований производительности, масштабируемости, простоты управления и соотношения цены и производительности, в которой реализованы функции маршрутизации, управления полосой пропускания, ВЧС и межсетевого экрана.

Маршрутизаторы Access Point используются там, где требуются производительность и масштабируемость, достаточные для поддержки больших объемов трафика и тысяч туннелей ВЧС. Маршрутизаторы Access Point совместимы с любой технологией ГВС — IP, Frame Relay, ATM – и поддерживают как ВЧС, объединяющие отдельные объекты, так и ВЧС удаленного доступа. Встроенный аппаратный ускоритель шифрования обеспечивает скорость до 90 Мбит/с при шифровании DES и 3DES.

Применение в маршрутизаторе Access Point технологии CBQ (class-based queuing) выводит Lucent на первое место в обеспечении качества обслуживания IP (QoS). Технология CBQ предусматривает разделение трафика на иерархические классы, которым присваиваются атрибуты полосы пропускания, определяющие привилегии доступа на границе между сетью предприятия и ВЧС. Для оптимизации загрузки IP-сети можно создавать уровни обслуживания, обеспечивать их выполнение и тарифицировать. Маршрутизатор Access Point полностью совместим со стандартом DiffServ (сигнализация обеспечения QoS соответствует текущему определению IETF).

Филиалы и региональные офисы

Шлюзы Lucent VPN, стартовая цена которых составляет 2000 долл., — это экономичное решение, включающее надежный межсетевой экран и, в качестве опции, аппаратное шифрование данных. Управление шлюзами осуществляется централизованно и масштабируется для поддержки до тысяч программных клиентов IPSec Client, установленных на удаленных и мобильных компьютерах. Семейство шлюзов ВЧС Lucent VPN Firewall Brick насчитывает шесть устройств: Firewall Brick 20, Firewall Brick 80, Firewall Brick 350, Firewall Brick 500, Firewall Brick 1000 и Firewall Brick 1100. Все они, обладая общей функциональностью, отличаются по производительности и соответственно области применения и ценовым параметрам.

Основная отличительная черта шлюзов Lucent VPN – тесная интеграция с надежным межсетевым экраном, имеющим сертификаты ICSA и NSA, а также встроенные средства аутентификации и контроля доступа, использующие лучшие в своей категории решения на базе стандартов.

В шлюзах Lucent VPN используется собственная операционная система, в которой устранены недостатки защиты стандартных ОС. Активную защиту можно усилить с помощью интегрированных систем обнаружения атак и проверки безопасности.

Удалённые объекты

Маршрутизаторы ВЧС линии Pipeline предназначены для региональных офисов и удаленных сотрудников, для установки у клиентов или партнеров. Они характеризуются хорошим соотношением цены и качества, низкой стоимостью владения, а также масштабируемостью, которая позволяет использовать их в различных условиях – от домашних офисов с одним пользователем до региональных отделений практически любого масштаба.

Маршрутизаторы Pipeline и SuperPipe со встроенным межсетевым экраном обеспечивают доступ ГВС, маршрутизацию, туннелирование и шифрование по протоколу IPSec и аутентификацию. Централизованное автоматизированное управление правилами ВЧС с помощью сервера LSMS (включая одновременно правила IPSec и межсетевого экрана) снижает стоимость владения и упрощает внедрение на крупномасштабных объектах.

Таблица 3.5. Основные характеристики VPN продуктов Lucent Technologies

Продукт	Интерфейсы	Управление	Производи-тельность	Протоко-лы туннели-рования	Алго-ритмы шифро-вания / Алго-ритмы аутенти-фикации
Access Point 1500 (маршрутизатор)	ЛВС: 2x10/100 Ethernet, Gb Ethernet, ГВС: MSSI, HSSI, 4xE1 с интегрир. DSU, DS-3 с интегрир. DSU, ATM OC3/STM-1	консоль, Telnet, SSH; SCP; HTTP/HTTPS; поддержка SNMPv2, SNMPv3; 2xRS232; Access Point QVPN Builder; Navis	700M FW– 300 000; 155M 3DES VPN– 5000 IPSec удален. доступа, 1500 IP-IP, 3500	IPSec, L2TP, IP-IP, GRE, Mobile IP FA/HA	DES, 3DES, RC4 / MD5, SHA-1

		iOperations	L2TP		
Access Point 600 (маршрутизатор)	ЛВС: 10/100 Ethernet; ГВС: MSSI, HSSI, T1/E1, ISDN, ATM OC3/STM-1	SNMP, командный язык сценариев, web-управление; Access Point QVPN Builder; Navis iOperations	220M FW; 90M 3DES VPN–600 IPSec, 3500 удален.доступа	IPSec, L2TP, IP-IP, GRE	
Access Point 300 (маршрутизатор)	ЛВС: 2x10/100 Ethernet; ГВС: MSSI или 2xT1/E1, ISDN S/T или ISDN U	SNMP, пакетные командные файлы, web-сервер; Access Point QVPN Builder; Navis iOperations	50M FW; 5M 3DES VPN–1500 IP-IP, 500 IPSec удален.доступа	IPSec, L2TP, IP-IP, GRE	
SuperPipe 175 (маршрутизатор)	ЛВС: 10/100 Ethernet; ГВС: E1, V.35/X.21, ADSL-DMT	NavisConnect, NavisAccess; SNMP(MIB); SecureConnect Manager и Lucent Security Management Server		IPSec	DES, 3DES, RC4 / MD5, SHA-1
SuperPipe 170 (маршрутизатор)	ЛВС: 10/100 Ethernet; ГВС: ADSL-DMT	NavisConnect, NavisAccess; SNMP(MIB); SecureConnect Manager и Lucent Security Management Server			
Superpipe 155 (мульти-сервисный маршрутиза-тор доступа)	ЛВС: 10/100 Ethernet; ГВС: 2 ISDN U BRI, E1; ISDN S/T	NavisConnect, SNMP(MIB II), Telnet, NavisAccess			
SuperPipe 95 (мульти-сервисный маршрутиза-тор доступа)	ЛВС: 10/100 Ethernet; ГВС: 2 BRI S/T	NavisConnect, SNMP(MIB II), Telnet; NavisAccess			
Firewall Brick 1100 (аппаратный МЭ)	7 10/100 Ethernet 4 Gigabit Ethernet	LSMS	3G FW–4 000 000; 1G 3DES VPN–7150	IPSec	DES, 3DES, RC4 / MD5, SHA-1
Firewall Brick 1000 (аппаратный МЭ)	9 10/100 Ethernet 4 Gigabit Ethernet		1,5G FW–3 000 000; 1G 3DES VPN–7150		
Firewall Brick 500 (аппаратный МЭ)	14 10/100 Ethernet 1 Gigabit Ethernet		975M FW–600 000; 450M 3DES VPN–8000		
Firewall Brick 350 (аппаратный МЭ)	7 10/100 Ethernet 1 Gigabit Ethernet		650M FW–1 000 000; 400M 3DES VPN–5400		
Firewall Brick 80 (аппаратный МЭ)	4 10/100 Ethernet		190M FW–30 000; 11M 3DES VPN–200		
Firewall Brick 20 (аппаратный МЭ)	3 10/100 Ethernet		140M FW–3 000; 3M 3DES VPN–55		

3.2.3. Решение компании Cisco Systems

Решение компании Cisco Systems представлено на рисунке 3.6.

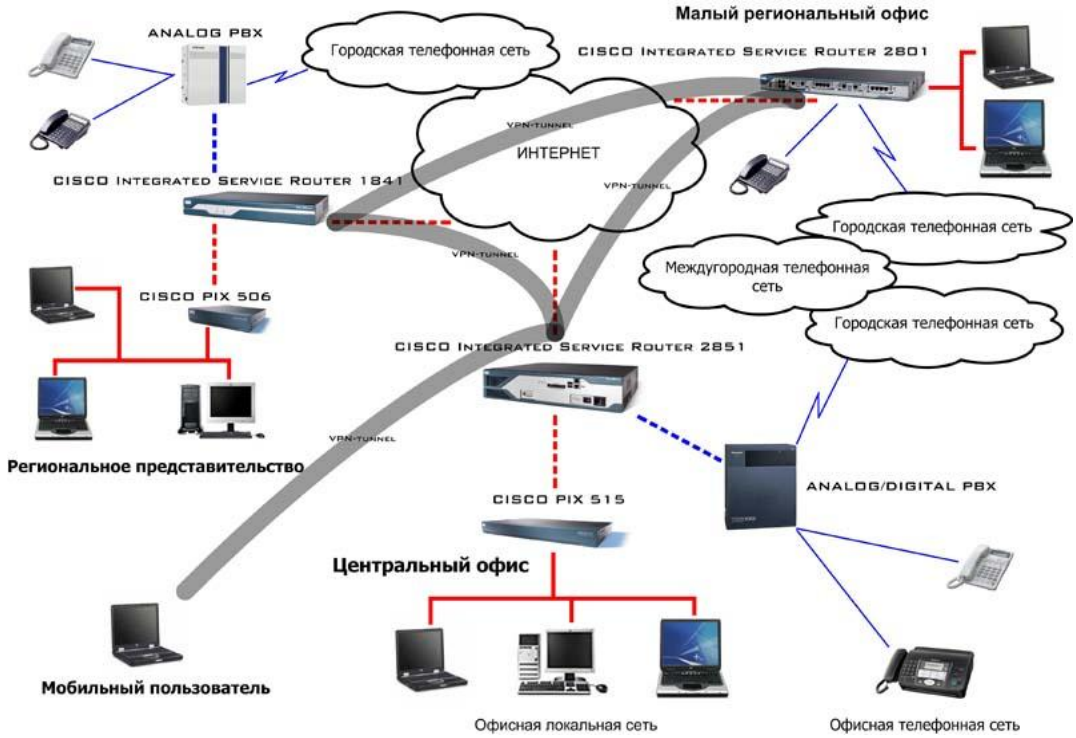

Рисунок 3.6. Организация VPN на оборудовании Cisco

Серия Cisco 1800, представленная маршрутизатором Cisco 1841, разработана для обеспечения потребностей небольших офисов и организаций в безопасном доступе к корпоративным сетям и сети Интернет. Cisco 1841 имеет встроенные средства аппаратного ускорения шифрования трафика, возможность дальнейшего увеличения производительности шифрования путём установки опционального модуля VPN; функциональность системы предотвращения вторжений (IPS) и межсетевого экрана; широкий спектра интерфейсных модулей, а так же запас производительности для дальнейшего расширения сети и внедрения будущих приложений.

Серия Cisco 2800 представляет собой маршрутизаторы с интеграцией сервисов(ISR), оптимизированные для безопасной передачи данных, голоса и видео на скорости канала связи. Серия Cisco 2800 отличается гибкой модульной конструкцией. Маршрутизаторы имеют интегрированные средства аппаратного ускорения шифрования, обеспечивают функциональность системы обнаружения вторжений и межсетевого экрана. Маршрутизатор обеспечивает обработку и управление телефонными соединениями, функциональность голосовой почты и другие сервисы. Большое количество различных типов интерфейсов и запас производительности создают основу для дальнейшего расширения сети и внедрения будущих приложений.

Таблица 3.6. Основные характеристики VPN продуктов Cisco

Продукт	Интерфейсы	Управление	Производи-тельность	Протоко-лы туннели-рования	Алго-ритмы шифро-вания / Алго-ритмы аутенти-фикации
Cisco ISR 2851	2 10/100/1000T; 1 порт AUX; 1 порт USB1.1	Командная строка, консоль, telnet		IPSec	DES, 3DES, AES-128, AES-192, AES-256 /
Cisco ISR 2801	2 10/100TX; 1 порт AUX; 1 порт USB1.1			IPSec	
Cisco ISR	2 10/100TX;			IPSec	

1841	1 порт AUX; 1 порт USB1.1; гнездо расширения AIM				MD5, SHA-1
Cisco Pix 515E	до 6 10/100 Ethernet; 8 VLAN 802.1g	SNMP; ПО PIX Device Manager, Cisco Secure Policy Manager	190M FW–176 000; 135M 3DES VPN–2000, 130M AES-128 VPN–2000	IPSec	3DES, AES-128 / MD5, SHA-1
Cisco Pix 506E	2 10/100 Ethernet		100M FW–53 000; 16M 3DES VPN–25, 30M AES-128 VPN–25	IPSec	

4. Характеристики услуги VPN

Качество услуги VPN нельзя определить в отрыве от качества обслуживания сетей доступа и транспортных сетей, используемых для оказания услуги VPN. В таблице 4.1 показана взаимосвязь параметров качества услуги VPN с характеристиками транспортной сети и сети доступа.

Таблица 4.1 Параметры качества услуги VPN

Параметры качества услуги VPN	Параметры качества узла телематической (ТМ) службы	Параметры качества сети доступа	Параметры качества транспортной сети
Параметры доступности услуги	Вероятность отказа сервера	Доля потерь вызовов	Коэффициент загрузки исходящих каналов узла ТМ службы
	Вероятность отказа на модемном пуле	Время установления соединения	
Параметры качества передачи	Вероятность потерь пакетов в узле ТМ службы	Время установления соединения	Вероятность потерь пакетов
	Задержка пакета на обработку в узле ТМ службы		Задержка пакета
			Вариация задержки пакета
	Надежность узла	Надежность соединения	Надежность соединения
	Безопасность	Безопасность	Безопасность

Для услуги VPN важными являются характеристики надежности и безопасности. Далее будем рассматривать только эти две характеристики услуги: надежность и безопасность. *Надежность* услуги выражается вероятностью исправного состояния соединения (коэффициентом готовности) или средним временем наработки системы на отказ. Надежность услуги обеспечивается надежностью элементов соединения, резервированием и ремонтом (восстановлением) элементов соединения. Под безопасностью системы понимается способность системы функционировать, не переходя в опасное состояние, в котором возникает ущерб большого масштаба. *Безопасность* услуги может выражаться как вероятностью возникновения ущерба, так и математическим ожиданием этого ущерба. Безопасность услуги обеспечивается защитными мерами (преградами).

Прежде чем оценивать надежность и безопасность услуги VPN, установим соотношение между понятиями надежности и безопасности.

1. Надежность системы выражается вероятностью исправного состояния системы. Безопасность системы выражается вероятностью опасного состояния системы.

2. В надежности исходным термином является *неисправность* (*отказ, дефект*), а в безопасности исходным термином является *опасное состояние* (*коллапс, вред*). *Отказ* – это событие, после возникновения которого система теряет свою работоспособность. *Опасное состояние* – это состояние, при котором возникает ущерб.
3. Модели надежности, как правило, учитывают элементы и состав системы, различные связи между ними и режимы работы системы. В моделях безопасности на первый план выходят не учитываемые в теории надежности компоненты: защитные средства, неблагоприятные внешние воздействия, умышленные действия людей.
4. Исходными данными для моделей надежности являются наблюдения в реальных условиях эксплуатации за такими событиями как отказы и восстановления элементов системы. Исходными данными для моделей безопасности являются наблюдения в реальных условиях эксплуатации за инициирующими событиями (например, атаками на систему), которые приводят к опасному состоянию. Так как наблюдаемые события являются редкими, то возникают трудности со статистической обработкой событий из-за малого объема информации. В связи с невозможностью экспериментов для оценки безопасности единственным выходом является проигрывание на модели возможных вариантов развития инициирующего события, *сценариев перехода системы в опасное состояние.*
5. При оценке безопасности необходимо знать *множество опасных состояний* и *логику их возникновения*. Поэтому специалист по безопасности должен уметь составлять сценарий перехода системы в опасное состояние, т.е. грамотно думать, как проще привести систему в опасное состояние, в отличие от специалиста по надежности, думающего о сохранении ее работоспособности.

5. Оценка надёжности услуги VPN

Модель надежности услуги VPN с точки зрения пользователей показана на рис.5.1. Модель надежности услуги VPN представлена в виде системы с последовательным в смысле надежности соединением блоков.

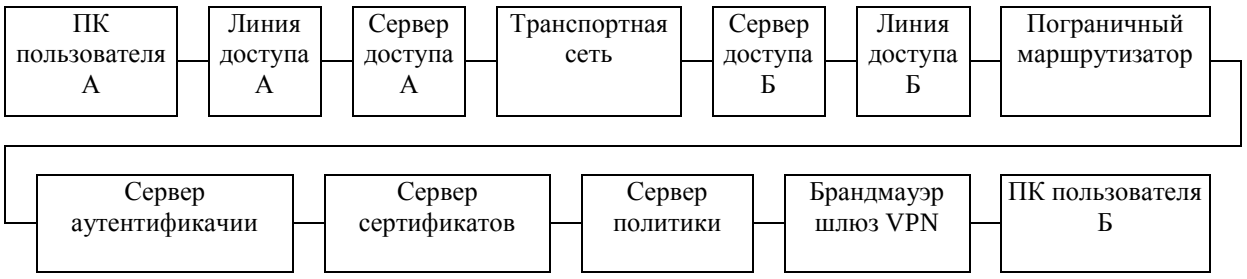

Рис. 5.1 Модель надежности услуги VPN

Надежность услуги (как и надежность любой системы) оценивается коэффициентом готовности услуги. Коэффициент готовности услуги VPN равен

$$К_Г = К^2_{ПК} \cdot К^2_{ЛД} \cdot К^2_{СД} \cdot К_{ТС} \cdot К_{ПМ} \cdot К^3_{СЕРВ} \cdot К_{МЭ}, \qquad (5.1)$$

где $К_{ПК}$ – коэффициент готовности ПК пользователя,
$К_{ЛД}$– коэффициент готовности абонентской линии,
$К_{СД}$– коэффициент готовности сервера доступа,
$К_{ТС}$– коэффициент готовности транспортной сети,
$К_{ПМ}$– коэффициент готовности пограничного маршрутизатора сети,
$К_{СЕРВ}$– коэффициент готовности сервера аутентификации, сервера сертификатов и сервера политики,
$К_{МЭ}$– коэффициент готовности брандмауэра (межсетевого экрана).

Модель надежности сервера доступа в общем случае описывается дублируемой системой с различными типами резерва (нагруженный, ненагруженный, облегченный резерв). Модель надежности сервера доступа показана на рис.5.2. Основной и резервный блоки состоят из двух элементов: технические средства сервера и программные средства сервера.

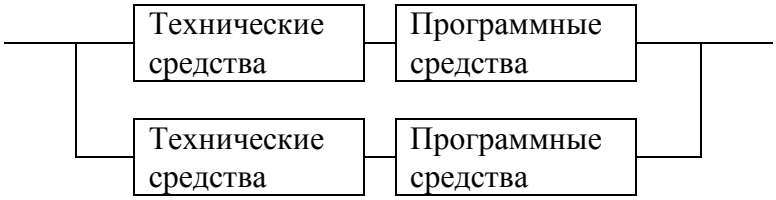

Рис. 5.2 Модель надежности сервера доступа

При последовательном соединении элементов системы в смысле надежности коэффициент готовности системы и интенсивность отказов системы равны

$$K_{\Gamma} = \prod_{i=1}^{n} K_{gi}\,,\ \lambda_c = \sum_{i=1}^{n} \lambda_i\,, \qquad (5.2)$$

где K_{gi} – коэффициент готовности элемента i, $K_{gi} = \dfrac{\mu_i}{\mu_i + \lambda_i}$,

λ_i – интенсивность отказов элемента i,

μ_i – интенсивность восстановления элемента i,

n – число элементов системы.

При параллельном соединении элементов системы в смысле надежности коэффициент простоя системы и интенсивности восстановлений системы равны

$$K_{\Pi} = \prod_{i=1}^{n} K_{pi}\,,\ \mu_c = \sum_{i=1}^{n} \mu_i\,,$$

где K_{pi} – коэффициент простоя элемента i.

Дублируемая система с нагруженным резервом из одного рабочего и одного резервного элемента в нагруженном резерве имеет коэффициент готовности

$$K_{\Gamma} = \frac{\mu^2 + 2\lambda\mu}{\mu^2 + 2\lambda\mu + 2\lambda^2}\,, \qquad (5.3)$$

где λ, μ – интенсивность отказов и восстановлений элемента системы.

В дублируемой системе с ненагруженным резервом элемент, находящийся в состоянии ненагруженного резерва, не может отказать. Коэффициент готовности системы равен

$$K_{\Gamma} = \frac{\lambda\mu + \mu^2}{\mu^2 + \mu\lambda + \lambda^2}\,. \qquad (5.4)$$

В системе с облегченным резервом резервный элемент может отказать, но интенсивность отказов резервного элемента (λ_2) меньше интенсивности отказов работающего элемента (λ_1). Коэффициент готовности системы равен

$$K_{\Gamma} = \frac{\mu^2 + \lambda_1 + \lambda_2 \ \mu}{\mu^2 + \lambda_1 + \lambda_2 \quad \lambda_1 + \mu}. \qquad (5.5)$$

Модель надежности ПК пользователя описывается нерезервируемой системой с двумя последовательно соединенными элементами, аппаратные средства ПК, программное обеспечение ПК. Модель надежности ПК показана на рис.5.3. ПК пользователя является менее надежным блоком, чем остальные блоки модели надежности услуги. Работоспособность ПК зависит не только от состояния аппаратуры и программного обеспечения, но и от антивирусной защиты и квалификации пользователя.

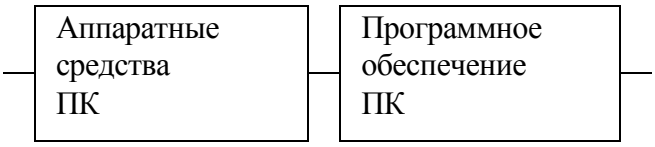

Рис.5.3 Модель надежности ПК пользователя.

Для определения коэффициента готовности ПК пользователя используются формулы

$$K_{\Gamma} = \frac{\mu}{\mu + \lambda} \qquad (5.6)$$

где λ - интенсивность отказов,

μ - интенсивность восстановлений.

$$\lambda = \frac{1}{m_t} \quad \mu = \frac{1}{m_\tau} \qquad (5.7)$$

где m_t, - среднее время жизни элемента,

m_τ - среднее время восстановления элемента.

Так как ПК – последовательная в смысле надежности система, то коэффициент готовности всей системы равен произведению коэффициентов готовности элементов, входящих в нее

$$К_{ПК} = К_{ГПС} \cdot К_{ГТС} \qquad (5.8)$$

Модель надежности линии доступа пользователя зависит от сети доступа, и в общем случае представляет собой сложную систему. Мы не будем рассматривать элементы сложной системы сети доступа, ограничимся простейшим случаем. Представим модель надежности линии пользователя в виде нерезервируемой системы с конечным временем восстановления (рис.5.4).

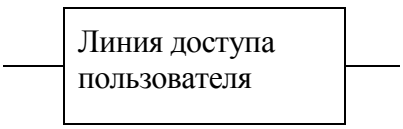

Рис.5.4. Модель надежности линии доступа пользователя.

Для определения коэффициента готовности линии пользователя используется формула (5.6)

Модель надежности транспортной сети описывается сложной системой. Будем полагать, что в транспортной сети нет маршрутов по умолчанию, и используется динамическая маршрутизация. Будем полагать, что транспортная сеть представляет автономную систему, для которой известна статистика отказов и восстановлений. Примем упрощенную модель надежности транспортной сети как нерезервируемой системы с конечным временем восстановления. Модель надежности транспортной сети показана на рис.5.5.

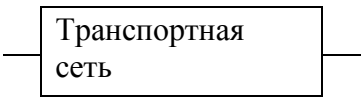

Рис.5.5. Модель надежности транспортной сети

Коэффициент готовности рассчитывается по формуле (5.6).
Модель надежности пограничного маршрутизатора сети описывается нерезервируемой системой с конечным временем восстановления. Модель надежности транспортной сети показана на рис.5.6.

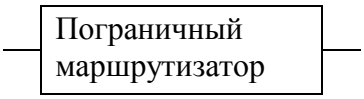

Рис.5.6. Модель надежности пограничного маршрутизатора
Модель надежности серверов, сертификатов аутентификации и политики описывается нерезервируемой системой с двумя последовательно соединенными элементами: аппаратные средства и программное обеспечение.

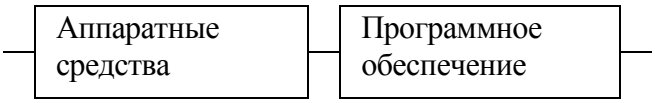

Рис.5.7 Модель надежности серверов, сертификатов аутентификации и политики.
Модель надежности межсетевого экрана, являющегося также шлюзом VPN, описывается нерезервируемой системой с двумя последовательно соединенными элементами: аппаратные средства и программное обеспечение.

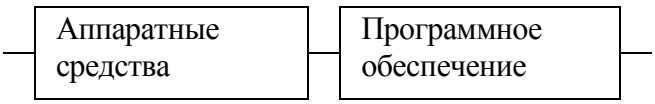

Рис.5.8 Модель надежности межсетевого экрана.

6. Оценка безопасности услуги VPN

В сетевой безопасности используются следующие термины.
Уязвимость (vulnerability) системы – это любая характеристика системы, использование которой нарушителем может привести к реализации угрозы.
Угрозой (threat) системы называют потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам системы.
Атакой (attack) на систему называют действие или действие последовательно связанных между собой действий нарушителя, которые приводят к реализации угрозы путем использования уязвимостей этой системы.
Результатом атаки могут быть:
- расширение прав доступа,
- искажение информации,
- раскрытие информации,
- кража сервисов,
- отказ в обслуживании.

Риск (risk) – возможность проведения захватчиком успешной атаки в отношении конкретной слабой стороны системы.

Оценка риска (risk assessment) – количественная оценка повреждения, которое может произойти. Таким образом, оценка риска – это *количественная мера опасности*. Любой риск представляет собой многокритериальную величину и не может оцениваться по одной компоненте. Этим объясняется многообразие подходов и методов оценки риска.
Для оценки риска используются экспертные, экономические, вероятностные модели и их комбинации. *Экспертные* модели оценивают уровень серьезности последствий атак по некоторой шкале. *Экономические модели* оценивают финансовые потери. *Вероятностные модели* оценивают вероятность успешной атаки.

Экспертная модель
Уровень серьезности последствий оценивается с точки зрения владельца системы по некоторой шкале. Концепция оценки серьезности последствий представлена на рис.6.1.

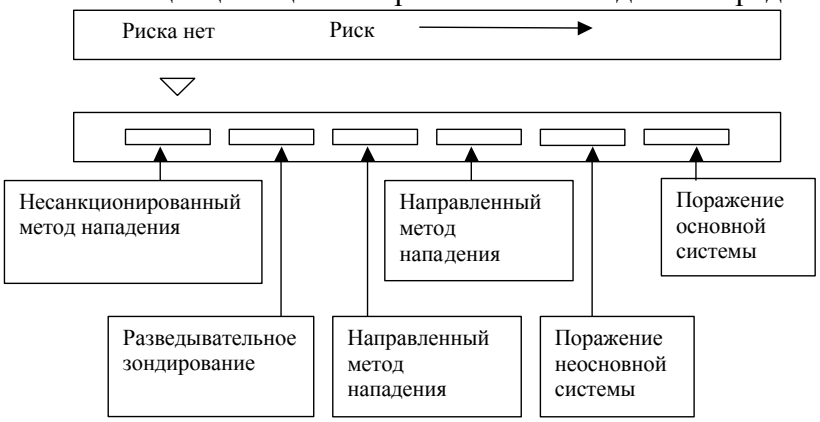

Рис.6.1. Общие представления об уровне серьёзности последствий
Для оценки условия серьезности последствий используется формула:

$$\langle уровень\ \ серьёзност и\rangle = (\langle важность\ \ цели\rangle + \langle вредность\ \ атаки\rangle) - (\langle системные\ \ контрмеры\rangle + \langle сетевые\ \ контрмеры\rangle) \quad (6.1)$$

Параметры формулы (1) оцениваются по пятибалльной шкале.
Таблица 6.1. Экспертные оценки параметров.

Оценка	Важность цели	Вредность атаки	Контролеры системы	Контролеры сети
5 баллов	Брандмауэр, сервер DNS, основной маршрутизатор	Получен корневой доступ к сети	Современная операционная система, дополнительная защита типа TCP Wrappers и Secure Shell	Ограничительный брандмауэр, работающий в одну сторону
4 балла	Ретранслятор, средство обмена электронной почтой	Отказ в обслуживании		Ограничительные брандмауэры с внешними соединениями (модемами)
3 балла		Пользовательский доступ через узнанный пароль	Старая операционная система	
2 балла	Пользовательская настольная система UNIX			Разрешительный брандмауэр
1 балл	MS-DOS 3.11		Нет TCP Wrappers, разрешены фиксированные нешифрованные пароли	

Экономическая модель
Экономическая модель позволяет оценить стоимость ущерба от атаки.

Стоимость потерь от снижения производительности сотрудников атакованного узла или сегмента равна

$$П_П = \frac{\sum Z_C}{\frac{N_C}{192}} \cdot t_П, \qquad (6.2)$$

где $t_П$ - время простоя вследствие атаки, час

Z_C - зарплата сотрудников атакованного узла, доллары за месяц ($/месяц)

N_C - число сотрудников атакованного узла.

Стоимость восстановления работоспособности атакованного узла или сегмента

$$П_В = П_{ВИ} + П_{ПВ} + П_{ЗЧ} \qquad (6.3)$$

где $П_{ВИ}$ - стоимость повторного ввода информации

$П_{ПВ}$ - стоимость восстановления узла (переустановка системы, конфигурирование и т.д.)

$П_{ЗЧ}$ - стоимость замены оборудования или запасных частей.

$$П_{ВИ} = \frac{\sum Z_C}{\frac{N_C}{192}} \cdot t_{ВИ}, \qquad (6.4)$$

$$П_{ПВ} = \frac{\sum Z_0}{\frac{N_0}{192}} \cdot t_В, \qquad (6.5)$$

где $t_{ВИ}$ - время повторного ввода потерянной информации, час

Z_0 - зарплата обслуживающего персонала (администраторов)

$t_В$ - время восстановления после атаки, час

N_0 - число обслуживающего персонала.

Упущенная выгода от простоя атакованного узла или сегмента

$$U = П_П + П_В + V, \qquad (6.6)$$

$$V = \frac{O}{52 \cdot 5 \cdot 8} \cdot (t_П + t_В + t_{ВИ}), \qquad (6.7)$$

где O – объём продаж атакованного узла или сегмента (в долларах США за год)

Общий ущерб от атаки равен

$$O_y = \sum_n \sum_I U, \qquad (6.8)$$

где I – число атакованных узлов,

n – число атак в год.

Вероятностная модель

Вероятностная модель позволяет оценить вероятность успешной атаки. Оценим вероятность успешной атаки для услуги виртуальной частной сети (Virtual Private Networks, VPN). Структурная модель риска VPN показана на рис.6.2.

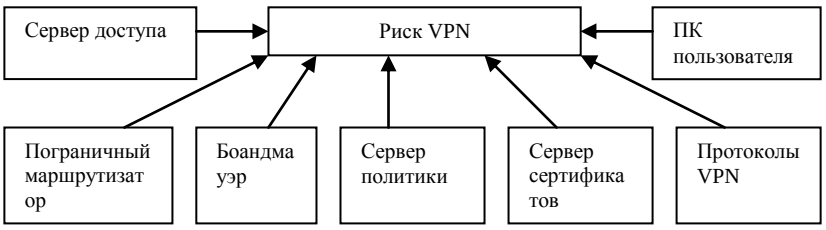

Рис.6.2. Структурная модель риска VPN.

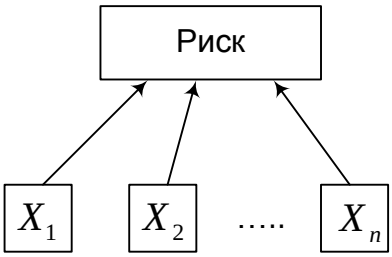

Рис.6.3. Модель риска типа «узла». $X_i, i = \overline{1,n}$ - объекты риска.

Структурная модель риска VPN относится к моделям типа «узла». Объектами риска ($X_i, i = \overline{1,n}$) является ПК, сервер доступа, брандмауэр, сервер политики, сервер сертификатов. Злоумышленник получает доступ к ресурсам объекта, если успешно преодолевает последовательность преград. С каждым объектом риска связан свой набор преград ($X_{ir}, r = \overline{1,N_i}$).

В таблице 6.2 приведены преграды для защиты от несанкционированного доступа и отображены характеристики преград и среднее время их возможного преодоления подготовленным нарушителем. Таким образом, таблица 6.2 отражает сценарий перехода системы VPN в опасное состояние. Таблица 6.2 может быть дополнена. Кроме того, для каждого объекта риска должна быть разработана своя таблица. Однако мы будем пользоваться таблицей 6.2 для всех серверов VPN. Подчеркнем лишь важность составления сценариев перехода системы в опасное состояние.

Т а б л и ц а 6.2. Преграды для защиты от несанкционированного доступа к серверу.

Преграда	Частота смены значений параметров преграды	Среднее время преодоления преграды нарушителем	Возможный способ преодоления преграды
1. Охраняемая территория со сменой охраны	Через 2 часа	30 мин.	Скрытое проникновение на территорию
2. Пропускная система в здании	Через сутки	10 мин.	Подделка документов, сговор, обман
3. Электронный ключ для включения компьютера	Через 5 лет (наработка до замены)	1 неделя	Кража, сговор
4. Пароль для входа в систему	Через 1 месяц	1 месяц	Подсматривание, сговор, подбор
5. Пароль для доступа к программным устройствам	Через 1 месяц	10 суток	Подсматривание, сговор, подбор
6. Пароль для доступа к требуемой информации в БД	Через 1 месяц	10 суток	Подсматривание, сговор, подбор
7. шифрование информации со сменой ключей	Через 1 месяц	2 года	Расшифровка, сговор

Вероятность успешной атаки равна

$$P_{\text{ðèñê}} = 1 - P_{\text{ÏÊ}}^2 \cdot P_{\text{ÑÄ}}^2 \cdot P_{\text{ÑÍ}} \cdot P_{\text{ÑÑ}} \cdot P_{\text{ÏÌ}} \cdot P_{\text{ÌÝ}} \cdot P_{\text{Ï}}, \qquad (6.9)$$

где $P_{ПК}$ - вероятность сохранения защищенности ПК,

$P_{СД}$ - вероятность сохранения защищенности сервера доступа,

$P_{СП}$ - вероятность сохранения защищенности сервера политики,

$P_{СС}$ - вероятность сохранения защищенности сервера сертификатов,

$P_{ПМ}$ - вероятность сохранения защищенности пограничного маршрутизатора,

$P_{МЭ}$ - вероятность сохранения защищенности брандмауэра,

P_{i} - вероятность защищенности от атак протоколов VPN.

Вероятность сохранения защищенности $P_i^{защ}$ объекта риска X_i услуги VPN равна

$$P_i^{защ} = 1 - \prod_{r=1}^{N_i} P_{ir}, \qquad (6.10)$$

где N_i - количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к i-объекту риска,

P_{ir} - вероятность преодоления нарушителем r-ой преграды i-объекта риска.

Вероятности преодоления преград определяются по статистическим данным анализаторами атак или комплексами обнаружения и защиты от атак.

Основными угрозами ПК пользователя являются вирусные угрозы.

Для случайных вирусных угроз сравнительно редкое использование профилактической диагностики незначительно ухудшает вероятностно-временные характеристики системы. Вероятность безопасного функционирования при диагностике 2 раза в неделю составит 0.77 - 0.90, а при диагностике 1 раз в сутки она повышается до 0.90 - 0.96.

Для опасных вирусных угроз профилактическая диагностика 1 раз в сутки не позволит обеспечить безопасность функционирования свыше 0.76, а с частотой 2 раза в сутки строго периодическая диагностика обеспечит безопасность с вероятностью не ниже 0.90.

Безопасность передачи по VPN обеспечивается протоколами VPN. При оценивании безопасности услуги VPN будем полагать, что протоколы VPN обеспечивают защиту от всех атак на протоколы и гарантируют защищенную передачу данных по открытой сети, $P_{i} = 1$.

7. Криптографические протоколы

7.1 Классификация криптографических протоколов

Протоколом называется последовательность действий, исполняемых двумя или более сторонами, спроектированная для решения какой-либо задачи.

Криптографическим протоколом называется протокол, в котором используются криптографические методы или шифры.

В криптографических протоколах используются стандарты шифрования, представленные на рис 7.1.

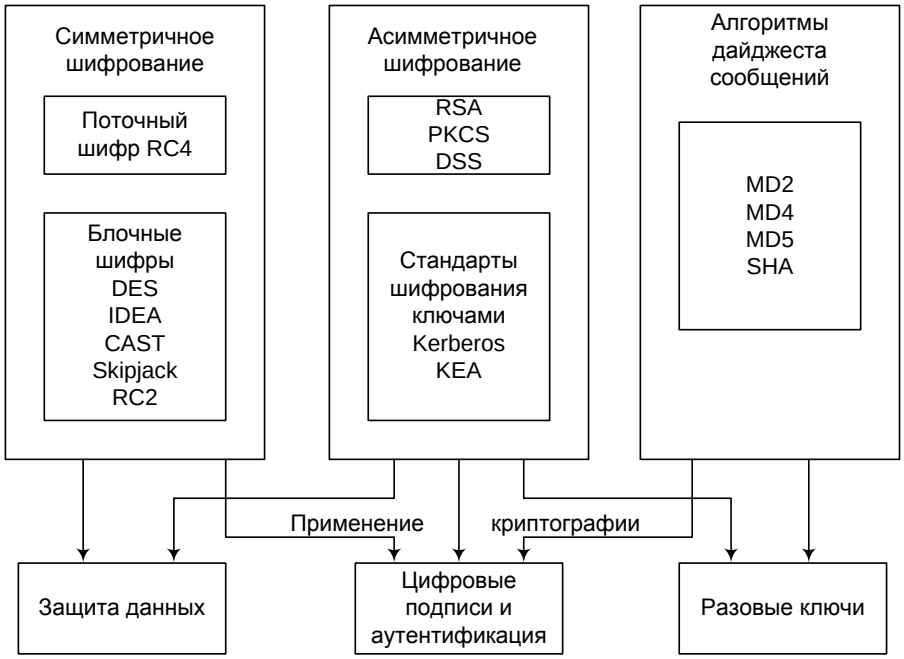

Рис.7.1. Криптографические методы и шифры.

Классификация криптографических протоколов представлена на рис 7.2.

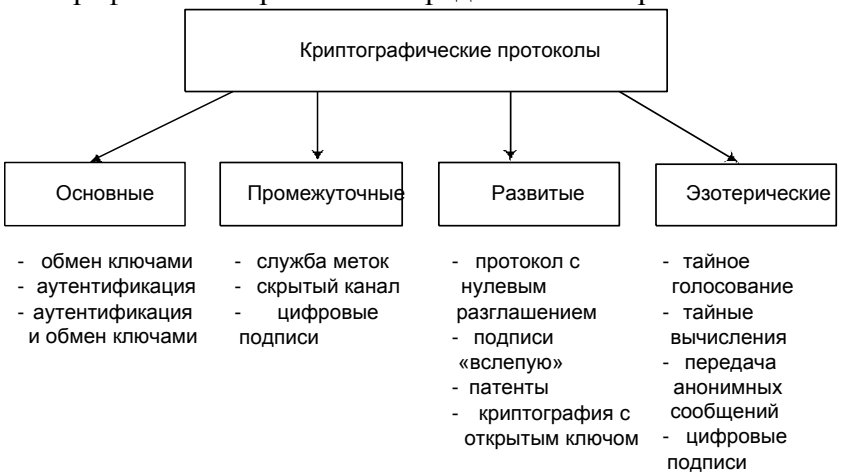

Рис.7.2. Криптографические протоколы.

На рис 7.3 показаны основные типы протоколов.

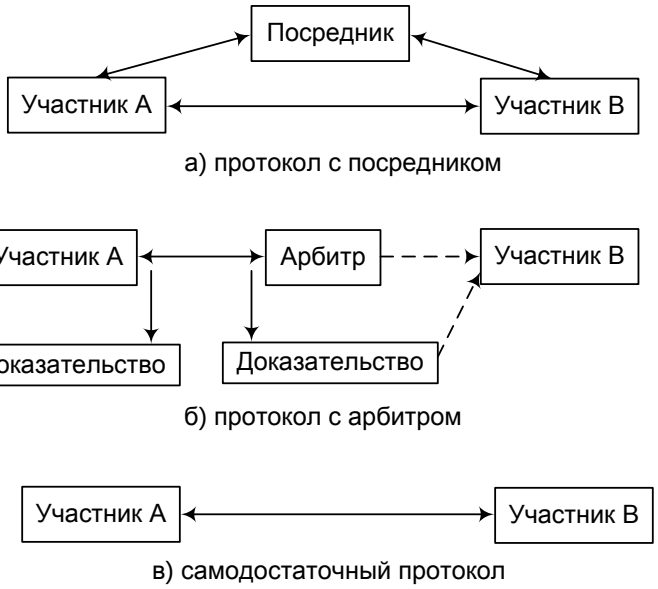

Рис.7.3. Типы протоколов.

На рис 7.4 показаны протоколы сетевой защиты.

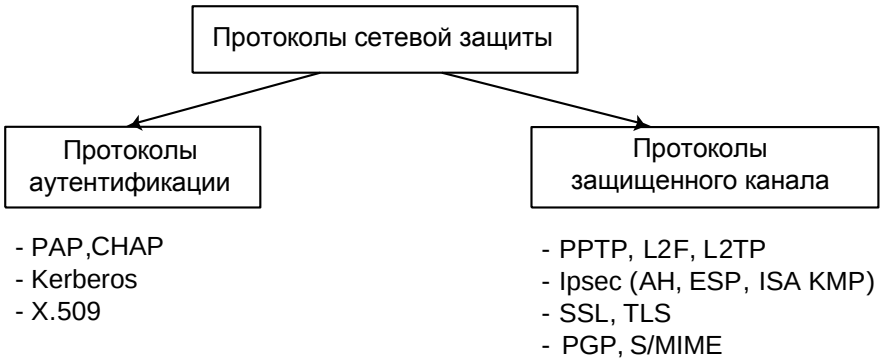

Рис.7.4. Протоколы сетевой защиты.

В протоколах защищенного канала канального и сетевого уровней используется туннелирование. *Туннелирование* – это процесс инкапсуляции одного типа пакета внутри другого с целью получения некоторого преимущества при его транспортировке.В туннельном режиме протокола ESP (IPsec) шифруется весь исходный IP-пакет, что исключает возможность атак, построенных на анализе трафика.

В транспортном режиме ESP(IPSec) шифрует только содержимое IP-пакета, что обеспечивает конфиденциальность, но не исключает анализ трафика пересылаемых пакетов.

Для описания протоколов примем обозначения:

A, B - участники протокола,

K_S - сеансовый ключ,

$K_A(K_B)$ - ключ $A(B)$, совместный с посредником,

$KU_A(KU_B)$ - открытый ключ $A(B)$,

$KR_A(KR_B)$ - закрытый ключ $A(B)$,

$E_K(\bullet)$ - шифрование,

$D_K(\bullet)$ - дешифрование,

$H(\bullet)$ - хэш-функция,

$C_K(\bullet)$ - код аутентичности,

$R_A(R_B)$ - случайное число (оказия), сгенерированное $A(B)$,

S - секретное слово,

T - метка даты/времени,

M - сообщение.

В таблицах 7.1-7.5 приведены элементы криптографических протоколов.

Таблица 7.1. Шифрование сообщений.

Традиционное шифрование	
$A \to B : E_K(M)$	• обеспечивает конфиденциальность (только A и B знают ключ K) • обеспечивает определенный уровень аутентификации (источником может быть только A) • не обеспечивает подпись (B может фальсифицировать получение сообщения, A имеет возможность отрицать отправку сообщения)
Шифрование с открытым ключом	
$A \to B : E_{KU_b}(M)$	• обеспечивает конфиденциальность (только B имеет ключ KR_b) • не обеспечивает аутентификацию (кто угодно может использовать ключ KU_b)
$A \to B : E_{KR_a}(M)$	• обеспечивает аутентификацию и подпись (только A имеет ключ KR_a, кто угодно может использовать KU_a, чтобы проверить подпись)

Таблица 7.2. Использование кодов аутентичности.

$A \to B : M \,\|\| C_K(M)$	• обеспечивает аутентификацию
$A \to B : E_{K_2}[M] \,\|\| C_{K_1}(M)$	• обеспечивает аутентификацию (только A и B знают K_1) • обеспечивает конфиденциальность (только Aи B знают K_2)
$A \to B : E_{K_2}[M] \,\|\| C_{K_1}(E_{K_2}(M))$	• обеспечивает аутентификацию • обеспечивает конфиденциальность

Таблица 7.3. Использование функций хэширования.

$A \to B : E_K[M \,\|\| H(M)]$	• обеспечивает конфиденциальность (только A и B знают K) • обеспечивает аутентификацию ($H(M)$ криптографически защищено)

$A \to B : M \,\|\| E_{KR_a}[H(M)]$	• обеспечивает аутентификацию и цифровую подпись ($H(M)$

	криптографически защищено, только A может создать $E_{KR_a}[H(M)]$)
$A \rightarrow B: E_K[M \parallel E_{KR_a}[H(M)]]$	• обеспечивает аутентификацию и цифровую подпись • обеспечивает конфиденциальность (только A и B знают K)
$A \rightarrow B: M \parallel H(M \parallel S)$	• обеспечивает аутентификацию (только A и B знают S)
$A \rightarrow B: E_K[M \parallel H(M) \parallel S]$	• обеспечивает аутентификацию (только A и B знают S) • обеспечивает конфиденциальность (только A и B знают K)

Таблица 7.4. Использование запросов/ответов.

$A \rightarrow B: R_a$ $B \rightarrow A: E_K(R_a)$	R_a обозначает оказию, сгенерированную стороной A. Ключ K совместно используется A и B. $f(\bullet)$ - функция типа приращения. Запросы/ответы используются для предотвращения воспроизведения сообщений.
$A \rightarrow B: E_K(R_a)$ $B \rightarrow A: R_a$	
$A \rightarrow B: E_K(R_a)$ $B \rightarrow A: E_K[f(R_a)]$	

Таблица 7.5. Использование арбитражной цифровой подписи.

Традиционное шифрование, арбитр может видеть сообщение
$X \rightarrow A: M \parallel E_{K_{XA}}[ID_X \parallel H(M)]$ $A \rightarrow Y: E_{K_{AY}}[ID_X \parallel M \parallel E_{K_{XA}}[ID_X \parallel H(M) \parallel T]$
Традиционное шифрование, арбитр не видит сообщения
$X \rightarrow A: ID_X \parallel E_{K_{XY}}[M] \parallel E_{K_{XA}}[ID_X \parallel H(E_{K_{XY}}[M])]$ $A \rightarrow Y: E_{K_{AY}}[ID_x \parallel E_{K_{XY}}[M] \parallel E_{K_{XA}}[ID_X \parallel H(E_{K_{XY}}[M])] \parallel T]$
Шифрование с открытым ключом, арбитр не видит сообщения
$X \rightarrow A: ID_X \parallel E_{KR_X}[ID_X \parallel E_{KU_Y}(E_{KR_X}[M])]$ $A \rightarrow Y: E_{KR_A}[ID_X \parallel E_{KU_Y}(E_{KR_X}[M]) \parallel T]$
В таблице приняты обозначения: X - отправитель,

Y - получатель, A - арбитр, M - сообщение

Используя обозначения, приведем примеры протоколов.

Пример 1. Протокол распределения сеансовых ключей с помощью центра распределения ключей (ЦРК).

1. $A \to \ddot{O}\text{Đ}\hat{E} : A \| B \| R_A$
2. $\ddot{O}\text{Đ}\hat{E} \to A : E_{K_A}(K_S \| B \| R_A \| E_{K_B}(K_S \| A))$
3. $A \to B : E_{K_B}(K_S \| A)$
4. $B \to A : E_{K_S}(R_B)$
5. $A \to B : E_{K_S}(f(R_B))$

Целью протокола является защищенная передача сеансового ключа K_S сторонам A и B. Сторона A получает K_S на шаге 2. Сообщение, передаваемое на шаге 3, может быть зашифровано и прочитано только стороной B. Шаг 4 отражает знание ключа K_S стороной B. Шаг 5 убеждает сторону B в том, что ключ K_S известен A и в том, что сообщение является новым, так как в нем используется R_B.

Пример 2. Протокол аутентификации и обмена ключами, в котором используются симметричная криптография, случайные числа и доверенный сервер, генерирующий сеансовый ключ.

1. А отсылает В свое имя и случайное число R_A.

$$A \to B : A \| R_A$$

2. В отсылает серверу свое имя и зашифрованное общим с В ключом сообщение, в котором конкатенируется имя А, случайное число R_A и собственное число R_B.

$$B \to S : B \| E_B(A \| R_A \| R_B)$$

3. Сервер генерирует А два сообщения. В первое сообщение входит имя В, сеансовый ключ К и случайные числа R_A и R_B. Это сообщение шифруется общим ключом S и А. Второе сообщение включает имя А и сеансовый ключ К. Сообщение шифруется общим ключом S и В.

$$S \to A : E_A(B \| K \| R_A \| R_B), E_B(A \| K)$$

4. А расшифровывает первое сообщение, извлекает ключ К, убеждается в том, что R_A совпадает со значение, отправленным на этапе 1. Затем посылает В два сообщения. Первое сообщение – это сообщение сервера, зашифрованное ключом В. Второе сообщение содержит случайное число R_B, зашифрованное сеансовым ключом.

$$A \to B : E_B(A \| K), E_K(R_B)$$

5. В расшифровывает первое сообщение, извлекает ключ К, убеждается в том, что R_B совпадает со значение отправленным на этапе 2.

7.2 Атаки на протоколы

Атаки на протоколы можно разделить на два класса:

1. При *пассивной атаке* взломщик не участвует в протоколе, он только следит за протоколом и пытается раздобыть ценную информацию на основе шифртекста.
2. При *активной атаке* взломщик пытается изменить протокол к собственной выгоде. С этой целью активный взломщик может выдавать себя за другого человека, повторять сообщения, заменять сообщения, разрывать линию, модифицировать информацию.

Примерами активных атак на протоколы являются атака «человек посередине», атака по словарю, атака с повторной передачей, атака с воспроизведением сообщений, атака на систему часов.

Атака «человек посередине» может быть успешной, если стороны A и B не имеют возможности проверить, действительно ли они общаются друг с другом. Помешать атаке «человек посередине» можно использованием цифровых подписей по ходу протокола обмена сеансовыми ключами либо

использованием одновременной передачи ключей и сообщений без предварительного обмена ключами.
Атака по словарю позволяет сравнивать краденный зашифрованный файл паролей с приготовленным файлом зашифрованных вероятных паролей, отыскивая совпадения. Затруднить атаку по словарю можно использованием привязок - случайных строк, которые конкатенируются с паролями перед их обработкой однонаправленной функцией.
Защита от *атак с повторной отсылкой сообщений* заключается в том, что операции шифрования и цифровой подписи должны различаться. Для этого нужно использовать разные ключи для каждой операции, либо использовать разные алгоритмы в каждой операции, либо наложение меток, либо создание цифровых подписей с применением хеш-функций.
Способами противодействия *атакам с воспроизведением сообщений* являются использование порядковых номеров сообщений, меток даты/времени, уникальных запросов (оказий) и ответов, содержащих корректное значение оказии.
Включив текущее время в криптографические протоколы, мы мешаем злоумышленнику пересылать старые сообщения под видом новых.
Однако успешная *атака на систему часов* (перевод часов назад или вперед, остановка часов) приводит к отправке сообщений с неправильной меткой даты/времени, что может иметь большие финансовые последствия.
Помешать атаке на систему часов можно, связывая между собой метки даты/времени всех сообщений.

7.3 Протоколы VPN

Для независимости от прикладных протоколов и приложений защищённые виртуальные сети формируются на одном из более низких уровней модели OSI — канальном, сетевом или сеансовом. Канальному (второму) уровню соответствуют такие протоколы реализации VPN, как PPTP, L2F, L2TP, сетевому (третьему) уровню — IPSec, SKIP, а сеансовому (пятому) уровню — SSL/TLS и SOCKS. Чем ниже уровень эталонной модели, на котором реализуется защита, тем она прозрачнее для приложений и незаметнее для пользователя. Но при снижении этого уровня уменьшается набор реализуемых услуг безопасности и становится сложнее организация управления. Чем выше защитный уровень, тем шире набор услуг безопасности, надёжнее контроль доступа и проще конфигурирование системы защиты, но в этом случае усиливается зависимость от используемых протоколов обмена и приложений [1].
Канальный уровень
Для стандартного формирования криптозащищённых туннелей на канальном уровне компанией Microsoft при поддержке других компаний был разработан протокол туннелирования PPTP (Point-to-Point Tunneling Protocol), представляющий собой расширение протокола PPP (Point-to-Point Protocol). Протокол PPTP предусматривает как аутентификацию удалённого пользователя, так и зашифрованную передачу данных, однако в этом протоколе не специфицируются конкретные методы аутентификации и шифрования.
Протокол L2F (Layer-2 Forwarding) разработан компанией Cisco Systems при поддержке компаний Shiva и Northern Telecom в качестве альтернативы протоколу PPTP. В отличие от протокола PPTP протокол L2F позволяет использовать для удалённого доступа к провайдеру Интернет не только протокол PPP, но и другие протоколы, например, SLIP. При формировании защищённых каналов по глобальной сети провайдерам Интернет не нужно осуществлять конфигурацию адресов и выполнять аутентификацию. Кроме того, для переноса данных через защищённый туннель могут использоваться различные протоколы сетевого уровня, а не только IP. В данном протоколе также не специфицируются конкретные методы аутентификации и шифрования.
Протокол L2TP (Layer-2 Tunneling Protocol) разработан в организации Internet Engineering Task Force (IETF) при поддержке компаний Microsoft и Cisco Systems как протокол защищённого туннелирования PPP-трафика через сети общего назначения с произвольной средой. L2TP, в отличие от PPTP, не привязан к протоколу IP, а потому может быть использован в сетях с коммутацией пакетов(в сетях ATM). L2TP также предусматривает управление потоками данных,

отсутствующее в L2F. Как и предшествующие протоколы канального уровня, спецификация L2TP не описывает методы аутентификации и шифрования.
Протоколы формирования защищённого туннеля на канальном уровне независимы от проколов сетевого уровня модели OSI. Они позволяют создавать защищённые каналы между удалёнными компьютерами и локальными сетями, работающими по различным протоколам сетевого уровня (IP, IPX или NetBEUI). Многопротокольность — основное преимущество инкапсулирующих протоколов канального уровня. Однако формирование защищённых туннелей на канальном уровне приводит к сложности конфигурирования и поддержки виртуальных каналов связи. Кроме того, протоколы канального уровня не специфицируют конкретные методы шифрования, аутентификации, проверки целостности каждого передаваемого пакета, а также средств управления ключами.
Можно сделать вывод, что протоколы создания защищённых виртуальных каналов на канальном уровне лучше всего подходят для защиты информационного взаимодействия при удалённом доступе к локальной сети.
Сетевой уровень
Спецификацией, где описаны стандартные методы для всех компонентов и функций защищённых виртуальных сетей, является протокол IPSec (Internet Protocol Security), соответствующий сетевому уровню модели OSI и входящий в состав IPv6. Протокол IPSec предусматривает стандартные методы аутентификации пользователей или компьютеров при инициации туннеля, стандартные способы шифрования конечными точками туннеля, формирования и проверки цифровой подписи, а также стандартные методы обмена и управления криптографическими ключами между конечными точками. Этот гибкий стандарт предлагает несколько способов для выполнения каждой задачи. Выбранные методы для одной задачи обычно не зависят от методов реализации других задач. Для функций аутентификации IPSec поддерживает цифровые сертификаты популярного стандарта X.509.
Туннель IPSec между двумя локальными сетями может поддерживать множество индивидуальных каналов передачи данных, в результате чего приложения данного типа получают преимущества с точки зрения масштабирования по сравнению с технологией второго уровня. Протокол IPSec может использоваться вместе с протоколом L2TP. Совместно эти протоколы обеспечивают наиболее высокий уровень гибкости при защите виртуальных каналов.
Для управления криптографическими ключами на сетевом уровне наиболее широкое распространение получили такие протоколы, как SKIP (Simple Key management for Internet Protocols) и ISAKMP (Internet Security Association and Key Management Protocol). SKIP проще в реализации, но он не поддерживает переговоров по поводу алгоритмов шифрования. Протокол ISAKMP поддерживает такие переговоры и выбран в качестве обязательного протокола для управления ключами в IPSec для IPv6, то есть ISAKMP является составной частью протокола IPSec.
Сеансовый уровень
Для шифрования информации на сеансовом уровне наибольшую популярность получил протокол SSL/TLS (Secure Sockets Layer/ Transport Layer Security), разработанный компанией Netscape Communications. Этот протокол создаёт защищённый туннель между конечными точками виртуальной сети, обеспечивая взаимную аутентификацию абонентов, а также конфиденциальность, подлинность и целостность циркулирующих по туннелю данных. Ядром протокола SSL/TLS является технология комплексного использования асимметричных и симметричных криптосистем компании RSA Data Security. Для аутентификации взаимодействующих сторон и криптозащиты ключа симметричного шифрования используются цифровые сертификаты открытых ключей пользователей (клиента и сервера), заверенные цифровыми подписями специальных Сертификационных Центров. Поддерживаются цифровые сертификаты, соответствующие общепринятому стандарту X.509.
С целью стандартизации процедуры взаимодействия клиент-серверных приложений TCP/IP через сервер-посредник (брандмауэр) комитет IETF утвердил протокол SOCKS. Данный протокол поддерживает приложения, требующие контроля над направлениями информационных потоков и

настройки условий доступа в зависимости от атрибутов пользователя и/или информации. В соответствии с SOCKS клиентский компьютер устанавливает аутентифицированный сеанс с сервером, исполняющим роль посредника (proxy). Посредник в свою очередь проводит любые операции, запрашиваемые клиентом. Поскольку посреднику известно о трафике на уровне сеанса, он может осуществлять тщательный контроль.

В отличие от виртуальных сетей, защищённых на сеансовом уровне, виртуальные сети на канальном или сетевом уровне обычно просто открывают или закрывают канал для всего трафика по аутентифицированному туннелю. Это может представлять проблему, если локальная сеть на другом конце туннеля является неблагонадёжной. Кроме того, туннели канального и сетевого уровня функционируют одинаково в обоих направлениях, а виртуальные сети на сеансовом уровне допускают независимое управление передачей в каждом направлении.

Протокол IPSec

Стандартные способы защиты информационного обмена на сетевом уровне модели OSI для IP-сети, являющейся основным видом публичных сетей, определяется протоколом IPSec (Internet Protocol Security). IPSec обеспечивает аутентификацию источника данных, криптографическое закрытие передаваемых пакетов сообщений, проверку их целостности и подлинности после приёма, защиту от навязывания повторных сообщений, а также частичную защиту от анализа трафика. Стандартизированными функциями IPSec-защиты могут и должны пользоваться протоколы более высоких уровней, в частности, управляющие протоколы, протоколы конфигурирования, а также протоколы маршрутизации.

В соответствии с протоколом IPSec архитектура средств безопасности информационного обмена на три уровня (рис 7.1).

На верхнем уровне расположены следующие протоколы:

– протокол согласования параметров виртуального канала и управления ключами (Internet Security Association Key Management Protocol — ISAKMP), обеспечивающий общее управление защищённым виртуальным соединением, включая согласование используемых алгоритмов криптозащиты, а также генерацию и распределение ключевой информации;

Рисунок 7.1 — Архитектура средств безопасности IPSec

– протокол аутентифицирующего заголовка (Authentication Header — AH), предусматривающий аутентификацию источника данных, проверку целостности и подлинности после приёма, а также защиту от навязывания повторных сообщений;

– протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload — ESP), обеспечивающий криптографическое закрытие передаваемых пакетов сообщений и предусматривающий также выполнение всех функций протокола аутентифицирующего заголовка (AH).

Использование в IPSec двух различных протоколов защиты виртуального канала (AH и ESP) обусловлено практикой, применяемой во многих странах на ограничение экспорта и/или импорта криптосредств. Каждый из этих протоколов может использоваться как самостоятельно, так и одновременно с другим.

Алгоритмы аутентификации и шифрования, используемые в протоколах аутентифицирующего заголовка (AH) и инкапсулирующей защиты содержимого (ESP), образуют средний уровень архитектуры IPSec. К этому уровню относятся также алгоритмы согласования параметров и управления ключами, применяемые в протоколе ISAKMP. Протоколы защиты виртуального канала верхнего уровня архитектуры IPSec (AH и ESP) не зависят от конкретных криптографических алгоритмов. Могут использоваться любые методы аутентификации, типы ключей (симметричные или несиметричные), алгоритмы шифрования и распределения ключей.

Алгоритмическая независимость протоколов AH и ESP требует предварительного согласования набора применяемых алгоритмов и их параметров, поддерживаемых взаимодействующими сторонами. Эту функцию и предусматривает протокол ISAKMP, в соответствии с которым при формировании защищённого виртуального канала взаимодействующие стороны должны выработать общий контекст безопасности (Security Association — SA) и только затем использовать элементы этого контекста, такие как алгоритмы и ключи.

Роль фундамента в архитектуре IPSec выполняет домен интерпретации (Domain of Interpretation — DOI), являющийся базой данных, хранящей сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах и т.п. Архитектура IPSec является полностью открытой. В IPSec могут использоваться протоколы и алгоритмы, которые изначально не разрабатывались для этой архитектуры. Поэтому возникла необходимость в домене интерпретации, который обеспечивал бы совместную работу всех включаемых протоколов и алгоритмов. Для того, чтобы в качестве алгоритмов аутентификации и шифрования в протоколах AH и ESP можно было использовать алгоритмы, соответствующие национальным стандартам, необходимо зарегистрировать эти алгоритмы в DOI.

В настоящий момент для протоколов AH и ESP зарегистрировано два алгоритма аутентификации: HMAC-MD5 (Hashed Message Authentication Code — Message Digest version 5) и HMAC-SHA1(Hashed Message Authentication Code — Secure Hash Algorithm version 1). Это алгоритмы аутентификации с секретным ключом. Если секретный ключ известен только передающей и принимающей сторонам, это обеспечит аутентификацию источника данных, а также целостность пакетов, пересылаемых между сторонами. Для обеспечения совместимости работы оборудования на начальной стадии реализации протокола IPSec по умолчанию принято использовать алгоритм аутентификации HMAC-MD5.

Для протокола ESP зарегистрировано семь алгоритмов шифрования. Алгоритм шифрования DES (Data Encryption Standart) принят по умолчанию и необходим для обеспечения IPSec совместимости. В качестве альтернативы DES определены алгоритмы Triple DES, CAST-128, RC-5, IDEA, Blowfish и ARCFour.

Протоколы AH и ESP поддерживают работу в двух режимах:

– туннельном, при котором IP-пакеты защищаются целиком, включая их заголовки;
– транспортном, обеспечивающим полную защиту только содержимого IP-пакетов.

Основным режимом является туннельный. При работе в этом режиме каждый обычный IP-пакет помещается целиком в криптозащищённом виде в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуют на специально выделенных защитных шлюзах, в роли которых могут выступать маршрутизаторы или межсетевые экраны. Между такими шлюзами формируются защищённые туннели IPSec. Перед передачей по такому туннелю исходные IP-пакеты передающей локальной сети инкапсулируются по протоколу IPSec в защищённые IP-пакеты. После передачи на другую сторону туннеля

защищённые IP-пакеты ’’распаковываются” и полученные исходные IP-пакеты передаются компьютерам приёмной локальной сети по стандартным правилам. Туннелирование IP-пакетов полностью прозрачно для обычных компьютеров в локальных сетях, являющихся держателями туннелей. На оконечных системах туннельный режим может использоваться для поддержки удалённых и мобильных пользователей. В этом случае на компьютерах этих пользователей должно быть установлено программное обеспечение, реализующее туннельный режим IPSec.

В транспортном режиме в конверт IPSec в криптозащищённом виде помещается только содержимое исходного IP-пакета и к полученному конверту добавляется исходный IP-заголовок. Соответственно в транспортном режиме заголовок IPSec размещается между сетевым (IP) и транспортным (TCP или UDP) заголовками обычного IP-пакета. Транспортный режим быстрее туннельного и разработан для применения на оконечных системах. Данный режим может использоваться для поддержки удалённых и мобильных пользователей, а также для защиты информационных потоков внутри локальных сетей. Кроме того, транспортный режим может применяться на шлюзах для защиты внутренних связей между одноранговыми шлюзами. Работа в транспортном режиме отражается на всех входящих в группу защищённого взаимодействия системах и в большинстве случаев требуется перепрограммирование сетевых приложений.

Протокол аутентифицирующего заголовка

Протокол аутентифицирующего заголовка (Authentication Header — AH) обеспечивает целостность IP-пакетов и аутентификацию источника данных, а также защиту от воспроизведения ранее посланных IP-пакетов. Этот протокол полностью защи0ает от подлога и случайного искажения содержимое IP-пакетов, включая данные протоколов более высоких уровней. Полнота защиты полей IP-заголовков зависит от используемого режима работы — туннельного или транспортного.

В туннельном режиме защищаются все поля IP-заголовков (рисунок 4.1). При защите каждый обычный IP-пакет помещается целиком в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет. В защищённом IP-пакете внутренний (первоначальный) IP-заголовок содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля.

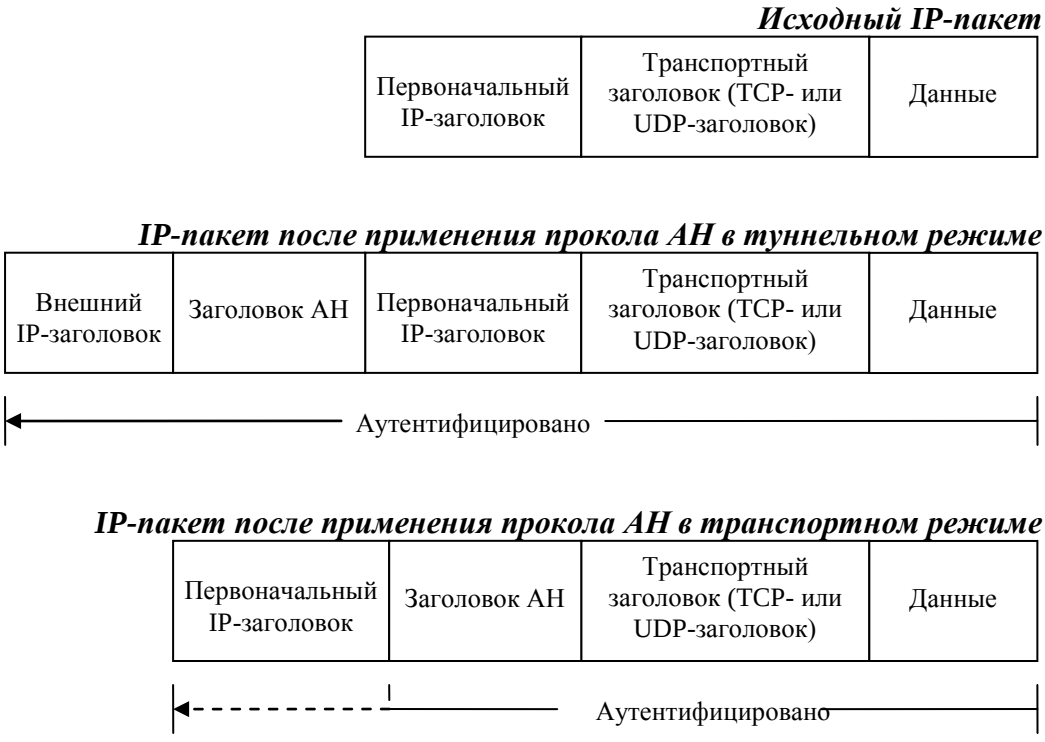

Рисунок 7.2 — IP-пакет до и после применения протокола AH

При использовании протокола AH в транспортном режиме защита не накладывается только на те поля IP-заголовков, которые меняются на маршруте доставки непредсказуемым образом. В транспортном режиме в конверт IPSec помещается только содержимое защищаемого IP-пакета и к полученному конверту добавляется исходный IP-заголовок (рисунок 4.1).
В формат заголовка AH входит поле переменной длины Authentication Data, содержащее информацию, используемую для аутентификации пакета и называемую MAC-кодом (Message Authentication Code). Это поле называют также цифровой подписью, имитовставкой, хэш-значением или криптографической контрольной суммой. Способ вычисления этого поля определяется алгоритмом аутентификации. В настоящее время предписывается обязательная поддержка алгоритмов HMAC-MD5 и HMAC-SHA1, основанных на применении односторонних хэш-функций с секретными ключами. Секретные ключи генерируются в соответствии с протоколом ISAKMP.
Таким образом, независимо от режима работы, протокол AH предоставляет меры защиты от атак, ориентированных на нарушение целостности и подлинности пакетов сообщений. С помощью этого протокола аутентифицируется каждый пакет, что делает неэффективной работу программ, пытающихся перехватить управление сеансом. Но следует иметь в виду, что аутентификация по протокол AH не допускает манипулирование основными полями IP-заголовка во время прохождения пакета. Поэтому данный протоколд нельзя применять в среде, где используется механизм трансляции сетевых адресов (Network Address Translation — NAT), так как манипулирование IP-заголовками необходимо для его работы.

Протокол инкапсулирующей защиты содержимого
Протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload — ESP) обеспечивает выполнение следующих функций по защите информационного обмена:

- криптографическое закрытие содержимого IP-пакетов;
- частичная защита от анализа трафика путём применения туннельного режима;
- формирование и проверка целостности цифровой подписи IP-пакетов для их защиты от нарушений подлинности и целостности;
- защита от воспроизведения IP-пакетов.

Представленный перечень функций по защите информационного обмена показывает, что функциональность протокола ESP шире, чем у протокола AH. Протокол ESP обеспечивает конфиденциальность данных, а также поддерживает все функции протокола AH по защите зашифрованных потоков данных от подлога, воспроизведения и случайного искажения.
Обобщённо все функции защиты, поддерживаемые протоколом ESP, можно свести к аутентификации, которую обеспечивает также протокол AH, и криптографическому закрытию передаваемых IP-пакетов. Спецификация IPSec допускает использование протокола ESP для криптографического закрытия IP-пакетов без использования функций аутентификации. Кроме того, допускается использование фиктивного шифрования при выполнении функций протокола AH. Таким образом, в протоколе ESP функции аутентификации и криптографического закрытия могут быть задействованы либо вместе, либо отдельно друг от друга. При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов (Network Address Translation — NAT), поскольку в этом случае адреса в заголовках IP-пакетов можно модифицировать.
Независимо от режима использования протокола ESP его заголовок формируется как инкапсулирующая оболочка для зашифрованного содержимого. В туннельном режиме использования протокола ESP в качестве инкапсулируемого пакета выступает весь исходный IP-пакет, а в транспортном — только его содержимое, то есть исходный TCP- или UDP-пакет.
Таким образом, если в соответствии с протоколом ESP предусматриваются и криптографическое закрытие и аутентификация, то аутентифицируется зашифрованный текст. Для входящих пакетов сначала производится аутентификация — это позволяет не тратить ресурсы на расшифровку поддельных пакетов, что в какой-то степени защищает от атак, ориентированных на отказ в обслуживании.

При использовании протокола ESP в туннельном режиме каждый исходный IP-пакет в криптозащищённом виде помещается целиком в конверт IPSec, а тот в свою очередь, инкапсулируется в другой IP-пакет. В защищённом IP-пакете внутренний (исходный) IP-заголовок, располагаемый в зашифрованной части, содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля. Когда ESP используется в транспортном режиме, в конверт IPSec в криптозащищённом виде помещается только содержимое исходного IP-пакета и к полученному конверту добавляется исходный IP-заголовок.

В настоящее время спецификация IPSec для криптографического закрытия IP-пакетов по протоколу ESP предписывает обязательную поддержку алгоритма шифрования DES-CBC (Data Encryption Standart in Cipher Block Chaining mode). Данный алгоритм шифрования применяется в протоколе ESP по умолчанию, и он необходим для обеспечения IPSec-совместимости. В качестве альтернативы DES определены алгоритмы Triple DES, CAST-128, RC-5, IDEA, Blowfish и ARCFour.

Алгоритм CAST (стандарт RFC 2144) считается таким же стойким, как алгоритм Triple DES со 128-битовым ключом. Кроме того. CAST быстрее, чем DES. Алгоритм RC5 (стандарт RFC 2040) является алгоритмом шифрования потока данных, использующим ключ переменной длины. Стойкость RC5 зависит от дины ключа, которая может достигать 256 бит. Алгоритм IDEA (Inretnational Data Encryption Algorithm) рассматривают как ’’быстрый’’ эквивалент Triple DES. Ещё одним алгоритмом, использующим ключ переменной длины, является Blowfish, который также считается достаточно стойким. Алгоритм ARCFour является общедоступной версией алгоритма RC4.

Выбор алгоритма, за исключение алгоритма DES, который является обязательным, целиком зависит от разработчика. Возможность выбора алгоритма шифрования предоставляет дополнительное преимущество: злоумышленник должен не только вскрыть шифр, но и определить, какой именно шифр ему надо вскрывать. Вместе с необходимостью подбора ключей это существенно снижает вероятность своевременного обхода криптозащиты.

Протоколы AH и ESP могут комбинироваться разными способами. Если используется транспортный режим, то протокол AH должен применяться после протокола ESP. В туннельном режиме протоколы AH и ESP применяются к разным вложенным пакетам и, кроме того, в данном режиме допускается многократная вложенность туннелей с различными начальными и/или конечными точками. Поэтому в случае туннельного режима число возможных комбинаций по совместному использованию протоколов AH и ESP существенно больше.

Управление защищенным туннелем

Создание и поддержка защищённого виртуального канала невозможны без реализации функций управления. В спецификации IPSec такие функции разделяются на две группы:

- общие функции управления, основанные на использовании базы данных политики безопасности (Security Policy Database — SPD);
- функции управления, ориентированные на согласование параметров туннеля и формирование контекста безопасности (Security Association — SA), который описывает общие параметры защищённого виртуального канала.

В соответствии с общими функциями управления все входящие и исходящие IP-пакеты должны сопоставляться с упорядоченным набором правил политики безопасности, которая задаётся для следующих объектов:

- для каждого сетевого интерфейса с задействованными средствами IPSec;
- для каждого исходящего и входящего потока данных.

Согласно спецификациям IPSec политика должна быть рассчитана на независимую обработку IP-пакетов на сетевом уровне модели OSI по современной технологии фильтрации. Соответственно должны существовать средства администрирования базы данных политики безопасности, подобные средствам администрирования базы правил межсетевых экранов. База данных политики безопасности (SPD) представляет собой упорядоченный набор правил, каждое из которых

включает совокупность селекторов и допустимых контекстов безопасности. Селекторы служат для отбора пакетов, а контексты задают требуемую обработку.

При сопоставлении с упорядоченным набором правил в первую очередь обрабатываются селекторы, в которых указывается совокупность анализируемых полей сетевого и более высоких протокольных уровней. В реализациях IPSec должна поддерживаться фильтрация IP-пакетов на основе анализа следующих элементов:

– исходного и целевого IP-адреса; при этом адреса могут быть индивидуальными и групповыми (допускается также применение в правилах диапазонов адресов и метасимволов ''любой'');
– имени пользователя или узла (в формате DNS или X.500);
– номеров используемого транспортного протокола;
– номеров исходного и целевого портов (могут применяться диапазоны и метасимволы).

Первое подходящее правило из базы данных политики безопасности (SPD) определяет дальнейшую судьбу пакета: пакет ликвидируется, либо пакет обрабатывается без использования средств IPSec, либо пакет обрабатывается средствами IPSec с учётом набора контекстов безопасности, ассоциированных с правилом.

В случае принятия решения об обработке пакета средствами IPSec анализируются контексты безопасности выбранного правила. Каждый контекст безопасности (SA) описывает параметры допустимого IPSec-соединения, включающие типы криптографических алгоритмов, ключи шифрования, а также другую служебную информацию. Если правило ссылается на несуществующий контекст, то для формирования защищённого IPSec-туннеля данный контекст должен быть создан. В этом случае должно поддерживаться автоматическое управление контекстами и ключами.

При создании контекста безопасности (SA) взаимодействующие стороны должны аутентифицировать друг друга и согласовать между собой параметры туннеля, включающие типы криптографических алгоритмов и ключи шифрования. Для решения этих задач в IPSec используется протокол согласования параметров виртуального канала и управления ключами (Internet Security Association Key Management Protocol — ISAKMP), обеспечивающий общее управление защищённым виртуальным соединением. Протокол ISAKMP описывает базовую технологию аутентификации, обмена ключами и согласования всех остальных параметров IPSec-туннеля при создании контекстов безопасности (SA). Однако ISAKMP не содержит конкретные алгоритмы обмена криптографическими ключами. Поэтому для обмена ключами могут использоваться другие протоколы. В настоящий момент в качестве такого протокола выбран протокол Oakley, основанный на алгоритме Диффи-Хеллмана. Объединение протоколов ISAKMP и Oakley обозначают как ISAKMP/ Oakley.

Согласно протоколу ISAKMP согласование параметров защищённого взаимодействия необходимо как при формировании IPSec-туннеля, так и при формировании в его рамках каждого защищённого однонаправленного соединения. Глобальные параметры туннеля образуют управляющий контекст и согласуются по протоколу ISAKMP/ Oakley. Параметры каждого защищённого однонаправленного соединения согласуются на основе созданного управляющего контекста и как раз образуют SA. Для идентификации каждого из контекстов безопасности предназначен индекс параметров безопасности (Security Parameters Index — SPI). Этот индекс включается в заголовки защищённых IPSec-пакетов, чтобы принимающая сторона смогла правильно их расшифровать и/или аутентифицировать, воспользовавшись указанным контекстом безопасности (SA).

Криптографические ключи для каждого защищённого однонаправленного соединения генерируются на основе ключей, выработанных в рамках управляющего контекста. При этом учитываются алгоритмы аутентификации и шифрования, используемые в протоколах AH и ESP.

В соответствии со спецификацией IPSec обработка исходящего и входящего трафика не является симметричной. Для исходящих пакетов просматривается база данных политики безопасности (SPD), находится подходящее правило, извлекаются ассоциированные с ним контексты

безопасности (SA) и применяются соответствующие функции защиты. Во входящих пакетах для каждого защитного протокола уже проставлено значение индекса параметров безопасности (SPI), однозначно определяющее контекст (SA). В этом случае просмотр базы данных политики безопасности не требуется.
Гибкость политики безопасности при использовании протокола IPSec определяется селекторами и контекстами безопасности, употреблёнными в правилах. Например, в случае, когда в селекторах фигурируют только IP-адреса, пара взаимодействующих компьютеров может применять один набор контекстов безопасности. Если же анализируются номера TCP- и UDP-портов, то набор контекстов может быть своим для каждого приложения. Соответственно, с одной стороны, два защитных шлюза могут организовать единый туннель для всех обслуживаемых компьютеров, а с другой — могут разграничить туннель путём организации разных контекстов по парам компьютеров или даже приложений.

8. Постановка задачи и исходные данные

Спроектировать виртуальную частную сеть (VPN) на основе Интернет для предприятия, имеющего территориально распределенные филиалы, и оценить надежность и безопасность услуги VPN. Исходными данными для проектирования и оценивания услуги VPN в общем случае являются типовые решения по организации услуги VPN, средние времена наработки на отказ элементов системы VPN, средние времена восстановления элементов системы VPN и вероятности (частоты) успешных атак. Исходные данные содержатся в таблицах 8.1 – 8.7. Для обозначения варианта используются цифры: m –последняя цифра номера зачетной книжки, n – предпоследняя цифра номера зачетной книжки.

Для проектирования и оценивания услуги VPN необходимо выполнить следующее:

1. Описать типовое решение по организации услуги VPN, предложенное компанией или фирмой, указанной в таблице 8.6. Описание VPN включает схему организации VPN, описание назначения и характеристик используемого оборудования VPN. При выполнении этого пункта рекомендуется не ограничиваться материалами учебного пособия и использовать источники Интернет.
2. Построить модель надежность услуги VPN, используя типовое решение компании, выбранной в пункте 1. Оценить коэффициент готовности услуги VPN, используя методику, описанную в разделе 5. Исходные данные содержатся в таблицах 8.1 – 8.4.
3. Построить модель безопасности услуги VPN, используя типовое решение компании, выбранной в пункте 1. Оценить безопасность услуги VPN как вероятности риска, используя методику, описанную в разделе 6. Исходные данные содержатся в таблицах 8.5 и 6.2.
4. Разработать протокол аутентификации и обмена ключами, используя элементы криптографических протоколов, приведенные в разделе 7.1. Исходные данные содержатся в таблицах 8.7 и 7.1-7.5. Разработанный протокол описать в соответствии с примером 2 в разделе 7.1 и указать, от каких атак на протоколы (раздел 7.2) защищает предложенный протокол.
5. Используя BAN-логику, выполнить формальный анализ разработанного протокола аутентификации и обмена ключами.
6. Предложить более полное описание угроз возникновения опасного состояния системы VPN, чем описание угроз в таблице 6.2, и выполнить пункт 3.
7. Оценить безопасность услуги VPN как ущерб (экономический показатель и/или балл), используя соответствующую методику в разделе 6.

Для курсового проектирования необходимо выполнить пункты 1–4. Для дипломного проектирования рекомендуется выполнить пункты 1–4 и некоторые из пунктов 5–7.

Таблица 8.1. Средние времена наработки на отказ элементов

№ варианта, m		0	1	2	3	4	5	6	7	8	9
ПК	ТС, месяц	5	6	7	8	9	10	5	12	7	6
	ПС, час	300	400	500	600	700	300	400	500	300	200
Линия доступа, год		1	2	3	4	1	2	3	4	1	2
Север доступа	ТС, год	1	2	3	4	5	1	2	3	4	5
	ПС, час	1000	2000	3000	1000	2000	3000	1000	2000	3000	1000
Транспортная сеть, год		5	6	7	8	9	10	11	12	13	14
Пограничный маршрутизатор, год		2	4	3	5	3	5	4	2	5	3
Сервера	ТС, год	3	5	2	4	5	3	5	3	4	2
	ПС, час	5000	6000	4000	6000	7000	5000	4000	6000	7000	5000
Брандмауэр	ТС, год	8000	6000	7000	8000	9000	6000	8000	7000	9000	6000
	ПС, час	4000	8000	6000	7000	5000	4000	6000	7000	8000	4000

Таблица 8.2. Средние времена восстановления элементов

№ варианта, n		0	1	2	3	4	5	6	7	8	9
ПК	ТС, час	3	4	5	6	2	3	4	5	6	4
	ПС, час	1	2	3	4	5	1	2	3	3	5
Линия доступа, час		7	8	9	10	11	12	13	14	15	20
Север доступа	ТС, час	5	6	7	8	5	6	7	8	5	6
	ПС, час	6	5	5	4	3	4	5	3	4	5
Транспортная сеть, час		0,5	0,6	0,7	0,8	0,9	1	1,1	1,2	1,3	1,4
Пограничный маршрутизатор, час		5	6	3	4	5	6	3	6	5	4
Сервера	ТС, час	3	4	5	6	2	3	4	5	6	4
	ПС, час	1	2	3	4	5	1	2	3	3	5
Брандмауэр	ТС,час	6	5	4	4	3	2	5	6	3	4
	ПС, час	3	5	3	2	4	1	5	2	3	1

Таблицв 8.3. Модели надежности элементов системы VPN

Элемент системы VPN	ПК	Линия доступа	Сервер доступа	Транспортная сеть	Пограничный маршрутизатор	Сервера	Брандмауэр
Модель надежности	Нерезервируемая система из 2 последовательно соединенных элементов	Нерезервируемая система	Дублируемая система с заданным режимом резервирования	Нерезервируемая система	Нерезервируемая система	Нерезервируемая система из 2 последовательно соединенных элементов	Нерезервируемая система из 2 последовательно соединенных элементов

Таблица 8.4. Режимы резервирования.

№ варианта, m	
0	Облегченный резерв, $\lambda_2=0,5\lambda_1$
1	Нагруженный резерв
2	Ненагруженный резерв
3	Облегченный резерв, $\lambda_2=0,2\lambda_1$
4	Нагруженный резерв
5	Ненагруженный резерв
6	Облегченный резерв, $\lambda_2=0,3\lambda_1$
7	Нагруженный резерв
8	Ненагруженный резерв
9	Облегченный резерв, $\lambda_2=0,4\lambda_1$

λ_1 – интенсивность отказов работающего элемента, λ_2 – интенсивность отказов резервного элемента.

Таблица 8.5. Вероятности успешных атак

№ варианта, m		0	1	2	3	4	5	6	7	8	9
ПК пользователя		0,23	0,15	0,1	0,06	0,04	0,3	0,2	0,22	0,24	0,12
Сервера	преграды 1-3	0,75	0,784	0,77	0,762	0,79	0,756	0,76	0,773	0,78	0,778
	преграды 4-6	0,21	0,246	0,23	0,224	0,24	0,248	0,22	0,215	0,25	0,232
	преграды 7	0,01	0,005	0,009	0,015	0,02	0,013	0,018	0,003	0,016	0,008
Брандмауэр		0,001	0,095	0,0015	0,0012	0,098	0,001	0,0014	0,096	0,0011	0,099
Пограничный маршрутизатор		0,001	0,0014	0,096	0,0011	0,001	0,099	0,095	0,0015	0,0012	0,098

Преграды 1-7 описаны в таблице 6.2.

Таблица 8.6. Типовые решения по организации VPN

№ варианта, n	0	1	2	3	4	5	6	7	8	9
Компания	АНКАД	Инфотекс	Микротест	Juniper Networks	Lusent	Cisco	АНКАД	Инфотекс	Lusent	Cisco

Таблица 8.7. Протоколы аутентификации и обмена ключами

№ варианта, m	Протокол
0	Протокол распределения ключей. В протоколе используются доверенный сервер, симметричная криптография, метки времени. Сеансовый ключ генерирует участник протокола.
1	Протокол распределения ключей. В протоколе используются доверенный сервер, симметричная криптография, случайные числа. Сеансовый ключ генерирует сервер.
2	Протокол распределения ключей. В протоколе используются доверенный сервер, симметричная криптография, порядковые номера, случайные числа. Сеансовый ключ генерирует сервер.
3	Протокол распределения ключей. В протоколе используются доверенный сервер, симметричная криптография, временные метки, время жизни. Сеансовый ключ генерирует участник протокола.
4	Протокол взаимной аутентификации участников протокола. В протоколе используется симметричная криптография и код MAC.
5	Протокол взаимной аутентификации и обмена ключами. В протоколе используются криптография с открытым ключом и симметричная криптография, временные метки и время жизни. Сеансовый ключ генерирует участник протокола.
6	Протокол взаимной аутентификации и обмена ключами. В протоколе используются криптография с открытым ключом, временные метки и случайные числа. Сеансовый ключ генерирует участник протокола.
7	Протокол распределения сеансовых ключей. В протоколе используются доверенный сервер, криптография с открытым ключом. У каждого участника уже имеется открытый ключ другого участника протокола. Сеансовый ключ генерирует участник протокола.
8	Протокол аутентификации участников и обмена сообщениями. В протоколе используется цифровая подпись.
9	Протокол взаимной аутентификации участников. В протоколе используются симметричная криптография и функция хэширования.

9. Требования к выполнению курсового проекта

Курсовой проект выполняется и оформляется в соответствии с требования РД ПГАТИ 2.11-2001.

Курсовой проект должен содержать:

- Задание и исходные данные варианта,
- Схему организации услуги VPN,
- Описание назначения и характеристик VPN-оборудования для выбранного решения,
- Модель надежности услуги VPN,
- Расчет коэффициента готовности услуги VPN,
- Модель безопасности услуги VPN,
- Расчет риска услуги VPN,
- Описание разработанного протокола аутентификации и обмена ключами,
- Описание атак, защиту от которых обеспечивает разработанный протокол,
- Заключение, содержащее краткое описание принятого решения по организации услуги VPN в таблицах.

В заключении приводятся таблицы, содержание которых показано ниже на примерах.

Таблица 10.1. Организация услуги VPN

Компания - разработчик	Средства VPN	Криптографические алгоритмы	Криптографические протоколы

Таблица 10.2. Характеристика услуги VPN

Коэффициент готовности услуги VPN	Меры повышения надежности услуги VPN	Риск услуги VPN	Меры снижения риска услуги VPN

Таблица10.3. Описание разработанного протокола

Назначение протокола	Используемые элементы шифрования, аутентификации и хэширования	Атаки, защиту от которых обеспечивает протокол

10. Источники

1. Денисова Т.Б. Надежность и безопасность услуги VPN, Электросвязь №9, 2005, С20-22.
2. Коваленко И.Н. Методы расчета высоконадежных систем. - Киев. Высшая школа, 1988.
3. Рябинин И.А. Надежность и безопасность структурно-сложных систем. – СПб.: Политехника, 2000.
4. Олифер В., Олифер Н. Новые технологии и оборудование IP-сетей.-СПб.:БХВ – Санкт-Петербург, 2000.
5. Шнайер Б. Прикладная криптография. – М.: Триумф, 2002.
6. Столлингс В. Криптография и защита сетей. – М.: Издательский дом «Вильямс», 2001.
7. Петров А.А. Компьютерная безопасность. – М.: ДМК, 2000.
8. Чмора А. Современная прикладная криптография. – М.: Гелиос АРВ, 2002.

9. Норткатт С., Новак Д. Обнаружение вторжений в сеть. – М.: Лори, 2002.
10. Норткатт С., Купер М., Фирноу М., Фредерик К. Анализ типовых нарушений безопасности в сетях. – М.: Издательский дом «Вильямс», 2001.
11. Лукацкий А. Обнаружение атак. – СПб.: БХВ - Петербург, 2003.
12. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательское агентство «Яхтсмен», 1996.
13. Безкоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КОК». – М.: СИНТЕГ, 2000.
14. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. – М.: Высшая школа, 1999.
15. РД ПГАТИ 2.11-2001. Курсовое проектирование. Выполнение и оформление курсовых проектов и работ. Правила и рекомендации. ПГАТИ.2001