САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА

Факультет СС, СК и ВТ

Дипломная работа

на тему

«Анализ использования протоколов IPSec для обеспечения информационной безопасности в сети Интернет»

Дипломник Губина А.А.

Руководитель работы Доронин Е.М.

Санкт-Петербург

2012г.

РЕФЕРАТ

Тема дипломной работы: «Анализ использования протоколов IPSec для обеспечения информационной безопасности в сети Интернет».

Пояснительная записка включает:

Листов 117.

Рисунков 85.

Таблиц 4.

Перечень ключевых слов: информационная безопасность, Интернет, угрозы, сетевые атаки, несанкционированный доступ (НСД), конфиденциальность, целостность, аутентификация, шифрование, протоколы IPSec.

Цель работы: раскрыть механизмы использования протоколов IPSec в сети Интернет, показать примеры их применения для обеспечения информационной безопасности.

В ходе дипломной работы рассмотрены проблемы информационной безопасности, обоснована необходимость обеспечения информационной безопасности в сети Интерент, рассмотрены основные виды угроз информационной безопасности и способы борьбы с ними, названы основные протоколы безопасности, даны описания протоколов IPSec и подробно рассмотрены принципы работы этих протоколов, а также преимущества использования протоколов IPSec для обеспечения защиты информации в сети Интернет. Проведено исследование влияния работы протоколов безопасности IPSec на производительность сети. Разработан обучающий видео-курс по настройке политики безопасности IPSec в ОС Microsoft Windows XP. Разработан контрольный тест для использования в процессе обучения.

СОДЕРЖАНИЕ

Введение

Первоначально сеть, которая в будущем получила название «Интернет» имела небольшое число пользователей, но в дальнейшем она стала обретать огромную популярность.

Информационные технологии успешно внедряются во все сферы человеческой деятельности. Благодаря всемирной сети Интернет с помощью стека протоколов TCP/IP и единого адресного пространства объединяются не только корпоративные и ведомственные сети, но и отдельные пользователи, которые имеют прямой доступ в Интернет со своих домашних компьютеров.

Проблема защиты передаваемой информации от несанкционированного доступа или искажения волнует многих пользователей, которым необходимо иметь постоянный доступ к своей персональной информации и быть уверенными в невозможности ее неправомерного использования.

Наиболее остро данная проблема стоит перед компаниями и организациями. При появлении угроз, связанных с возможностью потери, искажения, раскрытия конфиденциальных данных и утечки стратегически важной информации, организация или государство в целом может потерять не только огромные суммы денег, но и репутацию на политическом и экономическом уровне.

Добиться высокой степени защищенности можно только при использовании передовых технологий защиты сети передачи данных.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается и уровень угроз для используемых информационных технологий. С каждым годом появляются все новые и новые атаки на сети передачи данных. В ответ на новые атаки появляются новые или совершенствуются старые методы защиты информации и информационно-технической инфраструктуры.

Посредством использования современных способов и средств защиты целостности и конфиденциальности информации (антивирусных программ, межсетевых экранов, программных и аппаратных продуктов для защиты

информации от НСД, вирусных атак и др.) можно обеспечить безопасность автоматизированной системы в целом и личного автоматизированного рабочего места (АРМа) пользователя.

Успех применения систем защиты информации зависит от наличия у них развитых средств управления режимами работы и реализации функций, позволяющих существенно упрощать процессы установки, настройки и эксплуатации средств защиты.

В данной дипломной работе названы различные способы обеспечения информационной безопасности в сети Интернет и дан подробный анализ использования протоколов IPSec для этой цели. Проведены исследования эффективности работы протоколов IPSec и влияния использования этих протоколов на скорость передачи данных по сети.

В форме видеоурока разработано руководство по настройке политики безопасности IPSec на компьютере пользователя, показаны возможности настройки IPSec для работы в качестве межсетевого экрана. Разработан тест для проверки знаний, полученных после просмотра видеоурока.

1. Проблема информационной безопасности в сети Интернет

1.1 Интернет

На сегодняшний день человечество вплотную подошло к рубежу, за которым начинается новый этап его развития, получивший название «информационного общества». Современные компьютеры, глобальные информационные сети и сетевые технологии сильно изменили нашу жизнь. Новейшие технологии и различные средства связи интегрировались во все сферы человеческой жизни. Если раньше главным источником информации для человека было живое общение, то теперь можно получить необходимую информацию, не выходя из дома, имея только выход в Интернет. Интернет не имеет строго определённой аудитории. Он необходим и востребован всеми, вне зависимости от возраста, социального статуса, национальности, индивидуальных особенностей и прочих факторов. Трудно представить, но в 1992 году аудитория Интернета составляла всего 100 человек, которые имели специальные навыки. Сейчас доступ к Сети имеют более 30% жителей Земли.

Статистика использования сети Интернет в мире по данным агентства *«Internet World Stats»* приведена в табл. 1.1. По представленным данным можно сделать вывод о том, насколько быстро Интернет проникает в нашу повседневную жизнь. Так с 2000 по 2011 год число пользователей глобальной сети увеличилось более, чем в 5 раз, и это далеко не предел, так как доступ к Интернет имеют всего лишь 33% населения планеты.

По данным того же агентства в России к сети Интернет имеют доступ более 61 миллиона человек, что составляет около 44% всего населения страны. Выйдя за рамки науки, Интернет стал частью повседневной жизни, частью мировой культуры, новым параллельным измерением жизни общества. Интернет имеет свои законы и нормы, утверждённые на государственном уровне. Он даёт возможность получить общение, знания, работу, развлечения всем пользователям.

Таблица 1.1. Статистика использования Интернет в мире

Регион	***Население***	***Число пользователей (31 декабря 2000)***	***Число пользователей (31 декабря 2011)***	***Рост с 2000 по 2011 год***
Африка	1 037 524 058	4 514 400	139 875 242	2 988.4 %
Азия	3 879 740 877	114 304 000	1 016 799 076	789.6 %
Европа	816 426 346	105 096 093	500 723 686	376.4 %
Средний Восток	216 258 843	3 284 800	77 020 995	2 244.8 %
Северная Америка	347 394 870	108 096 800	273 067 546	152.6 %
Латинская Америка	597 283 165	18 068 919	235 819 740	1 205.1 %
Океания и Австралия	35 426 995	7 620 480	23 927 457	214.0 %
Весь мир	6 930 055 154	360 985 492	2 267 233 742	528.1 %

Определение термина Интернет (англ. Internet) было дано 24 октября 1995 года Федеральным советом США по компьютерным сетям (FNC – Federal Networking Council): Internet – это глобальная информационная система, которая логически соединена посредством адресного пространства, основанного на протоколе IP (Internet Protocol) или заменяющих его протоколов, способна поддерживать передачу данных посредством протокола TCP (Transmission Control Protocol) или заменяющих его протоколов, обеспечивает, использует или делает доступными услуги по передаче данных и соответствующую инфраструктуру.

Принято считать, что первоосновой сети Интернет является сеть ARPAnet, созданная в 60-х годах двадцатого столетия по указу Министерства Обороны США. Проект оказался таким удачным, что сетью заинтересовались и другие компании. Множество сетей, построенных на схожих принципах, были объединены между собой и образовали единое информационное пространство. До середины 90-х годов сеть Интернет выполняла довольно узкую функцию: предоставляла пользователям ПК обмениваться почтой и новостями. До 1993 года Интернет использовался исключительно в научно-техническом кругу.

Мощным толчком для развития мирового информационного пространства послужило появление службы World Wide Web (WWW). Теперь каждый пользователь компьютера, имеющий доступ к Сети, мог создать собственный Web-сервер и разместить на нем различные материалы, доступные для общего обозрения. Практически все сферы интересов человечества, нашли свое отражение в Интернет. В зоне его влияния оказалось государство, СМИ, бизнес, образование, здравоохранение и многое другое.

Сегодня сеть Интернет имеет невообразимые размеры и состоит из сотен тысяч сетей, разбросанных по всему миру. Глобальная сеть больше не зависит от базовой (или магистральной) сети или от работы правительственных структур. Современный Интернет – это творение поставщиков услуг, работающих на коммерческой основе. Национальные поставщики сетевых услуг, то есть поставщики первого звена, а также региональные поставщики услуг создают собственную инфраструктуру. Поставщики услуг Интернета (Internet Service Providers, ISP) обеспечивают локальный доступ и обслуживание пользователей.

У истоков Интернет в России стоят компьютерные сети ОИЯИ (г. Дубна) и Института им. Курчатого И. В. (г. Москва).

Высшая школа – естественный и активный участник работ по развитию Интернет в России. В 1993 году в Госкомвузе РФ были разработаны концепция и программа создания российской университетской компьютерной сети, которая получила название RUNNet (Russian UNiversity Network). Сеть RUNNet необходима для достижения двух целей: формирования единого информационного пространства российской высшей школы и его интеграции в мировую информационную систему образования, науки и культуры, развивающуюся в рамках глобальной сети Internet. В 1994-95 годах была создана основа RUNNet – опорная сеть, обеспечивающая магистральную связь между всеми экономическими регионами России и подключение к Интернет через зарубежные академические сети. В эту

опорную сеть включены компьютерные узлы крупных научных и учебных центров страны, связанные между собой спутниковыми каналами.

1.2 Ключевые принципы и обобщенная структура сети Интернет

Интернет состоит из многих тысяч корпоративных, научных, правительственных и домашних компьютерных сетей. Компьютеры в Сети обмениваются друг с другом информацией по каналам общественных телекоммуникаций (выделенным телефонным аналоговым и цифровым линиям, оптическим каналам связи и радиоканалам, в том числе спутниковым линиям связи).

Основными компонентами глобальной сети являются локальные вычислительные сети. Если локальная сеть подключена к глобальной, то каждая рабочая станция этой сети может быть подключена к ней. Существуют также компьютеры, подключенные непосредственно к глобальной сети. Они называются хостами (host – хозяин).

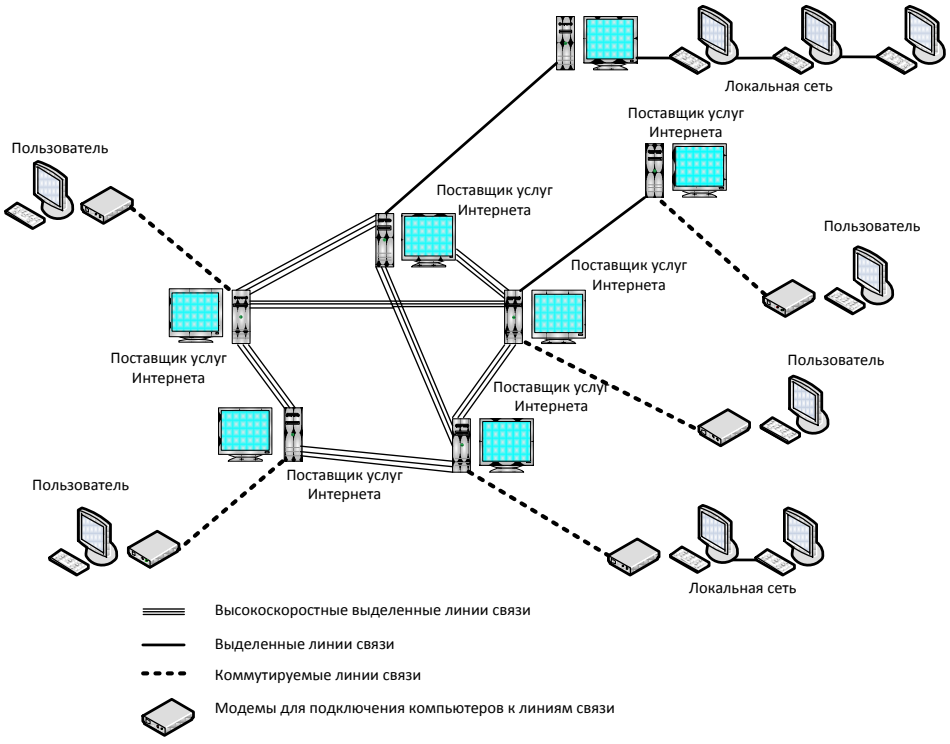


Рис. 1.1. Структура сети Интернет

Информация в Интернет хранится на Web и Ftp-серверах. Отдельные пользователи подключаются к сети через компьютеры сервис-провайдеров

(Internet Service Provider – ISP). Региональный провайдер подключается к более крупному провайдеру национального масштаба, имеющему узлы в различных городах страны. Сети национальных провайдеров объединяются в сети транснациональных провайдеров или провайдеров первого уровня (рис. 1.1).

Важной особенностью сети Интернет является высокая надежность. При выходе из строя части компьютеров или линий связи сеть будет функционировать и передавать сообщения по другим линиям связи благодаря тому, что в Интернет нет единого центра управления.

Существует целый ряд некоммерческих организаций, обеспечивающих функционирование Интернета. Среди них следует отметить следующие:

Общество Интернета (англ. Internet Society, ISOC) – международная профессиональная организация, которая занимается развитием и обеспечением доступности сети Интернет. Основной задачей ISOC является обеспечение развития, эволюции и использования Интернета в мировом масштабе. Общество Интернета является головной организацией и представляет организационную основу для множества различных консультативных и исследовательских групп, занимающихся развитием Интернета, включая IETF и IAB.

Совет по архитектуре Интернета (англ. Internet Architecture Board, IAB) Утверждает новые протоколы, стандарты, проекты развития Сети, правила выдачи адресов и т.д. IAB руководит группами IANA, IETF, IRTF.

Рабочая инженерная группа по решению задач проектирования Интернета (англ. Internet Engineering Task Force, IETF). Это открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, которое занимается развитием протоколов и архитектуры Интернета, отвечает за решение инженерных задач в сетях, выпускает большинство документов RFC, используемых производителями для внедрения стандартов в архитектуру Интернета.

Рабочая исследовательская группа по развитию Интернета (англ. Internet Research Task Force, IRTF) – одно из подразделений IAB, отвечающее за разработку протоколов Интернет и исследования в области будущего Интернета.

Корпорация Интернет по выделенным именам и номерам (Internet Corporation for Assigned Names and Numbers, ICANN) – группа, заведующая системой названия доменов и присвоения протокольных номеров в сети Интернет.

Администрирация адресного пространства Интернет (Internet Assigned Numbers Authority, IANA) – организация, отвечающая за предоставление IP-адресов, доменов верхнего уровня и номеров протокола IP, а также распределение ресурсов портов.

Региональный интернет-регистратор (англ. Regional Internet Registry, RIR) – организация, занимающаяся вопросами адресации и маршрутизации в сети Интернет, отвечает за техническую сторону функционирования сети: выделение IP-адресов, номеров автономных систем, регистрацию зон DNS. Часто региональные регистраторы занимаются статистическим анализом сетей, мониторингом точек обмена трафиком и поддержкой корневых зон DNS.

VeriSign – организация, поддерживающая домены первого уровня .com, .net и некоторые другие.

В основе работы глобальной сети Интернет лежит набор (стек) протоколов TCP/IP. Наличие стека протоколов TCP/IP является обязательным условием подключения к Интернету, поэтому рост этой сети приводит к росту интереса к TCP/IP.

Название «TCP/IP» связано с целым семейством протоколов передачи данных. Оно происходит от названий двух протоколов этого семейства: протокола управления передачей (TCP, Transmission Control Protocol) и протокола Internet (IP, Internet Protocol).

Протокол – это свод официальных правил поведения. Для того, чтобы компьютеры смогли общаться, необходим набор правил, которому подчиняется это общение. В обмене данными подобные наборы правил называются протоколами. Стек протоколов – это иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети.

TCP/IP создает гетерогенную сеть с открытыми протоколами, не зависящими от деталей разработки архитектуры компьютера и реализации операционной системы. Открытая природа протоколов TCP/IP требует открытости процесса разработки стандарта и свободного доступа к соответствующим документам. Разработка стандартов Интернета происходит на открытых сессиях комитета по технологической поддержки сети Интернет IETF. Разработанные протоколы публикуются как документы RFC *(Request for Comments, запрос комментариев)*. Существуют три типа документов RFC: стандарты *(standards, STD), современные практики(best current practices, BCP), а также уведомляющие (for your information, FYI).*

Стек протоколов TCP/IP обладает рядом следующих важных особенностей:

1. Это свободно распространяемые открытые стандарты протоколов, не зависящие от конкретного аппаратного обеспечения и операционной системы.
2. Независимость от конкретных физических устройств, что позволяет интегрировать самые разные типы сетей посредством TCP/IP. В качестве физического транспорта может использоваться почти любая система: Ethernet, соединение DSL, коммутируемое соединение, оптоволоконный канал и др.
3. Универсальная схема адресации, позволяющая произвольному устройству обращаться к любому другому устройству сети по уникальному адресу.
4. Это стандартизированные высокоуровневые протоколы, согласующие работу распространенных пользовательских служб.

Для описания структуры и функциональности протоколов обмена данными часто используется архитектурная модель, разработанная международной организацией по стандартизации (International Standards Organization, ISO). Данная модель называется Эталонной Моделью Взаимодействия Открытых Систем (ЭМВОС, Open System Interconnection (OSI) Reference Model). Термины, определенные в рамках модели OSI, имеют широкое применение.

Опорная модель OSI состоит из семи уровней, определяющих функциональность протоколов обмена данными. Каждый из уровней модели OSI представляет функцию, выполняемую при передаче данных между приложениями, взаимодействующими по сети. Названия и краткие функциональные описания уровней модели ***ISO/OSI*** приведены на рис. 1.2.

Модель ISO/OSI

7	***Прикладной уровень*** ***(Application Layer)*** *Состоит из сетевых приложений*
6	***Уровень представления*** ***(Presentation Layer)*** *Стандартизирует представление данных в приложениях*
5	***Сеансовый уровень*** ***(Session Layer)*** *Управляет сеансами взаимодействия приложений*
4	***Транспортный уровень*** ***(Transport Layer)*** *Обеспечивает передачу данных с требуемой степенью надежности.*
3	***Сетевой уровень*** ***(Network Layer)*** *Управляет сетевыми соединениями в пользу вышележащих уровней*
2	***Канальный уровень*** ***(Data Link Layer)*** *Проверяет доступность среды передачи, реализует механизмы обнаружения и корректировки ошибок, обеспечивает корректность передачи фреймов*
1	***Физический уровень*** ***(Physical Layer)*** *Передает биты по физическому каналу, определяет характеристики электрических сигналов, стандартизирует разъемы и т.п.*

Рис. 1.2. Уровни модели ISO/OSI

Уровень не содержит определение отдельного протокола; определяемая уровнем функциональность может быть реализована любым

числом протоколов. Таким образом, каждый уровень способен вмещать произвольное количество протоколов, каждый из которых реализует службу, соответствующую функциональности этого уровня. Например, протоколы передачи файлов и электронной почты реализуют пользовательские службы и принадлежат к прикладному уровню.

Наиболее распространенными функциональными службами в Интернет являются:

- E-mail - электронная почта. Для реализации электронной почты используются протоколы: SMTP (Simple Mail Transfer Protocol - простой протокол электронной почты), POP3 (Post Office Protocol Version 3 - протокол почтового отделения, версия 3). IMAP (Internet Message Access Protocol - протокол для доступа к электронной почте).
- WWW – распределенная система гипермедиа Word Wide Web. В основу системы легла технология гипертекста и прикладной протокол HTTP для передачи Web-страниц. Возможность просмотра Web-страниц предоставляют прикладные программы – браузеры. К наиболее популярным из них относятся Internet Explorer, Mozilla Firefox, MyIE Web Browser, Opera и др.
- FTP-служба. Это служба, которая позволяет пересылать файлы между компьютерами, работающими в сетях TCP/IP, при помощи прикладного протокола передачи файлов FTP (File Transfer Protocol).
- Telnet – доступ к компьютерам в режиме удаленного терминала. Используется протокол Telnet.
- Службы для электронного общения в режиме онлайн: мессенджеры и VoIP сервис.

Модель стека протоколов TCP/IP была разработана Министерством обороны США в процессе создания сети, способной сохранять работоспособность в любых условиях. Задачу гарантировать доставку пакетов в любое время, при любых условиях и в любую точку сети решили

созданием набора протоколов TCP/IP, впоследствии ставшего стандартом при построении сети Интернет.

Модель TCP/IP состоит из четырех уровней: уровня приложений, транспортного уровня, межсетевого уровня *Internet* и уровня доступа к сети. Стоит отметить, что некоторые из уровней моделей ISO/OSI и TCP/IP имеют одинаковые названия, однако функции, выполняемые на этих уровнях, могут быть различны. Рассмотрим функциональность каждого из уровней (рис.1.3):

Модель стека протоколов TCP/IP

4	***Прикладной уровень*** ***(Application Layer)*** *Состоит из сетевых приложений и процессов*
3	***Транспортный уровень*** ***(Transport Layer)*** *Обеспечивает функциональность доставки данных адресату*
2	***Уровень Internet*** ***(Internet Layer)*** *Дает определение дейтаграммы и отвечает за маршрутизацию данных*
1	***Уровень доступа к сети*** ***(Network Access Layer)*** *Состоит из функций доступа к физической сети*

Рис. 1.3. Уровни модели TCP/IP

Уровень доступа к сети.

Этот уровень описывает методы построения локальных (LAN) и распределенных (WAN) вычислительных сетей и соответствует физическому и канальному уровням модели OSI, отвечает за физическую связь со средой передачи данных для данного аппаратного типа сетевого интерфейса.

Функциональность данного уровня включает инкапсуляцию IP-пакетов в передаваемые по сети фреймы, а также преобразование IP-адресов в физические адреса.

Уровень Internet

Этот уровень управляет сетевыми соединениями и освобождает протоколы более высоких уровней от необходимости непосредственного взаимодействия с физической инфраструктурой сети. Его называют сетевым

уровнем модели TCP/IP. Поскольку сетевой уровень стека TCP/IP в первую очередь отвечает за межсетевое взаимодействие, его часто называют также Internet-уровнем модели TCP/IP.

Internet-уровень обеспечивает отправку пакетов сетевыми устройствами посредством соответствующего протокола. На этом уровне происходит выбор наилучшего маршрута и пересылка пакета. На Internet-уровне стека TCP/IP работают перечисленные ниже протоколы.

- *IP* — протокол без установления соединения, обеспечивающий выбор наилучшего маршрута для доставки пакетов.
- *ICMP (Internet Control Message Protocol)* - протокол управляющих сообщений в сети Интернет, предоставляет функции контроля и управления сообщениями.
- *ARP (Address Resolution Protocol)* - протокол преобразования адресов, определяет адреса канального уровня (MAC-адреса) по известным IP-адресам.
- *RARP (Reverse Address Resolution Protocol)* - протокол обратного преобразования адресов, определяет IP-адреса для известных адресов канального уровня (MAC-адресов).

Протокол IP имеет следующую функциональность: определяет формат пакета и схему адресации, осуществляет передачу данных от уровня Internet к уровню сетевого доступа, осуществляет маршрутизацию к удаленным узлам. Он не осуществляет проверку данных и коррекцию ошибок. Обе функции выполняются на более высоких уровнях: транспортном и уровне приложений.

Транспортный уровень

Транспортный уровень предоставляет транспортные услуги от узла отправителя к узлу получателя. Он поддерживает логическое соединение между конечными точками сетевого маршрута. Наиболее важными протоколами транспортного уровня являются протокол управления передачей *TCP* (*Transmission Control Protocol*), с установлением соединения,

и протокол пользовательских дейтаграмм *UDP (User Datagram Protocol),* без установления соединения, то есть доставка данных не гарантирована. Оба протокола выполняют доставку данных между прикладным уровнем и уровнем Internet.

Прикладной уровень

Модель TCP/IP включает протокол верхнего уровня, использующий сеансовый уровень (session), уровень представления (presentation) и уровень приложений (application) модели OSI. Уровень приложений решает задачи представления, кодирования данных и контроля взаимодействия между конечными системами. В набор TCP/IP входят протоколы: HTTP, FTP, TFTP, SMTP, SNMP, telnet и др.

Благодаря тому, что протоколы TCP/IP являются стандартами, по которым была создана сеть Интернет, модель TCP/IP получила широкое распространение. В большинстве случаев существующие сети построены не в строгом соответствии с эталонной моделью OSI. Она служит лишь руководством для понимания коммуникационных процессов и доказала свою эффективность как методологический инструмент.

Каждый компьютер в сети Интернет имеет свой уникальный IP-адрес. Для адресов версии IPv4 адрес имеет длину 32 бита. Адреса версии IPv6 имеют длину 128 бит.

Адреса в Интернете могут быть представлены как в цифровом, так и в символьным виде. При пересылке информации компьютеры используют цифровые IP-адреса, а пользователи используют в основном имена в символьном виде.

Для указания ресурса в Интернете используются URL (Universal Resource Locator). URL указывает, с помощью какого протокола следует обращаться, какую программу следует запустить на сервере и к какому конкретному файлу следует обратиться на сервере.

1.3 Роль сети Интернет в жизни общества

Интернет – самый массовый и оперативный источник информации. Огромным количеством Web-станиц сегодня представлены самые различные организации, фирмы и компании. В Интернет расположены «электронные» варианты многих тысяч газет и журналов, через Сеть вещают сотни радиостанций и телекомпаний.

Интернет – крупнейший в мире источник развлечений. Интернет предоставляет огромный выбор всевозможных игр и самой разнообразной музыки, фильмов, видеороликов, книг, картинных галерей и фотовыставок, отвечающих любым нашим потребностям и вкусам.

Интернет – самое прогрессивное средство общения и коммуникации. Социальные сети, форумы и чаты - неотъемлемая часть жизни современного человека. Каждый день пользователи Сети отправляют друг другу сотни миллионов электронных посланий. Многие из них пользуются услугами Интернет-телефонии и видеоконференций, и с каждым днем эти технологии общения становятся все более востребованными и популярными.

Интернет – самое благоприятное пространство для бизнеса. При современном темпе жизни все большую популярность приобретает электронная торговля, позволяющая пользователю совершить покупку практически любого товара в удобное время в любой точке планеты. Для крупных фирм и корпораций Сеть стала идеальной средой для проведения всевозможных операций и расчетов, торговли, совещаний в реальном времени.

Интернет – это идеальный инструмент для рекламы. Сеть дает любому человеку практически бесплатную возможность оповестить многомиллионную аудиторию о предлагаемых им услугах или продукции.

Интернет – это обширный простор для творчества. С помощью Сети можно заявить о себе, о своих интересах, увлечениях и способностях на весь мир, а также самосовершенствоваться и обучаться чему угодно, не выходя из дома, получая при этом огромное количество необходимой и полезной

информации, просматривая видеоуроки и ролики, фотографии, материалы на любую интересующую вас тематику.

1.4 Актуальность проблемы обеспечения информационной безопасности в сети Интернет

Отрасль информационных технологий развивается очень быстрыми темпами, каждый день в мире появляются новые решения, технологии и идеи по внедрению этих технологий в нашу повседневную жизнь. Проблемы информатизации общества решаются на государственном уровне, правительства озабочены уровнем информатизации всех слоев и категорий населения, принимается множество законов о введении информационных новшеств во все сферы человеческой деятельности.

Сейчас уже сложно представить жизнь без мобильных телефонов, электронной почты, интересных и полезных сетевых приложений, сетевого общения, возможности срочных деловых переговоров или получения важной информации через Интернет в любом месте, где бы ни возникла такая необходимость, без ограничений во времени и в пространстве.

Информационные технологии уверенно проникают в нашу жизнь, а значит все больше сведений о нас, которые находятся в Сети, необходимо защищать.

Электронные дневники и журналы, электронные медицинские карты, виртуальные банки, предоставляющие возможность проведение банковских операций через Сеть, электронные деньги и платежи, предоставляющие возможность оплаты покупок и услуг через Интернет, все это удобные нововведения, но они же представляют собой потенциальную опасность, и могут быть причиной вторжения в личную жизнь каждого человека.

Все эти нововведения требуют особого внимания к конфиденциальности информации. При недостаточном внимании к этой проблеме злоумышленник легко сможет получить информацию о состоянии здоровья любого человека, атрибуты его банковской карты, аккаунты

соцсетей и электронной почты, паспортные данные, базы и списки клиентов любой организации, финансовые данные граждан и повредить или использовать эту информацию в своих целях. Для обычных людей, вынужденных использовать Интернет в качестве хранилища своих персональных данных, очень важно быть уверенными в том, что информация, владельцами которой они являются, не будет получена несанкционированными пользователями.

С развитием информационных и компьютерных технологий, без обеспечения информационной безопасности стало невозможно существование мелких и крупных компаний и организаций. На сегодняшний день ключевую роль в обеспечении эффективного выполнения бизнес-процессов как коммерческих, так и государственных предприятий играют автоматизированные системы (АС). Вместе с тем повсеместное использование АС для хранения, обработки и передачи информации приводит к повышению актуальности проблем, связанных с их защитой. Подтверждением этому служит тот факт, что за последние несколько лет, как в России, так и в ведущих зарубежных странах имеет место тенденция увеличения числа информационных атак, приводящих к значительным финансовым и материальным потерям.

Практически любая АС может выступать в качестве объекта информационной атаки. Для реализации информационной атаки нарушителю необходимо активизировать или, другими словами, использовать определённую уязвимость АС, т.е. слабое место АС, на основе которого возможна успешная реализация атаки. Примерами уязвимостей АС могут являться: некорректная конфигурация сетевых служб АС, наличие ПО без установленных модулей обновления, использование нестойких к угадыванию паролей, отсутствие необходимых средств защиты информации и др. Логическая связь уязвимости, атаки и её возможных последствий показана на рис. 1.4:

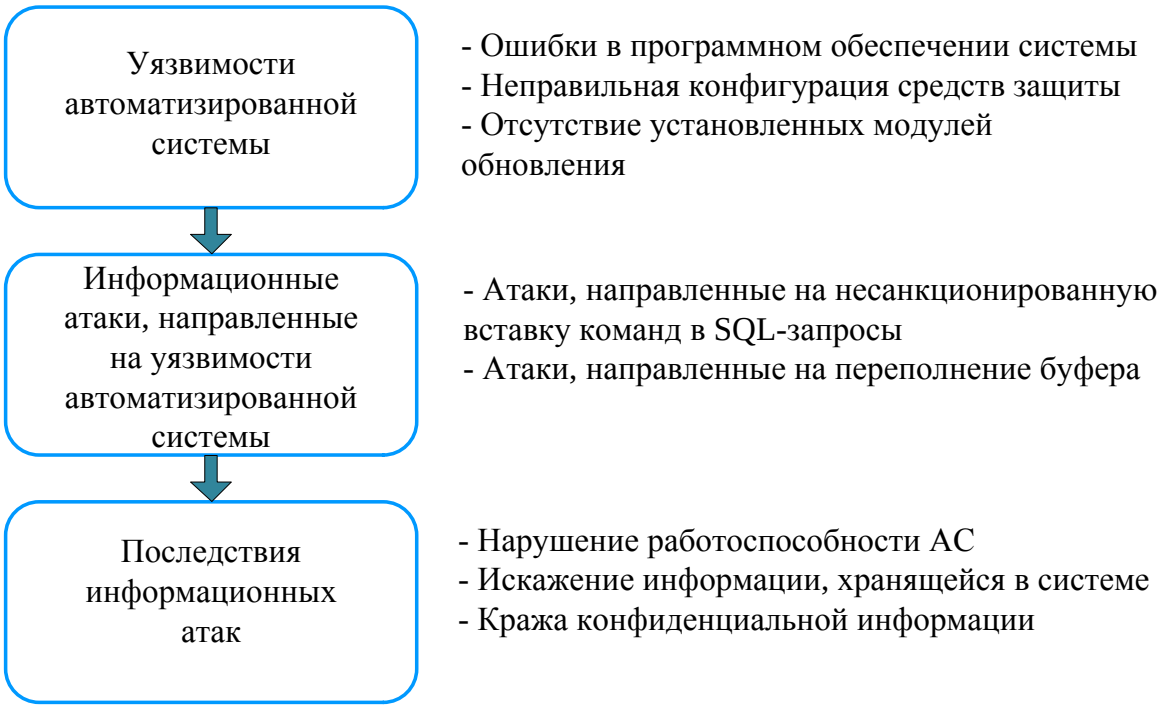


Рис. 1.4. Связь уязвимости, атаки и её возможных последствий

В настоящее время успешная работа предприятий, использующих те или иные информационные системы, зависит от того насколько хорошо они защищены от возможных угроз безопасности. Если организация не может быть уверенна, что ее конфиденциальная информация защищена от утечки или повреждения, ей стоит отказаться от использования инфокоммуникационных услуг, что в условиях современной экономики практически нереально, так как неизбежно приведет к потере возможности быстро реагировать на изменения рынка, а значит, к утрате конкурентоспособности. Поэтому современным предприятиям необходимо использовать автоматизированные системы и сети передачи данных и быть уверенными, что информационная безопасность обеспечена.

Помимо спроса коммерческих предприятий на сетевые услуги, растет и число пользователей сети Интернет, каждый из которых может быть инициатором хакерских атак или их жертвой. Доступ к данным в Интернет может получить абсолютно любой пользователь, если эти данные незащищены соответствующим образом, и умышленно повредить, уничтожить или перехватить и использовать их в своих целях. Кроме того данные могут быть повреждены непреднамеренно, из-за ошибок в

программном обеспечении, технических сбоев в сети. Все это представляет собой серьезную угрозу безопасности пользовательских данных. Добиться высокой степени защищенности можно только, если использовать передовые технологии защиты сети передачи данных. Вследствие распространения и увеличения доступности сетевых технологий, службы обеспечения безопасности стали важной частью работы сети.

Следовательно, когда есть необходимость работать в информационном пространстве и передавать данные через общедоступные сети, такие как Интернет, возникает острая потребность в надежной защите информации. Это позволяет утверждать, что проблема защиты информации является сегодня злободневной и актуальной.

2. Обеспечение информационной безопасности в сети Интернет

2.1 Понятие информационная безопасность

Существует система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. В качестве примера можно привести стандарт ISO 15408, известный как "Common Criteria".

Деятельность по обеспечению защиты информации организуется специальными государственными органами (подразделениями).

Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Служба внешней разведки Российской Федерации (СВР России);
- Министерство обороны Российской Федерации (Минобороны России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Основные национальные стандарты в области защиты информации

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.

ГОСТ Р 50.1.053-2005 Информационные технологии, основные термины и определения в области технической защиты информации.

ГОСТ Р 50922-2006, пункт 2.4.5 дает следующее определение безопасности информации:

Безопасность информации (данных): Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью»:

Информационная безопасность – механизм защиты, обеспечивающий:

конфиденциальность: доступ к информации только авторизованных пользователей;

целостность: достоверность и полноту информации и методов ее обработки;

доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

2.2 Риски и угрозы информационной безопасности

Информация, поддерживающие ее процессы, информационные системы и сетевая инфраструктура являются существенными активами организации. Конфиденциальность, целостность и доступность информации могут существенно способствовать обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации. Зависимость от информационных систем и услуг означает, что организации становятся все более уязвимыми по отношению к угрозам безопасности, которые могут быть определены как совокупность действий, направленных на нарушение одного из трёх свойств информации – *конфиденциальности*, *целостности* или *доступности*.

Угроза информационной безопасности (англ. information security treat) – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере. Уязвимость компьютерной системы – характеристика, которая делает возможным возникновение угрозы. Атака на компьютерную систему – это поиск и использование злоумышленником уязвимости системы. Другими словами, атака – это реализация угрозы.

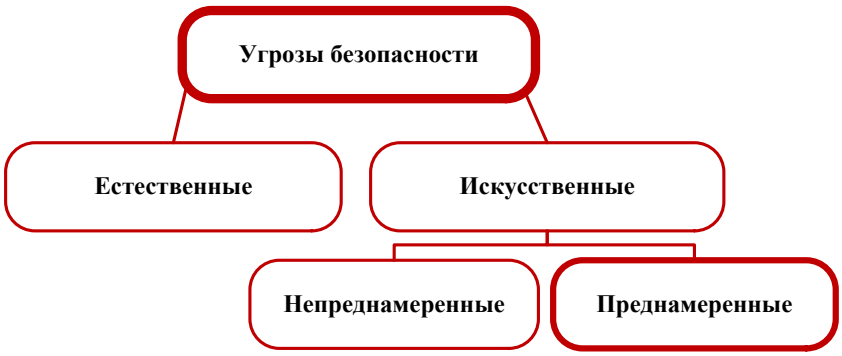


Рис. 2.1. Классификация угроз безопасности

Угрозы информационной безопасности делятся на два основных типа – это естественные и искусственные угрозы (рис. 2.1). К естественным угрозам относятся пожары, наводнения, удары молний и другие стихийные бедствия и явления, приводящие к аварийным ситуациям, возникновение которых не зависит от человека. Для обеспечения безопасности информации, необходимым условием является оборудование помещений, в которых находятся элементы системы (носители цифровых данных, серверы, архивы и пр.).

Искусственные угрозы – это угрозы, вызванные деятельностью человека. Они могут быть преднамеренными и непреднамеренными, (т.е. случайными). Система должна быть устойчива как к случайным, так и к преднамеренным враждебным воздействиям.

Угрозы, носящие случайный характер, или непреднамеренные угрозы, связаны с отказами, сбоями аппаратуры, ошибками операторов и т.п. Фактор появления таких угроз обусловлен ограниченной надежностью работы человека и техники.

Угрозы, носящие злоумышленный характер, или преднамеренные угрозы, вызваны, как правило, преднамеренным желанием субъекта осуществить несанкционированные изменения с целью нарушения корректного выполнения преобразований, конфиденциальности, достоверности и целостности данных. Данный класс угроз очень динамичен и постоянно пополняется.

К умышленным угрозам относятся:

- несанкционированный доступ к информации и сетевым ресурсам;
- раскрытие и модификация данных и программ, их копирование;
- раскрытие, модификация или подмена трафика вычислительной сети;
- разработка и распространение компьютерных вирусов, ввод в программное обеспечение логических бомб;
- кража магнитных носителей и расчетных документов;
- разрушение архивной информации или умышленное ее уничтожение;
- фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
- перехват и ознакомление с информацией, передаваемой по каналам связи, и т. п.

По расположению источника, угрозы делятся на внутренние и внешние.

Внутренние угрозы – угрозы исходящие от действий сотрудников (пользователей), допущенных к работе с системой, или сотрудников (администраторов и технического персонала), отвечающих за функционирование и обслуживание программного и аппаратного обеспечения, технических средств защиты.

Внешние угрозы – угрозы связанные с противоправной деятельностью преступных групп или отдельных лиц, не имеющих доступа к системе. К внешним преднамеренным угрозам можно отнести угрозы хакерских атак.

В общем случае выделяют три основных вида умышленных угроз безопасности: угрозы конфиденциальности, целостности и доступности.

Свойство конфиденциальности позволяет не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам. Нарушение конфиденциальности, это, прежде

всего, кража информации или перехват и расшифровка сетевых пакетов, т.е. анализ трафика. Обычно с реализацией этой угрозы и начинается большинство серьезных атак. Угроза нарушения целостности включает в себя любое умышленное изменение (модификацию или удаление) данных, хранящихся в системе. Доступность информации – это свойство информации быть доступной и используемой по запросу со стороны любого уполномоченного пользователя. Угроза отказа в обслуживании возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы.

Виды угроз случайного и преднамеренного характера приведены в табл. 2.1. На рис. 2.2 представлены программные угрозы безопасности.

Таблица 2.1

Несанкционированные действия	
Случайные	***Преднамеренные***
● Ошибки в программном обеспечении ● Ошибки в работе персонала ● Отказы и сбои оборудования ● Помехи в линиях связи из-за воздействий внешней среды ● Несанкционированный доступ: случайное ознакомление с конфиденциальной информацией посторонних лиц	● Нарушение конфиденциальности информации (кража данных, перехват и расшифровка сетевых пакетов) ● Нарушение целостности информации (модификация или удаление данных) ●Нарушение доступности информации (отказ в обслуживании) Методы воздействия: ● Вредоносные программы (вирусы, черви, троянские программы, программы-шпионы и др.). ● Программы, организующие DoS-атаки и другие атаки, спам, несанкционированный доступ (перехват и взлом паролей, взлом ОС, взлом приложений и протоколов (TCP/FTP/SSH/DNS/HTTP/SMTP/ протоколов маршрутизации)

Рис. 2.2. Программные угрозы безопасности

2.3 Способы обеспечения информационной безопасности в сети Интернет

Комплексный подход к защите информации предусматривает согласованное применение правовых, организационных и программно-технических мер, перекрывающих в совокупности все основные каналы реализации вирусных угроз. В соответствии с этим подходом в организации должен быть реализован следующий комплекс мер:

- меры по выявлению и устранению уязвимостей, на основе которых реализуются угрозы. Это позволит исключить причины возможного возникновения информационных атак;
- меры, направленные на своевременное обнаружение и блокирование информационных атак;
- меры, обеспечивающие выявление и ликвидацию последствий атак. Данный класс мер защиты направлен на минимизацию ущерба, нанесённого в результате реализации угроз безопасности.

Важно понимать, что эффективная реализация вышеперечисленных мер на предприятии возможна только при условии наличия нормативно-

методического, технологического и кадрового обеспечения информационной безопасности (рис. 2.3).

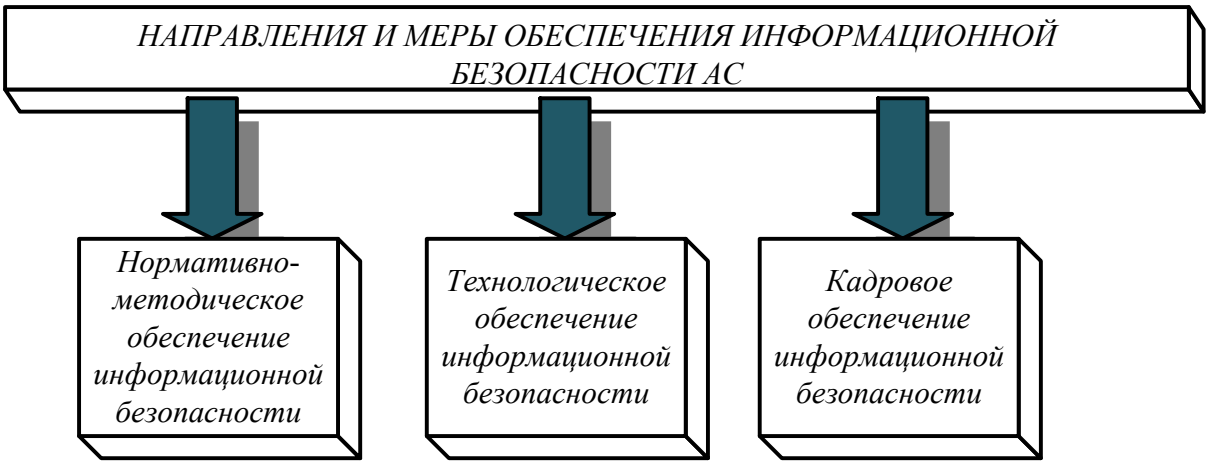


Рис. 2.3. Основные направления обеспечения информационной безопасности

Наибольшая эффективность будет получена в случае применения комплексной защиты вышеперечисленных способов.

Нормативно-методическое обеспечение информационной безопасности предполагает создание сбалансированной правовой базы в области защиты от угроз. Организационные средства защиты связаны с разработкой и внедрением на предприятиях нормативно-правовых документов, определяющих требования к информационной безопасности, такие как политика и концепция обеспечения информационной безопасности, должностные инструкции по работе персонала с АС и т.д.

В рамках кадрового обеспечения информационной безопасности в компании должен быть организован процесс обучения сотрудников по вопросам противодействия информационным атакам.

Программно-технические способы и средства обеспечения информационной безопасности являются основой системы защиты информации. Это совокупность алгоритмов, программ и протоколов, обеспечивающих шифрование, контроль за НСД, защиту от вредоносных программ и многое другое. На сегодняшний день можно выделить следующие основные виды технических средств защиты:

- средства криптографической защиты информации;

- средства разграничения доступа пользователей к ресурсам АС;
- средства межсетевого экранирования;
- средства анализа защищённости АС;
- средства обнаружения атак;
- средства антивирусной защиты;
- средства контентного анализа;
- средства защиты от спама.

Средства криптографической защиты информации представляют собой средства вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее конфиденциальности и контроля целостности.

Средства разграничения доступа предназначены для защиты от несанкционированного доступа к информационным ресурсам системы. Разграничение доступа реализуется средствами защиты на основе процедур идентификации, аутентификации и авторизации пользователей, претендующих на получение доступа к информационным ресурсам АС (рис. 2.4).

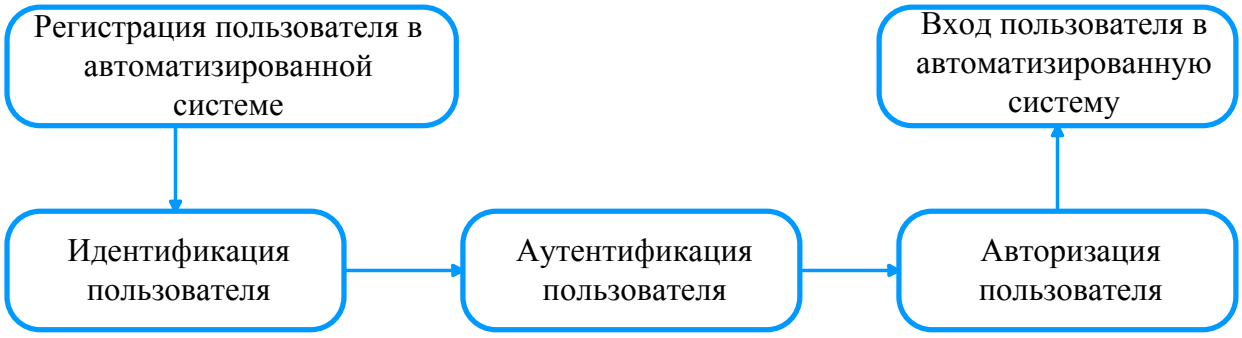


Рис. 2.4. Процедура входа пользователя в автоматизированную систему

Межсетевые экраны (МЭ) реализуют методы контроля за информацией, поступающей в АС и/или выходящей из АС, и обеспечения защиты АС посредством фильтрации информации на основе критериев, заданных администратором. Процедура фильтрации включает в себя анализ заголовков каждого пакета, проходящего через МЭ, и передачу его дальше по маршруту следования только в случае, если он удовлетворяет заданным

правилам фильтрации. При помощи фильтрования МЭ позволяют обеспечить защиту от сетевых атак путём удаления из информационного потока тех пакетов данных, которые представляют потенциальную опасность для АС.

Средства анализа защищённости предназначены для выявления уязвимостей в программно-аппаратном обеспечении АС.

Системы обнаружения атак представляют собой специализированные программные или программно-аппаратные комплексы, предназначенные для выявления информационных атак на ресурсы АС посредством сбора и анализа данных о событиях, регистрируемых в системе.

Средства антивирусной защиты предназначены для обнаружения и удаления вредоносного ПО, присутствующего в АС. К таким вредоносным программам относятся компьютерные вирусы, а также ПО типа «троянский конь», "spyware" и "adware".

Средства защиты от спама обеспечивают выявление и фильтрацию незапрошенных почтовых сообщений рекламного характера. В ряде случаев для рассылки спама используется вредоносное ПО, внедряемое на хосты АС и использующее адресные книги, которые хранятся в почтовых клиентах пользователей.

Средства контентного анализа предназначены для мониторинга сетевого трафика с целью выявления нарушений политики безопасности. В настоящее время можно выделить два основных вида средств контентного анализа – системы аудита почтовых сообщений и системы мониторинга Интернет-трафика. Системы аудита почтовых сообщений предполагают сбор информации о SMTP-сообщениях, циркулирующих в АС, и её последующий анализ с целью выявления несанкционированных почтовых сообщений, нарушающих требования безопасности, заданные администратором. Так, например, системы этого типа позволяют выявлять и блокировать возможные каналы утечки конфиденциальной информации через почтовую систему. Системы мониторинга Интернет-трафика предназначены для контроля доступа пользователей к ресурсам сети Интернет. Средства защиты данного типа позволяют заблокировать доступ пользователей к запрещённым Интернет-ресурсам, а также выявить попытку передачи конфиденциальной

информации по протоколу HTTP. Системы мониторинга устанавливаются таким образом, чтобы через них проходил весь сетевой трафик, передаваемый в сеть Интернет.

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

1) шифрование;
2) электронная цифровая подпись;
3) механизмы управления доступом;
4) механизмы контроля целостности данных;
5) механизмы аутентификации;
6) механизмы дополнения трафика;
7) механизмы управления маршрутизацией;
8) механизмы нотаризации. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

Общая схема решений для защиты от программных угроз представлена на рис. 2.5.

Рис. 2.5. Решения для защиты от программных угроз

2.4 Протоколы безопасности

В Интернет уже давно существует целый ряд комитетов, которые занимаются стандартизацией всех интернет-технологий. Эти организации, составляющие основную часть Рабочей группы инженеров Интернета (IETF), уже стандартизировали нескольких важных протоколов, тем самым ускорив их внедрение в Сети.

Secure Socket Layer (SSL) и Secure Shell Protocol (SSH) протоколы безопасности, работающие на транспортном уровне. Они обеспечивают безопасную передачу данных между клиентом и сервером. Оба протокола разработаны рабочей группой IETF по безопасности транспортного уровня (Transport Layer Security – TLS). Безопасный протокол передачи гипертекста (S-HTTP) предоставляет надежный механизм web-транзакций. Средство SOCKS является рамочной структурой, позволяющей приложениям клиент/сервер в доменах TCP и UDP удобно и безопасно пользоваться услугами межсетевого экрана. Протокол безопасности IP (IPSec) представляет собой набор стандартов поддержки целостности и конфиденциальности данных на сетевом уровне (в сетях IP). X.509 – это стандарт безопасности и аутентификации, который поддерживает структуры безопасности электронного информационного транспорта. Он определяет структуру данных цифрового сертификата и решает вопросы обращения общих ключей. X.509 является важнейшим компонентом инфраструктуры общих ключей (PKI).

В качестве средств обеспечения безопасности в сети Интернет наиболее популярны протоколы защищенной передачи данных, а именно SSL (TLS), SET, IPSec.

SSL (TLS)

Наиболее популярный сетевой протокол шифрования данных для безопасной передачи по сети. Представляет собой набор криптографических алгоритмов, методов и правил их применения. Позволяет устанавливать

защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи.

SET

SET (Security Electronics Transaction) – перспективный протокол, обеспечивающий безопасные электронные транзакции в Интернете. Он основан на использовании цифровых сертификатов по стандарту X.509 и предназначен для организации электронной торговли через сеть. Данный протокол является стандартом, разработанным компаниями "MasterCard" и "Visa" при участии "IBM", "GlobeSet" и других партнеров. С его помощью покупатели могут приобретать товары через Интернет, используя самый защищенный на сегодняшний день механизм выполнения платежей. SET – это открытый стандартный многосторонний протокол для проведения платежей в Интернете с использованием пластиковых карточек. Он обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных. SET можно считать стандартной технологией или системой протоколов выполнения безопасных платежей на основе пластиковых карт через Интернет.

IPSec

В 1994 году Совет по архитектуре Интернет (IAB) выпустил отчет «Безопасность архитектуры Интернет». В этом документе рассмотрены основные области применения дополнительных средств безопасности в сети Интернет, а именно защита от несанкционированного мониторинга, подмены пакетов и управления потоками данных. В числе первоочередных и наиболее важных защитных мер названы необходимость разработки концепции и основных механизмов обеспечения целостности и конфиденциальности потоков данных. Поскольку изменение базовых протоколов семейства TCP/IP вызвало бы полную перестройку сети Интернет, была поставлена задача обеспечения безопасности информационного обмена в открытых

телекоммуникационных сетях на базе существующих протоколов. Таким образом, начала создаваться спецификация Secure IP, дополнительная по отношению к протоколам IPv4 и входящая в стандарт IPv6. Она разрабатывается Рабочей группой IP Security IETF. В настоящее время IPSec включает три алгоритмо-независимых базовых спецификации, представляющих соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом уровне и защищает информацию на основе сквозного шифрования: независимо от работающего приложения, шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети. IPSec работает поверх обычных протоколов связи, поддерживая DES, MD5 и ряд других криптографических алгоритмов.

Обеспечение информационной безопасности на сетевом уровне с помощью IPSec включает:

- поддержку немодифицированных конечных систем;
- поддержку транспортных протоколов, отличных от TCP;
- поддержку виртуальных сетей в незащищенных сетях;
- защиту заголовка транспортного уровня от перехвата (предохранение от несанкционированного анализа трафика);
- защиту от атак типа «отказ в обслуживании».

Кроме того, IPSec имеет два важных преимущества:

- его применение не требует изменений в промежуточных устройствах сети;
- рабочие места и серверы не обязательно должны поддерживать IPSec.

Протокол IPsec доминирует в большинстве реализаций виртуальных частных сетей. В настоящее время на рынке представлены как программные реализации (например, протокол реализован в операционной системе Windows компании Microsoft), так и программно-аппаратные реализации

IPsec – это решения Cisco, Nokia. Несмотря на большое число различных решений, все они довольно хорошо совместимы друг с другом.

Сравнение протоколов IPSec и SSL представлено в таблице 2.2.

Таблица 2.2

Особенности	***Ipsec***	***SSL***
Аппаратная зависимость	*Да*	*Да*
Код	*Не требуется изменений для приложений. Может потребовать доступ к исходному коду стека TCP/IP*	*Требуются изменения в приложениях. Могут потребоваться новые DLL или доступ к исходному коду приложений.*
Защита	*IP-пакет целиком. Включает защиту для протоколов верхних уровней.*	*Только уровень приложений.*
Фильтрация пакетов	*Основан на аутентифицированных заголовках, адресах отправителя и получателя, и т.п. Простая и дешевая, подходит для роутеров.*	*Основана на содержимом и семантике высокого уровня. Более сложная.*
Платформы	*Любые системы, включая роутеры.*	*В основном, конечные системы (клиенты/серверы), а также брэндмауэры.*
Firewall/VPN	*Весь трафик защищен.*	*Защищен только трафик уровня приложений.*
Прозрачность	*Для пользователей и приложений.*	*Только для пользователей.*

3. Протоколы IPSec

3.1. Структура и принцип работы протоколов IPSec

Корпорация Microsoft предоставляет технологию IPSec, встроенную в операционную систему Windows, которая позволяет защищать сеть, как от внешних, так и от возможных внутренних атак. IPSec (Internet Protocol Security) — система стандартов, направленная на установление и поддержание защищённого канала для передачи данных. IPSec предусматривает аутентификацию при установлении канала, шифрование передаваемых данных и распространение секретных ключей, необходимых для работы протоколов аутентификации и шифрования. Средства IPSec реализуют защиту содержимого пакетов IP, а также защиту от сетевых атак путём фильтрации пакетов и использования только надёжных соединений.

Систему открытых стандартов Internet Protocol Security (IPSec) предложила Рабочая группа инженеров Интернета (IETF). Протоколы IPSec обеспечивают защиту сетей, используя для этого криптографические протоколы безопасности и динамическое управление ключами.

Стек протоколов IPsec действует на сетевом уровне, защищая и аутентифицируя IP-пакеты между устройствами, участвующими в соединении. Он не привязан к конкретным алгоритмам шифрования, аутентификации и безопасности и технологиям генерации ключей, может использоваться для защиты одного или нескольких «путей» между парой хостов, между парой шлюзов безопасности или между шлюзом безопасности и хостом.

Службы безопасности IPsec

Конфиденциальность – шифрование передаваемых данных с целью их защиты от несанкционированного просмотра.

Целостность данных – гарантирует, что данные в процессе передачи через Интернет не были изменены. IPsec гарантирует целостность данных с помощью контрольных сумм, простой проверки по избыточности.

Аутентификация – гарантирует, что соединение установлено с нужным партнером. Получатель может аутентифицировать источник пакета, гарантируя и сертифицируя подлинность источника информации.

Защита от повторения пакетов (защита от replay-атак) – гарантирует, что каждый пакет уникален и не дублируется. Защита пакетов IPsec обеспечивается за счет сравнения номеров последовательности полученных пакетов со скользящим окном хоста назначения или шлюза безопасности. Пакет с номером последовательности ниже скользящего окна считается запоздавшим или дублированным. Запоздавшие или дублированные пакеты отбрасываются.

IPsec поддерживает две формы целостности: целостность, не зависящая от соединения и частичную целостность последовательности. Целостность, не зависящая от соединения, является сервисом безопасности, который определяет модификацию конкретной IP датаграммы. Частичная целостность последовательности является anti-reply сервисом, с помощью которого определяется получение дубликатов IP датаграмм.

IPsec использует два протокола для обеспечения безопасности трафика – Authentication Header (AH) и Encapsulating Security Payload (ESP) (рис. 3.1).

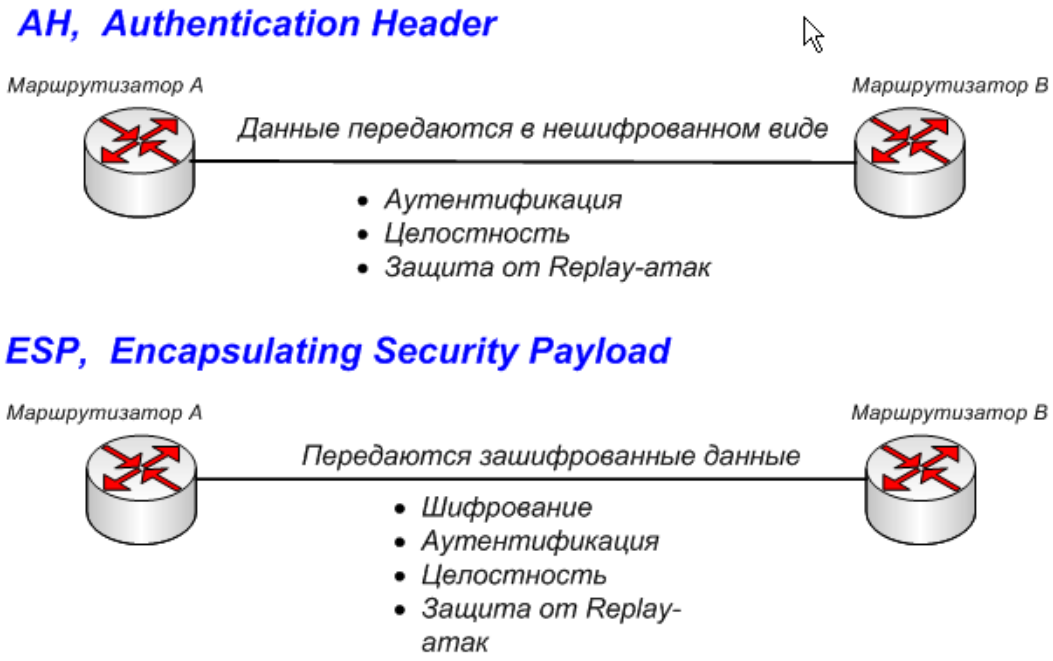


Рис. 3.1. Протоколы безопасности IPSec

Authentication Header (AH) обеспечивает аутентификацию и целостность IP-пакетов, передаваемых между двумя системами, и дополнительно может обеспечивать anti-replay сервис. AH не обеспечивает конфиденциальности (шифрования) пакетов. Данные передаются в незашифрованном виде. AH - это протокол, который следует использовать, когда конфиденциальность не требуется или не разрешена.

Encapsulating Security Payload (ESP) протокол обеспечивает конфиденциальность (шифрование), целостность и аутентификацию данных. Хотя использование шифрования и аутентификации в протоколе ESP необязательно, необходимо выбрать хотя бы одну из этих функций. Так же ESP может дополнительно обеспечивать anti-replay сервис.

Протокол **IKE (Internet Key Exchange)** используется для определения способа инициализации защищённого канала, кроме того, IKE определяет процедуры обмена и управления секретными ключами соединения.

IPsec использует существующие алгоритмы шифрования, аутентификации и обмена ключами. Некоторые из стандартных алгоритмов, используемых IPsec, перечислены ниже:

- **DES:** Выполняет шифрование и дешифровку данных.
- **3DES:** Использует 3 различных 56 битных ключа (DES encrypt, DES decrypt, DES encrypt)**,** предлагает значительное увеличение криптографической сложности по сравнению с 56-битным алгоритмом DES.
- **AES**: Обеспечивает повышенную сложность шифрования в зависимости от используемой длины ключа, использует ключ от 128 - 256 бит.
- **MD5:** Аутентифицирует данные пакета с использованием 128-битного общего секретного ключа.
- **SHA-1:** Аутентифицирует данные пакета с использованием 160-битного общего секретного ключа.
- **DH**: Для обмена секретными ключами в IPsec используется алгоритм

Diffie-Helman, позволяет двум сторонам формировать общий секретный ключ, используемый для алгоритмов шифрования и хэширования по небезопасному каналу связи.

IPsec предоставляет структуру, администратор выбирает алгоритмы, на базе которых реализуются службы безопасности в рамках этой структуры. На рис. 3.2 приведена структура IPsec.

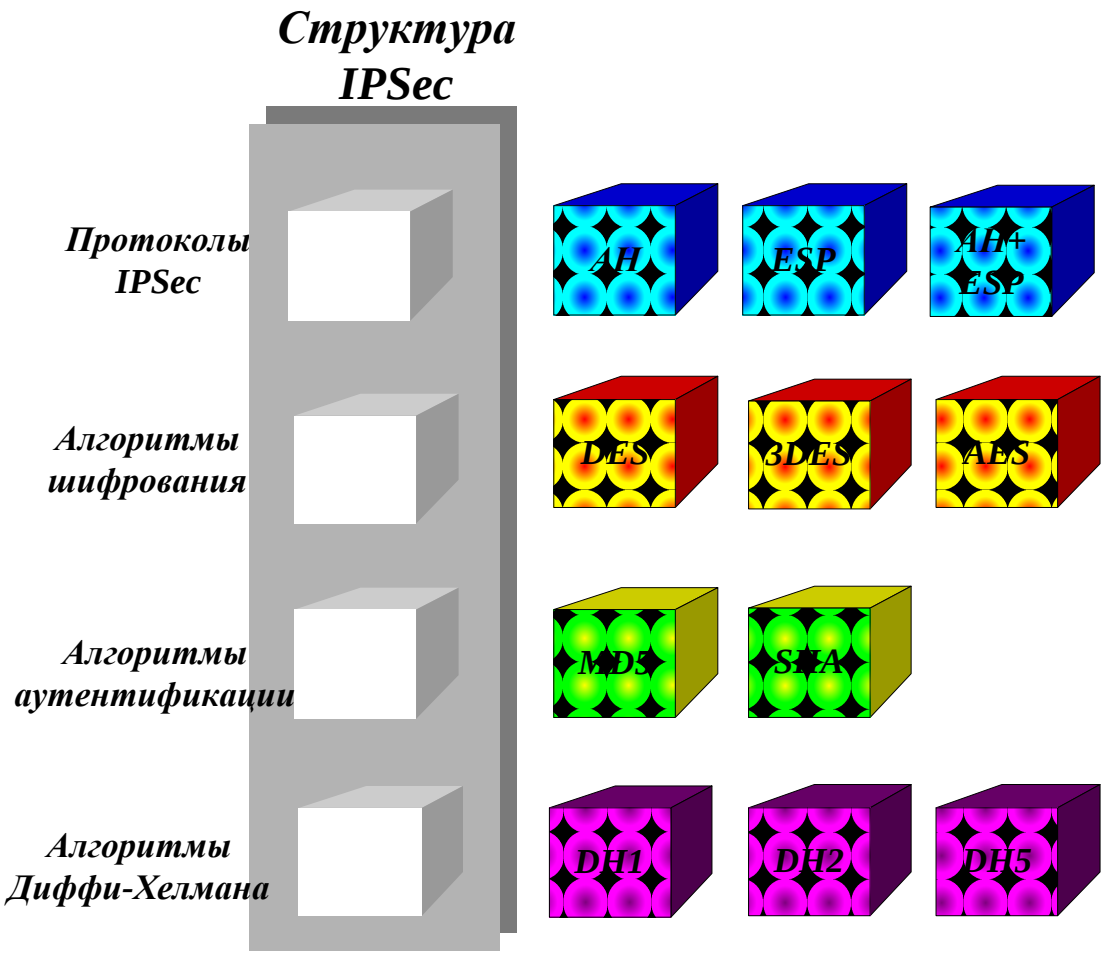


Рис. 3.2. Структура IPsec

IPsec обеспечивает сервисы безопасности на IP-уровне, выбирая нужные протоколы безопасности, определяя алгоритмы, используемые сервисами, и предоставляя все криптографические ключи требуемым сервисам.

Общий набор параметров безопасности IPSec называется политикой IPSec (рис. 3.3). Политика состоит из набора правил, определяющих обработку сетевого трафика. Каждое правило содержит относящиеся к нему

набор фильтров и действия, которые данное правило будет производить с пакетом, соответствующим условиям фильтра. В качестве параметров фильтров могут быть заданы IP-адреса, адреса сети или полное доменное имя отправителя и получателя пакета, тип IP-протокола (ICMP, TCP, UDP и т. д.), номера TCP и UDP портов отправителя и получателя.

Правило также определяет, какие методы аутентификации потребуются для обмена данными между хостами. В качестве действия задается один из следующих параметров - пакет блокируется (Block), передается без применения IPSec (Permit) и передается с применением IPSec (Negotiate Security, согласование безопасности).

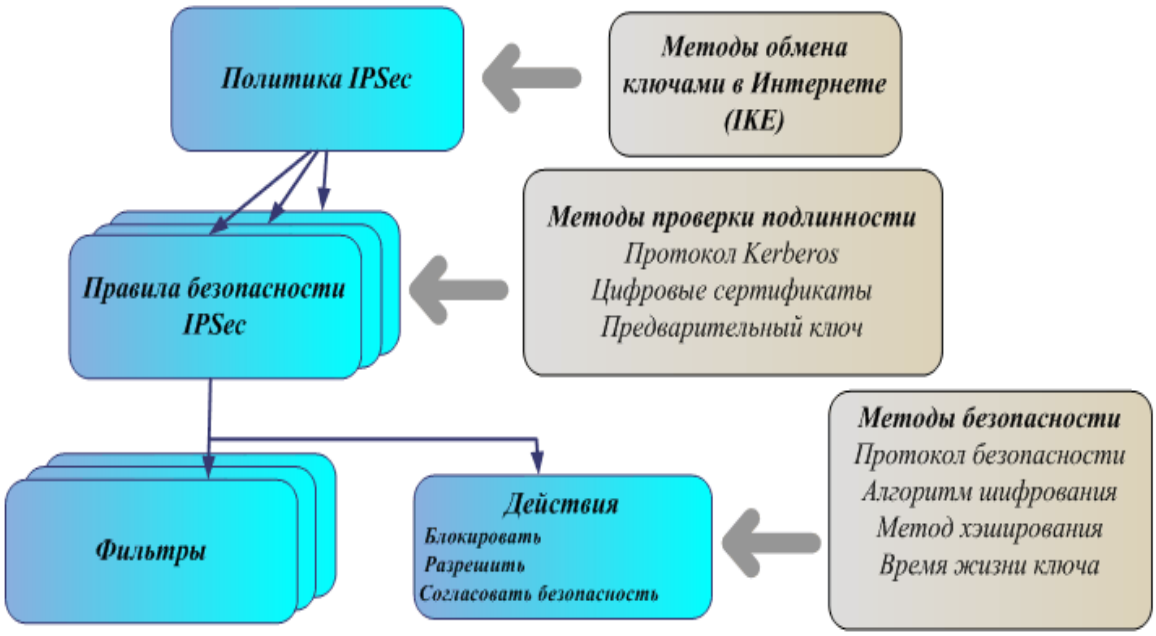


Рис.3.3. Политика IPSec

Протокол IKE позволяет установить доверительные отношения между хостами, согласовать параметры безопасности и динамического создания общего ключа. Соглашение о параметрах безопасности, под управлением которых создается ключ, называют ассоциацией безопасности (SA, security association). Протокол IKE, включающий ISAKMP и Oakley, использует рамочную структуру ISAKMP для поддержки подмножества режимов обмена ключами Oakley.

Протокол управления ключами Ассоциации безопасности Интернет (Internet Security Association Key Management Protocol — ISAKMP) определяет процедуры установления, согласования, изменения и удаления SA. Все процессы согласования параметров проходят через *ISAKMP*, такие как header authentication и payload encapsulation. *ISAKMP* выполняет аутентификацию пира, но не включает обмен ключами.

Протокол определения ключей Oakley Key Determination Protocol пользуется гибридным методом Диффи-Хеллмана, чтобы создать ключи сессии Интернет для центральных компьютеров и маршрутизаторов. Протокол Oakley решает важную задачу обеспечения полной безопасности эстафетной передачи данных. Он основан на криптографических методах. Полная защита эстафетной передачи означает, что если хотя бы один ключ раскрыт, раскрыты будут только те данные, которые зашифрованы этим ключом. Что же касается данных, зашифрованных последующими ключами, они останутся в полной безопасности.

Понятие ассоциации безопасности SA является фундаментальным в IPsec. Ее предназначение — защитить процесс обмена информацией между двумя сообщающимися сторонами. SA включает следующие данные (рис. 3.4):

1. IP-адрес получателя.
2. Протокол безопасности, используемый при передаче данных.
3. Секретные ключи, применяемые при шифрации.
4. Метод форматирования, определяющий, каким образом создаются заголовки и то, какая часть этих заголовков и данных пользователя будет защищена в процессе передачи данных.
5. Индекс параметров защиты (Security Parameter Index — SPI) — один из идентификаторов SA. Он определяет то, как принимающая сторона будет обрабатывать поступающий поток данных.

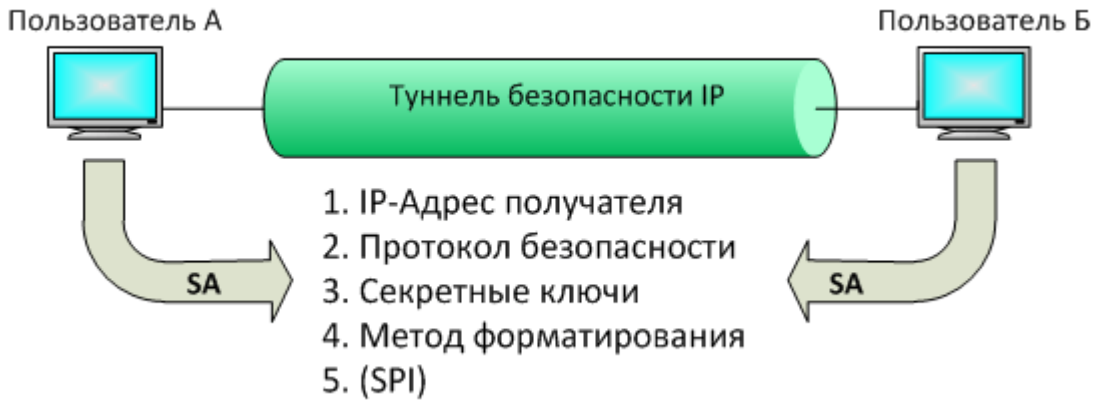


Рис. 3.4. Ассоциация безопасности и туннель IP

SA - это совокупность параметров соединения, которые дают возможность сервисам обеспечивать безопасный трафик. SA является однонаправленной, т.е. определяет выполняемые действия при передаче данных только в одном направлении. Таким образом, при двунаправленном соединении должны использоваться две SA, по одной на каждое направление. Основной идеей двусторонней передачи данных является использование двух SA с одинаковыми метахарактеристиками, но различными ключами. Эта идея известна под названием двунаправленных SA. SA могут быть сгруппированы вместе (пакет SA) для обеспечения необходимых свойств защиты данных. SA определяет использование протоколов безопасности AH или ESP. Если к потоку трафика применяются оба протокола, то для каждого из них создается своя SA. Правилом для таких пакетов SA является одинаковый IP-адрес получателя во всех SA пакета.

SA однозначно определяется тройкой, состоящей из Security Parameter Index (SPI), IP Destination Address (адресом назначения) и идентификатора протокола безопасности (AH или ESP).

Рассмотрим типичные для Интернета ассоциации безопасности, необходимые для работы IPSec-совместимых узлов и шлюзов безопасности.

1. Ассоциация безопасности и соответствующий ей туннель, соединяющий два хоста, обеспечивая таким образом сквозную защиту

передаваемых данных. В данном случае Интернет (или Интранет) не имеет понятия об этой ассоциации безопасности и не участвует в ней (рис. 3.5, а).

Рис. 3.5, а

2. Ассоциация безопасности и соответствующий ей туннель располагаются между двумя шлюзами безопасности. Хосты освобождены от необходимости применения ассоциации безопасности, и предполагается, что их связь со шлюзами осуществляется по безопасным соединениям. В этом случае может использоваться одна SA для всего обмена данными внутри, например, группы смежных подсетей (рис. 3.5, б).

Рис. 3.5, б

3. Туннель используется как между шлюзами безопасности, так и для прямой связи между хостами (рис. 3.5, в).

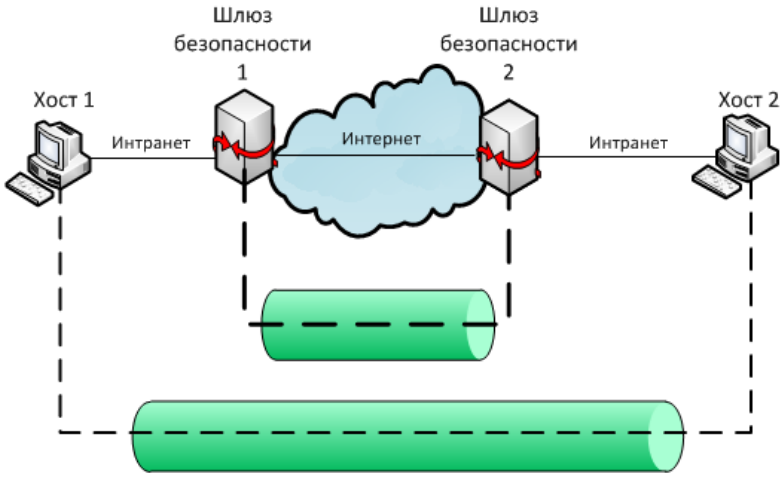


Рис. 3.5, в

4. Ситуация, когда удаленный хост (Хост 1) соединяется с организацией через Интернет или когда сервер находится позади шлюза безопасности. Соединение происходит через Интернет. Примером такого случая могут быть пользователи сотовых телефонов (рис. 3.5, г).

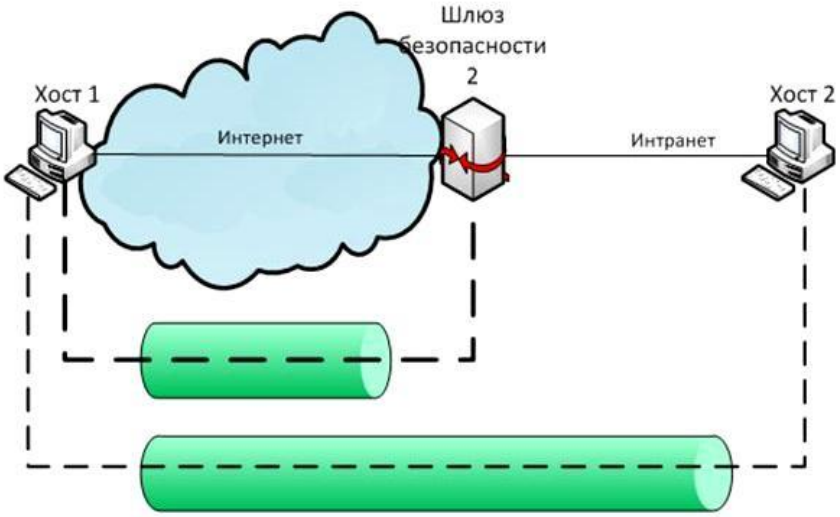


Рис. 3.5, г

Определены два режима SA: режим транспорта и режим туннелирования. Режимы работы протоколов IPSec обеспечивают различный уровень безопасности и применимы в различных условиях.

Транспортный режим обеспечивает безопасное соединение между двумя компьютерами, как правило, объединенными единой (локальной) сетью. При использовании транспортного режима обеспечивается защита поля полезных данных IP, содержащего протоколы транспортного уровня

(TCP, UDP), которое, в свою очередь, содержит информацию прикладных служб. Транспортный режим служит для защиты данных преимущественно внутри одной сети, безопасность которой не может быть надежно обеспечена другими способами без значительных затрат, либо когда требуется высокий уровень безопасности, что достигается совместным использованием различных протоколов. В качестве примеров можно назвать беспроводные сети, а также кабельные сети, покрывающие большие территории. Транспортный режим является режимом для IPSec по умолчанию.

Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

Режим туннелирования

Если хотя бы одним из концов соединения является шлюз безопасности, то SA обязательно должна выполняться в туннелирующем режиме. Два хоста могут при желании так же устанавливать режим туннелирования. Туннельный режим протокола IPsec используется в тех случаях, когда требуется защитить данные (в том числе заголовки IP), передаваемые через общедоступную сеть. Примерами могут служить связи между удаленными подразделениями компании.

Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. При использовании этого режима весь пакет IP инкапсулируется в заголовок AH или ESP и дополнительный заголовок IP. Заголовок протокола безопасности расположен между внешним и внутренним IP заголовком. IP-адреса внешнего заголовка IP указывают конечные точки туннеля, а IP-адреса инкапсулированного заголовка IP указывают исходную точку и точку назначения пакета. Благодаря этому обеспечивается защита всего IP-пакета, включая заголовок IP.

При этом, адресные поля внешнего заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном

организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

На рис. 3.6,а показана структура исходного IP-пакета, на рис.3.6,б показан пакет транспортного режима, а на рис.3.6,в — туннельного. В случае использования ESP в пакетах появляется два дополнительных поля: ESP-концевик и значение MAC. MAC – это код идентификации сообщения, для которого используется значение проверки целостности ICV, для чего IPSec требует реализации процедур HMAC-MD5 и HMAC-SHA-1. Эти поля помещаются после поля L_7, которое представляет обмен данными прикладного уровня (FTP, HTTP и др.).

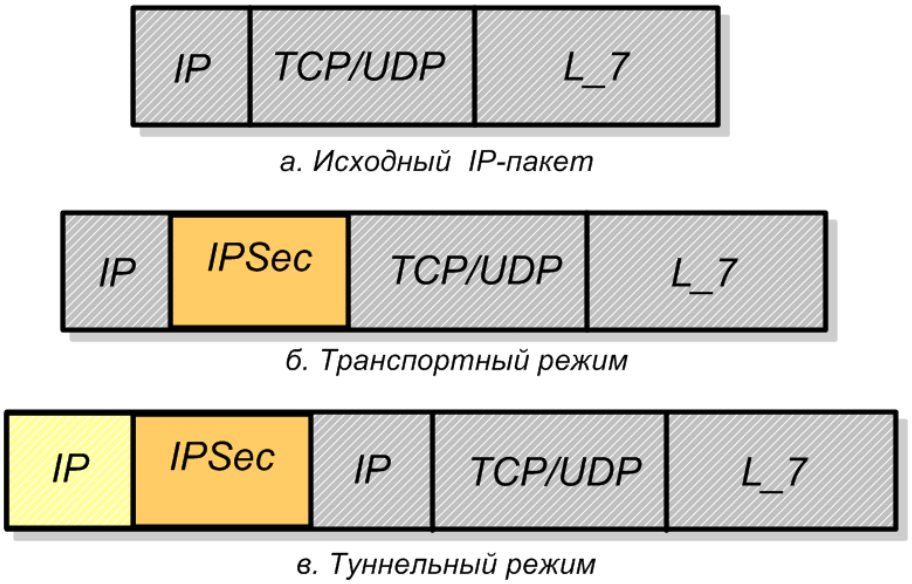


Рис. 3.6. Режимы IPSec.

Базы данных IPSec

IPSec нуждается в изрядном количестве информации для обеспечения безопасности пользователей. SA определяет, какие услуги по обеспечению безопасности предоставляются пользователю. Такие требования к безопасности хранятся в двух базах данных: БД ассоциаций безопасности (SAD) и БД Политики Безопасности (SPD). Они являются хранилищами

информации для IPSec, и их содержимое, сконфигурированное администратором безопасности, управляет «поведением» IPSec.

SAD содержит параметры, которые связаны с каждой активной ассоциацией безопасности. Поскольку SA являются однонаправленными, в SAD хранятся пары SA, по одной для каждого направления.

В базе данных SAD содержится:

- AH: алгоритм аутентификации.
- AH: аутентификационный секретный ключ (authentication secret).
- ESP: алгоритм шифрования.
- ESP: секретный ключ шифрования.
- ESP: разрешение аутентификации (yes/no).
- Параметры обмена ключами.
- Ограничения маршрутизации.
- IP политика фильтрации.

SPD описывает политики, которые определяют характер обработки всего IP-трафика, т.е. задают, какой поток данных и каким образом этот поток данных обрабатывается (отвергнуть, обойти IPSec, применить IPSec), как обрабатывать входящий и исходящий потоки. Таким образом, к этой базе данных обращаются для обработки каждого входящего и исходящего пакета. Каждая запись в SPD определяется набором значений полей IP и протокола верхнего уровня, называемых селекторами. Эти селекторы используются для фильтрации исходящего трафика, для того чтобы поставить его в соответствие с определенной SA. Обработка исходящих IP-пакетов производится в следующей последовательности.

- Сравниваются значения соответствующих полей в пакете (селекторные поля) с SPD и находится нуль или более SA.
- Определяется SA (если таковая имеется) для пакета и связанный с ней SPI.
- Выполняются необходимые операции IPsec (AH или ESP).

SPD запись определяется следующими селекторами:

- *IP-адрес места назначения*.
- *IP-адрес отправителя*.
- *UserID*. Идентификатор пользователя служит для идентификации политики, соответствующей имени пользователя или системы.
- *Уровень чувствительности данных*.
- *Протокол транспортного уровня*. Это значение извлекается из поля следующий заголовок пакета IPv4 или IPv6. Это может быть индивидуальный код протокола, список кодов протокола или диапазон таких кодов.
- *Протокол IPsec* (AH, ESP или AH/ESP). Извлекается (если присутствует) из поля следующий заголовок пакета IPv4 или IPv6.
- *Порты отправителя и получателя*. Это могут быть индивидуальные номера портов TCP или UDP, список портов или произвольный порт.
- *Класс IPv6*. Значение класса получается из заголовка IPv6. Это может быть специфическое значение и код произвольного класса.
- *Метка потока IPv6*. Значение метки потока получается из заголовка IPv6. Это может быть специфическое значение метки потока или код произвольной метки.
- *Тип сервиса IPv4*. Значение ToS получается из заголовка IPv4. Это может быть специфическое значение ToS или указатель произвольного значения.

Каждый сетевой интерфейс, для которого необходима обработка IPsec, требует определения баз данных для входящего и исходящего трафика.

Протокол IPSec состоит из трех основных компонентов: службы агента политики IPSec, обмена ключами в Интернете (IKE), а также драйвера IPSec.

Этапы работы IPSec:

1. **Начало процесса IPSec.** Приложение, трафику которого требуется защита IPSec, начинает процесс обмена данными IKE-протокола.

2. **Первая фаза IKE.** Главной целью обмена данными, происходящего в первой фазе IKE, является аутентификация сторон IPSec и создание

защищенного канала между сторонами, позволяющего начать обмен IKE. Основным результатом этой фазы является согласование параметров ассоциаций защиты IKE (SA) между сторонами с целью создания защищенного канала для последующих обменов IKE.

3. **Вторая фаза IKE.** IKE-процесс ведет согласование параметров ассоциации безопасности IPSec, устанавливает соответствующие ассоциации безопасности IPSec с целью создания туннеля IPSec.

4. **Передача данных.** Происходит обмен данными между сообщающимися сторонами IPSec, который основывается на параметрах IPSec и ключах, хранимых в базе данных ассоциаций безопасности.

5. **Завершение работы IPSec.** Ассоциации безопасности IPSec завершают свою работу либо в результате их удаления, либо по причине превышения предельного времени их существования.

Как происходит обмен данными между двумя хостами с применением IPSec, показано на рис. 3.7.

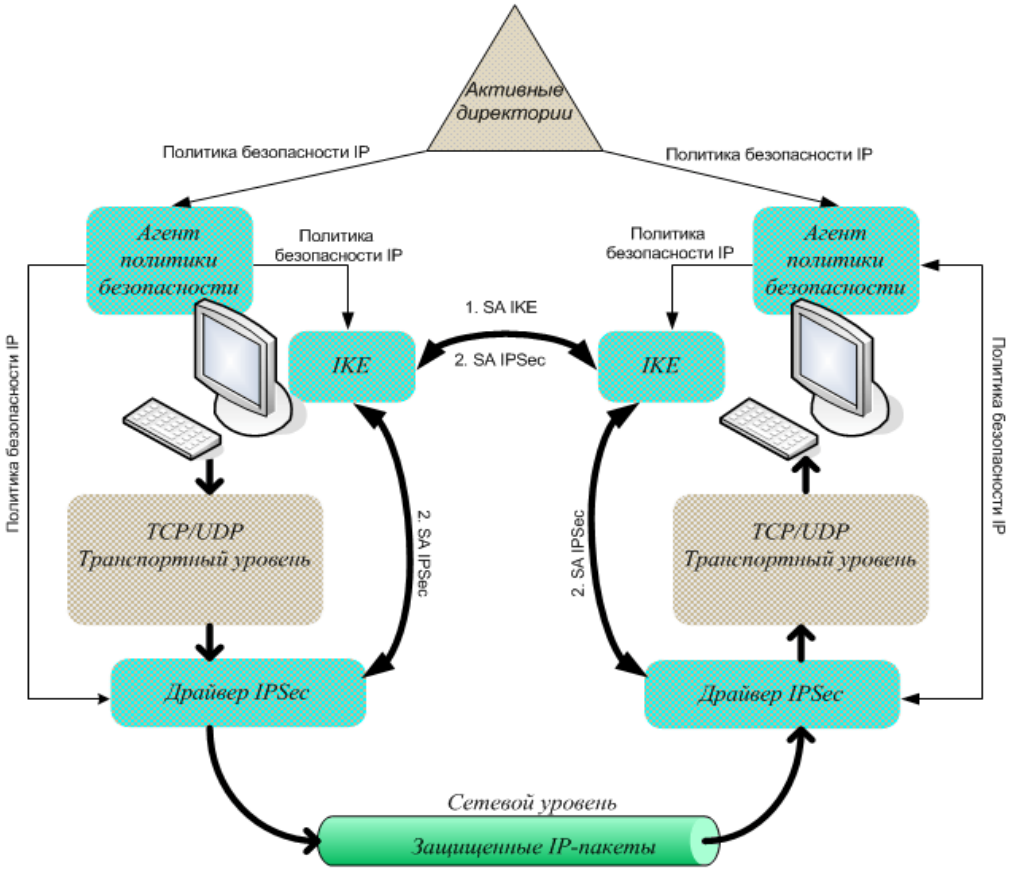


Рис. 3.7. Обмен данными между хостами

Активные директории (Active Directory, AD) — реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows NT. Active Directory позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики, устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

На пользовательском уровне процесс «засекречивания» IP-пакетов совершенно прозрачен. Пользователь запускает приложение, использующее протокол TCP/IP, например, FTP, и пересылает данные другому пользователю.

Агент политики IPSec предназначен для загрузки сведений политик IPSec, их передачи в другие компоненты IPSec, а также для обеспечения работы служб безопасности, которым необходимы данные сведения. Агент политики IPSec представляет собой службу, которая расположена на каждом компьютере с операционной системой Windows и отображается в списке служб как «Служба IPSec». Эта служба выполняет следующие действия: загружает назначенную политику IPSec, опрашивает о наличии изменений в конфигурации самой политики, отправляет сведения назначенной политики IPSec в драйвер IPSec.

Обмен ключами в Интернете. Перед началом безопасного обмена данными, между двумя компьютерами должно быть установлено безопасное подключение. Для создания соглашения между двумя компьютерами существует метод сопоставления безопасности и разрешения обмена ключами, который называется обменом ключами в Интернете (Internet Key Exchange, IKE). Данный метод централизует управление сопоставлением

безопасности, тем самым сокращая время подключения, а также создаёт общие секретные ключи, которые используются для защиты и управления данными.

Для обеспечения успешной и безопасной связи IKE выполняет операцию в два этапа. На первом этапе (первая фаза IKE) два компьютера создают безопасный канал с проверкой подлинности, который называется сопоставлением безопасного режима. Во время этого этапа сначала выполняется согласование политики безопасности основного режима при помощи алгоритма шифрования (DES или 3DES), алгоритма проверки целостности (MD5 или SHA1), группы Диффи-Хелмана или метода проверки подлинности (Kerberos, сертификат или предварительный ключ). После этого на первом этапе осуществляется обмен сведениями, которые необходимы алгоритму определения ключа Диффи-Хелмана для создания общего секретного ключа. После обмена на каждом компьютере создается основной ключ, используемый для защиты проверки подлинности. Последним шагом на данном этапе является проверка подлинности. В этот момент компьютеры выполняют проверку подлинности при обмене ключами Дифи-Хелмана. Все сведения учетной записи хешируются и шифруются с помощью ключей, созданных по результатам обмена сведениями о группе Дифи-Хелмана на предыдущем шаге.

Ассоциация безопасности IKE определяет параметры обмена IKE: используемый метод аутентификации, алгоритмы шифрования и хэширования, используемая группа Диффи-Хеллмана, максимальное время существования ассоциации защиты IKE в секундах или килобайтах и совместно используемые секретные значения ключей для алгоритмов шифрования.

Таким образом, в ходе первой фазы IKE выполняются следующие действия (рис.3.8):

Рис. 3.8. Первая фаза IKE

Первая фаза IKE может выполняться в одном из двух режимов: основном (Main Mode) и энергичном (Aggressive Mode). В энергичном режиме меньше число обменов параметрами между сторонами, и число пересылаемых при этом пакетов, в результате чего необходимо меньше времени для установки сеанса IPSec. Однако, недостатком использования энергичного режима является то, что обе стороны обмениваются информацией до того, как создан защищенный канал.

На втором этапе обмена ключами в Интернете (вторая фаза IKE) сопоставления безопасности согласуются от имени драйвера IPSec. Вторая фаза IKE выполняется в быстром режиме, после того как в результате первой фазы IKE создается защищенный туннель. Во время данного этапа выполняются следующие шаги: идет согласование политики, во время которого компьютеры IPSec обмениваются такими требованиями к защите передачи данных, как протокол IPSec, а именно AH или ESP, алгоритм хеширования для проверки подлинности (MD5 или SHA1), а также, если запрашивается, алгоритм шифрования (DES или 3DES). Далее происходит

обновление или обмен материалом для создания ключа сеанса. В это время IKE обновляет сведения о ключе, после чего происходит создание новых общих ключей для проверки подлинности и шифрование пакетов. И, напоследок, идет процесс сопоставления безопасности, после чего ключи передаются в драйвер IPSec вместе с SPI.

Таким образом, задачей второй фазы IKE является согласование параметров ассоциации безопасности IPSec с целью создания туннеля IPSec. В этой фазе выполняются следующие действия (рис. 3.9):

Рис. 3.9. Вторая фаза IKE

Драйвер IPSec получает список активных фильтров от агента политики IPSec и после чего сверяет все входящие и исходящие пакеты с фильтрами в текущем списке. В том случае, если пакет полностью совпадает с данным фильтром, то к нему применяется действие самого фильтра. Если же пакет не соответствует ни одному доступному фильтру, то он возвращается в драйвер TCP/IP для приема или передачи без всяких изменений. Как для обработки входящего, так и исходящего трафика применяются ключи и сопоставление

безопасности быстрого режима. В свою очередь, драйвер IPSec содержит в своей базе данных все текущие сопоставления безопасности быстрого режима и для правильного применения сопоставлений безопасности и пакетов использует индекс параметров безопасности.

После того, как согласование безопасности будет завершено, драйвер IPSec на отправляющем компьютере принимает от IKE сопоставление безопасности, которое содержит ключ сеанса. Затем драйвер IPSec в базе данных находит исходящее сопоставление безопасности и вставляет индекс параметров безопасности в заголовок AH или ESP. После этого он подписывает пакеты и отправляет их на уровень IP для пересылки на компьютер назначения.

После завершения второй фазы IKE и создания ассоциаций защиты IPSec в быстром режиме, начинается обмен информацией через туннель IPSec,связывающий стороны IPSec. Пакеты шифруются и дешифруются с помощью алгоритмов шифрования и ключей, указанных ассоциацией защиты IPSec.

При получении IP-пакетов, которые считаются небезопасными, драйвер IPSec всегда их сверяет со списком фильтров, задающим туннели IPSec, а затем со всеми фильтрами передачи данных между сторонами подключения.

Ассоциация безопасности IPSec задает также предел времени своего существования в килобайтах передаваемых данных или в секундах. Она имеет специальный счетчик, значение которого уменьшается на единицу за каждую секунду или после передачи каждого килобайта данных.

По окончании передачи всех данных согласования быстрого режима удаляются, однако сопоставление основного режима остается действующим какое-то время. Этот интервал (время жизни) задается в настройках IPSec-политики. Он позволяет при возобновлении передачи данных выполнять

лишь согласование быстрого режима, экономя время, необходимое для установления защищенного соединения.

3.2. Протоколы обеспечения безопасности AH и ESP

В IPSec определены два протокола обеспечения безопасности AH и ESP.

Протокол AH (Authentication Header - заголовок аутентификации). Протокол защиты, обеспечивающий аутентификацию (удостоверение происхождения данных или проверку подлинности), целостность и, если это определено ассоциацией безопасности, защиту от атак воспроизведения. Протокол AH действует как цифровая подпись и гарантирует, что данные в пакете IP не будут несанкционированно изменены, то есть обеспечивает целостность, не зависящую от соединения (connectionless integrity). Протокол AH не обеспечивает сервис шифрования и дешифрования, поэтому данные остаются доступными для чтения. AH подписывает пакеты используя алгоритмы хеширования с ключами (MD5, а в более современных реализациях SHA1).

Протокол ESP (Encapsulating Security Payload – вложенные защищенные передаваемые данные). Протокол защиты, обеспечивающий конфиденциальность (шифрование), аутентификацию и целостность данных, не зависящую от соединения, а также, в качестве опции, сервис защиты от атак воспроизведения. В случае ESP по крайней мере одна из этих функций должна быть реализована. Полный набор выполняемых действий определяется настройками ассоциации безопасности.

В ESP аутентификация и целостность, независящая от соединения, являются связанными операциями и называются идентификацией. Они предлагаются как необязательное дополнение к операциям шифрации. ESP может выполнять шифрацию отдельно от других операций, но такое отделение от операций по обеспечению сохранности данных и их идентификации может привести к атакам на передаваемые данные. Защита от повторения доступна только в случае, когда используется аутентификация, и ее применение

определяет получатель. Конфиденциальность потока данных обеспечивается только при использовании туннельного режима.

Оба протокола являются средствами контроля доступа и могут применяться как раздельно, так и вместе. Эти протоколы поддерживают IPv4 и IPv6. Форматы заголовков представлены на рис. 3.10. и рис.3.11.

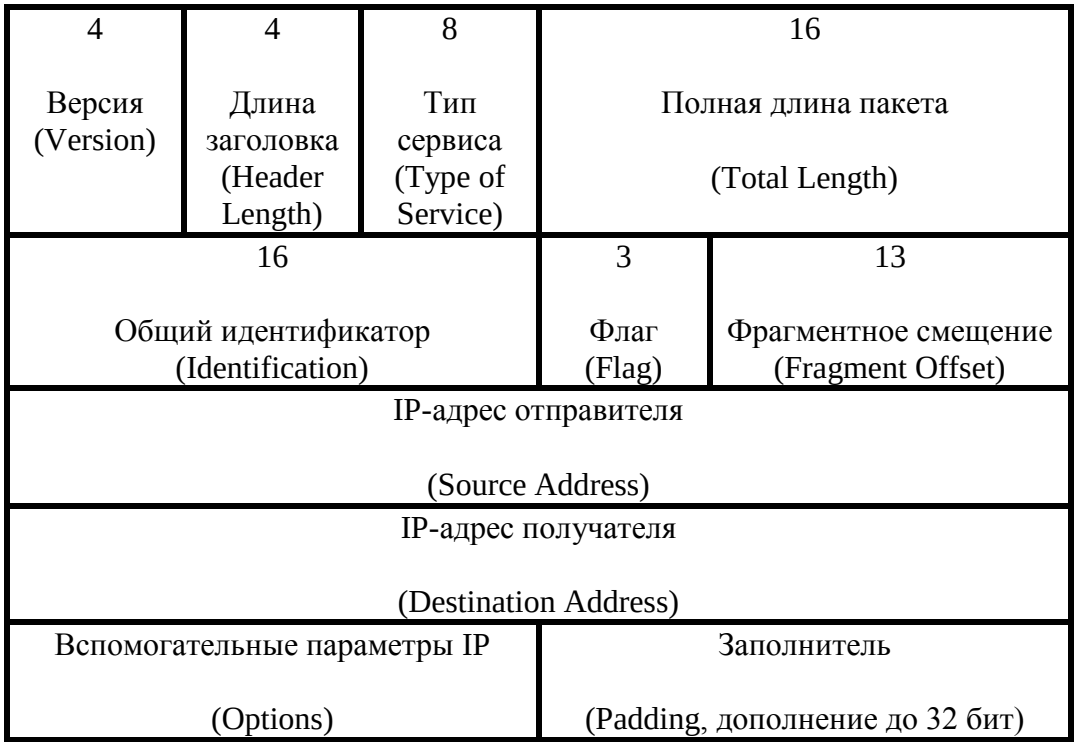


Рис. 3.10. Формат заголовка IPv4

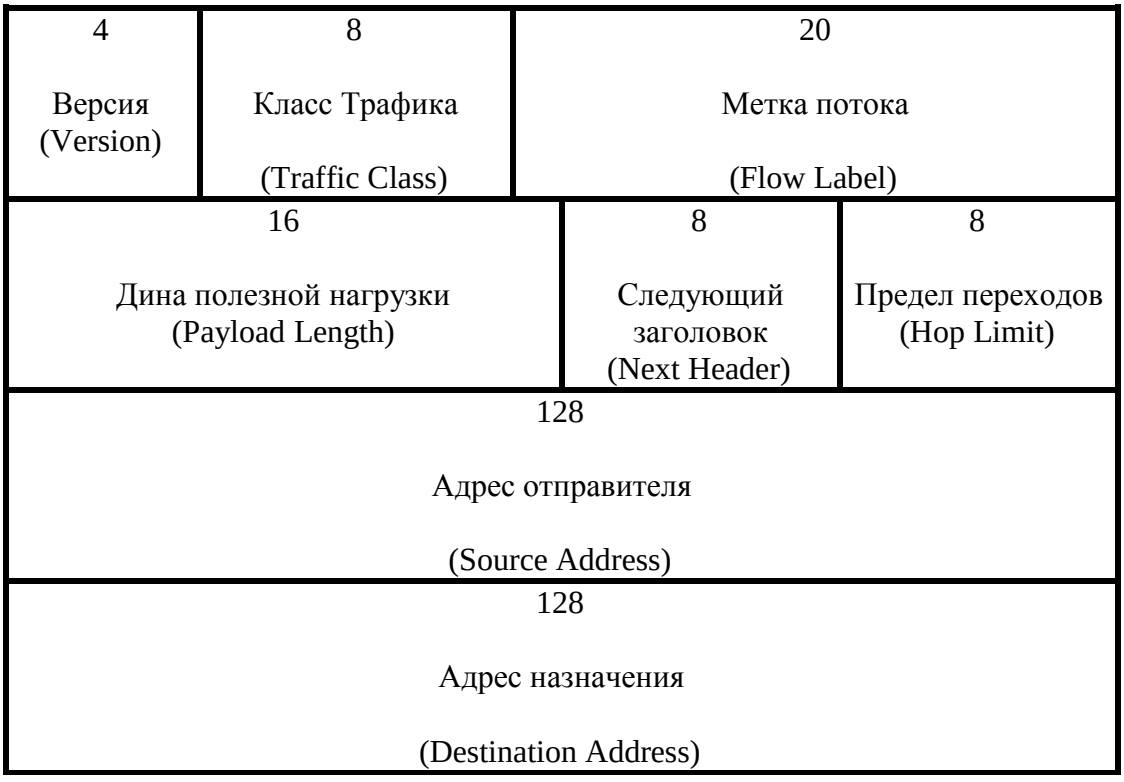


Рис. 3.11. Формат заголовка IPv6

Если значение поля может быть изменено в процессе передачи, то при вычислении значения проверки целостности ICV значение этого поля приравнивается к нулю. Если поле меняется, но его значение у получателя может быть предсказано, тогда это значение присваивается с тем, чтобы можно было посчитать ICV.

RFC 4302 является самой последней спецификацией протокола AH. На рис. 3.12. представлен формат этого варианта протокола. При использовании AH, в протокольный заголовок (IPv4, IPv6), непосредственно предшествующий заголовку AH, следует помещать значение 51 в поле Protocol (IPv4) или Next Header (IPv6).

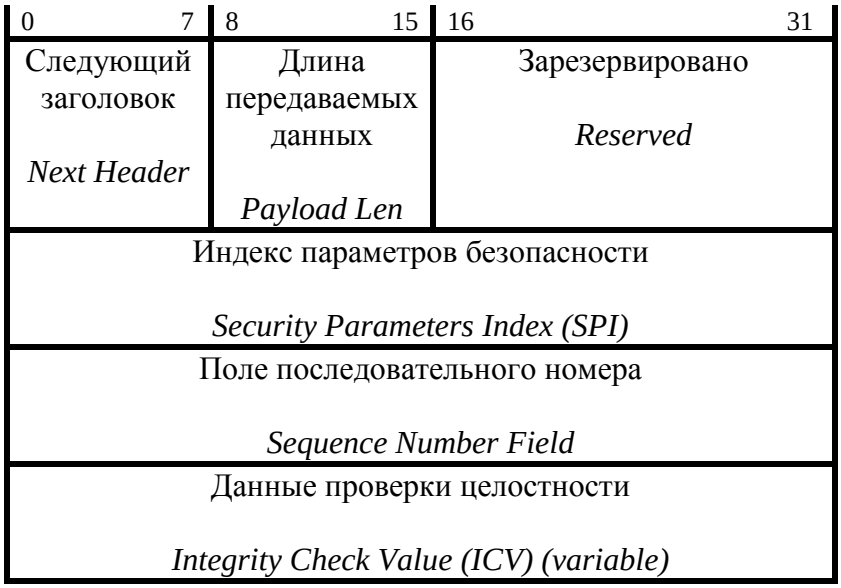


Рис. 3.12. Формат аутентифицирующего заголовка (AH) в соответствии с RFC 4302

Все поля заголовка включаются в значение проверки целостности. Эти поля предназначены для выполнения следующих функций:

Следующий заголовок (Next Header). Поле, которое указывает тип передаваемых данных, идущих после данных идентификации.

Длина передаваемых данных. Поле, указывающее размер заголовка AH в 32-битных словах.

Зарезервировано. Поле, которое является зарезервированным для будущего использования и должно равняться 0.

*Индекс параметра безопасно*сти. Поле, значение которого в комбинации с IP-адресом получателя и протоколом безопасности (AH), однозначно задает

ассоциации безопасности для данной датаграммы. Если значение поля равно нулю, это означает, что ассоциации безопасности не существует.

Поле последовательного номера. Значение поля последовательного номера формируется отправителем по умолчанию и служит для защиты от replay-атак. Это поле всегда присутствует, даже если получатель не использует защиту от повторений в данной SA. Если такая защита используется, передаваемый последовательный номер не может повторяться. Первый пакет ассоциации безопасности имеет порядковый номер 1. Когда порядковый номер достигает максимального значения (4,294,967,295 или $2^{32} - 1$), новые сопоставления безопасности IPsec устанавливаются для поддержания порядкового номера от повтора SA. Если устанавливаются новые сопоставления безопасности IPSec, то порядковый номер для сопоставления безопасности начинается с 0.

Данные идентификации. Поле переменной длины, которое содержит значение проверки целостности ICV расчета отправителя, то есть значение HMAC MD5 или HMAC SHA1.

Значение проверки целостности (Integrity Check Value — ICV) в AH вычисляются на основе:

- полей IP-заголовка, которые либо неизменны, либо их значения можно предсказать по получении;
- заголовка AH (а также возможных заполняющих битов);
- всех заголовков и данных верхнего уровня.

IP-пакет, к которому был применен AH, может быть фрагментирован маршрутизаторами на пути от отправителя к получателю, но такие фрагменты должны быть собраны в целое до обработки AH у получателя. Получающий узел вычисляет ICV на основе соответствующих полей пакета и сравнивает результат со значением, переданным в поле Данные Идентификации. Если они совпадают, датаграмма пропускается.

RFC 4303 – это самая последняя спецификация ESP. Протоколу ESP организация IANA назначила номер 50. ESP состоит из нешифрованного

заголовка, за которым следуют зашифрованные данные. Эти данные состоят из защищенных полей заголовка ESP и данных пользователя, которыми могут быть вся датаграмма IP, включая заголовки верхнего уровня и данные пользователя. На рис. 3.13 показан формат заголовка ESP.

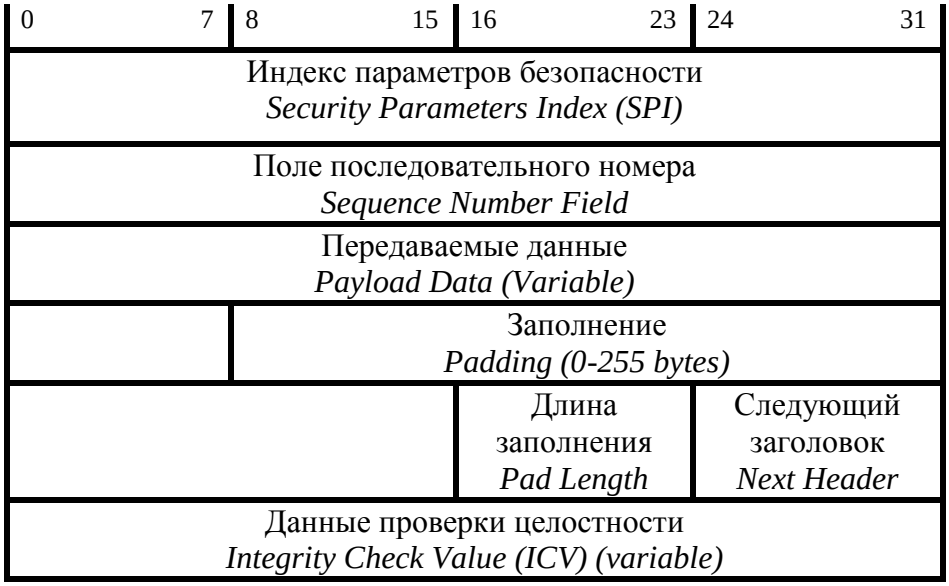


Рис. 3.13. Формат идентифицирующего заголовка (AH) в соответствии с RFC 4303

Все поля заголовка должны присутствовать, и включаются в значение проверки целостности. Эти поля выполняют следующие функции:

Индекс параметра безопасности. Значение этого поля, в комбинации с IP-адресом получателя и номером протокола (ESP), однозначно определяют ассоциацию безопасности данной датаграммы. SPI обычно выбирается получающим узлом в процессе определения SA.

Последовательный номер. Как и в AH, в ESP это поле всегда присутствует, даже если получатель не собирается воспользоваться защитой от повторения в конкретном SA. Если же такая защита применяется (по умолчанию это так), передаваемый последовательный номер не может повторяться.

Предаваемые данные. Поле содержит зашифрованные данные.

Дополнение. Поле переменной длины (от 0 до 255 байт), которое используется для заполнения полезных данных соответствующей длины, служит для обеспечения требования о длине открытого текста. Количество заполняющих байтов зависит от реализации.

Длина дополнения. Поле, длиной в один байт, которое задает количество байтов в поле заполнения.

Следующий заголовок. Однобайтовое поле, которое используется для определения типа данных, находящихся в поле *Передаваемые данные*.

Проверка подлинности данных. Поле переменной длины, которое содержит значение ICV отправителя, то есть значение HMAC MD5 или HMAC SHA1.

Обработка исходящих пакетов

Отправитель при шифрации пакетов производит следующие действия:

- Помещает в поле *Передаваемые данные* ESP исходную информацию протокола верхнего уровня, если находится в транспортном режиме, или всю исходную датаграмму IP, если находится в туннельном режиме.
- Дополняет до нужной длины, если необходимо.
- Шифрует результат (данные, дополняющие биты, длину дополнения и следующий заголовок) с использованием ключа, алгоритма шифрации и режима аутентификации, заданного в SA.
- Если выбрана идентификация, то сначала выполняется шифрация, которая не выполняется над полем *Данные идентификации*.

Обработка входящих пакетов

Если пакет, пришедший на обработку ESP, является фрагментом, то есть поле смещения фрагмента не равно нулю или установлен флаг, указывающий, что должны прийти еще фрагменты, то тогда получатель должен отвергнуть такой пакет и сообщить об ошибке. Запись об этом должна содержать значение SPI, дату и время получения, адрес отправителя, адрес получателя, последовательный номер и (в случае IPv6) идентификатор потока.

Поиск ассоциации безопасности. По получении (собранного) пакета, содержащего заголовок ESP, получатель определяет соответствующую (двунаправленную) SA, основываясь на адресе получателя, номере протокола безопасности (ESP) и SPI. В SA указывается, должно ли быть проверено поле с последовательным номером, должно ли присутствовать поле идентификации и какой алгоритм и ключи используются при дешифрации и вычислении ICV (если такая обработка задана).

Проверка последовательного номера. Все реализации ESP должны обеспечивать защиту от повторений, хотя такая защита может, в зависимости от настроек в SA, и не использоваться получателем.

Проверка значения проверки целостности (ICV). Если в SA требуется использование идентификации, то получатель вычисляет ICV для пакета ESP (за исключением поля с данными идентификации) с применением указанного алгоритма идентификации и удостоверяется, что полученное значение совпадает с тем, что находится в поле идентификации данного пакета. Если вновь вычисленное и переданное ICV совпадают, то проверка для данной датаграммы считается пройденной. Если же они не совпадают, то тогда получатель должен отвергнуть этот IP-пакет и сообщить об ошибке.

Дешифровка пакета. Получающий узел IPSec выполняет следующие действия:

1. Дешифрует поля с блоком данных, дополняющими битами, длиной дополнения и следующим заголовком с использованием ключа, алгоритма дешифрации, режима аутентификации и данными криптографической синхронизации (если есть), заданными в SA.

2. Обрабатывает все дополняющие биты, как указано в спецификации алгоритма дешифрации.

3. Восстанавливает исходную датаграмму IP:

- Транспортный режим. Из исходного IP-заголовка и информации исходного протокола верхнего уровня, находящегося в поле передаваемых данных ESP.
- Туннельный режим. Из IP-заголовка и всей датаграммы IP, находящейся в поле передаваемых данных ESP.

Защита IP-пакетов с помощью AH

Протокол AH может работать в двух режимах — транспортном и туннельном.

В транспортном режиме AH помещается между заголовком IP и заголовком протокола следующего уровня, как показано на рис. 3.14. В случае использования IPv4 заголовок AH вставляется после IP-заголовка и любых содержащихся в нем настроек, и перед протоколом верхнего уровня (Upper-Level Protocol — ULP) или перед любым другим заголовком IPSec. «Протокол верхнего уровня» означает

любой протокол, использующий IP-датаграмму. Такими протоколами могут быть TCP, UDP, OSPF, ICMP и т. д.

Исходный пакет IPv4

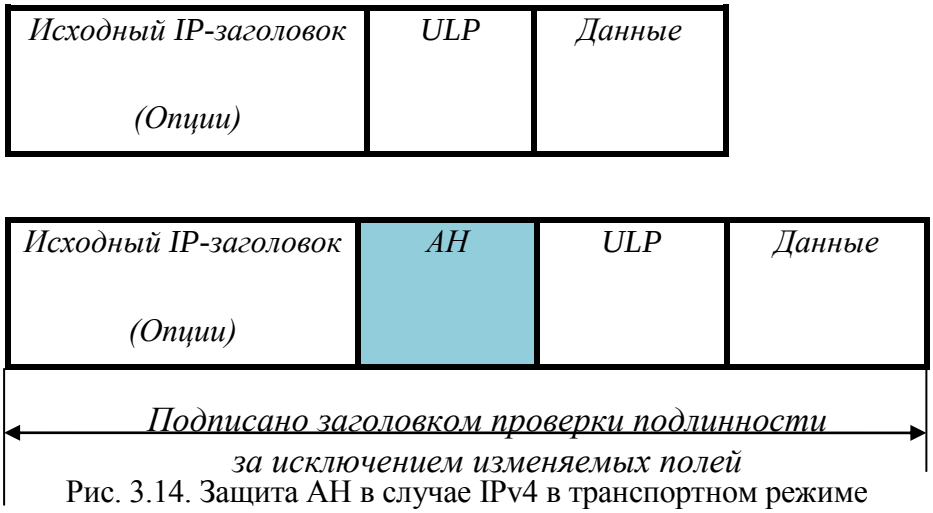
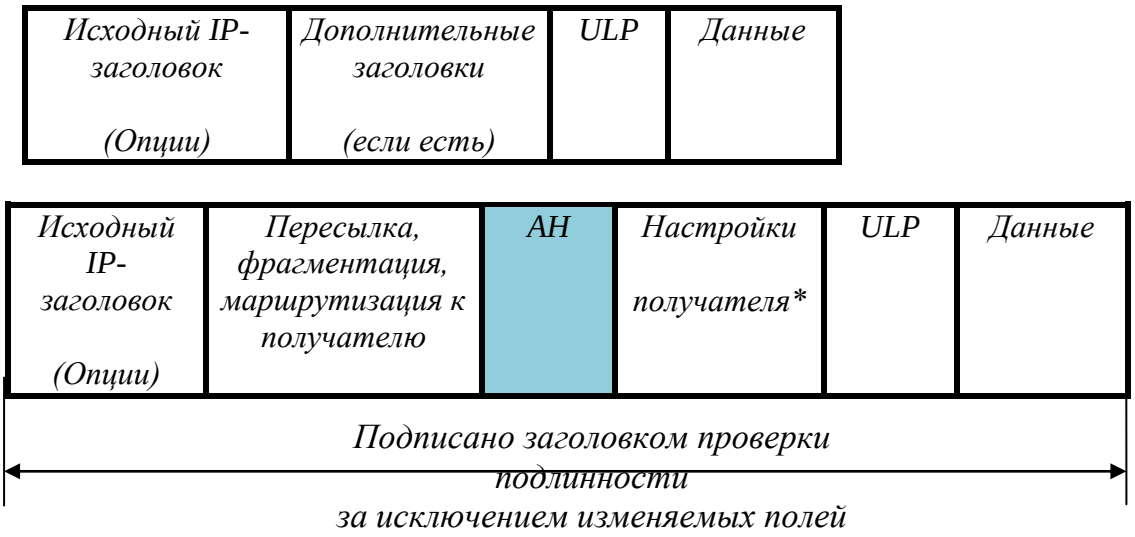


Рис. 3.14. Защита АН в случае IPv4 в транспортном режиме

В случае использования IPv6 заголовок АН представляется как передаваемые данные и размещается осле заголовков размещения (hop-by-hop, routing, fragmentation). Заголовок (заголовки) расширений с настройками получателя могут появиться либо перед, либо после заголовка АН, в зависимости от требований. На рис. 3.15 показано размещение АН для транспортного режима в случае IPv6.

Исходный пакет IPv6



* при наличии могут находиться перед АН, после АН или на обеих позициях

Рис. 3.15. Защита АН в случае IPv6 в транспортном режиме

На рис. 3.16 и рис. 3.17 показана защита AH в случае IPv4 и IPv6 в туннельном режиме. AH в режиме туннелирования подписывает пакет для сохранения целостности и инкапсулирует его в заголовки IP и AH, данные при этом остаются доступными для чтения. Если протокол AH используется в туннельном режиме, части внешнего IP заголовка являются защищенными, как и весь туннелируемый IP пакет, включая весь внутренний IP-заголовок. Во внутреннем и внешнем заголовках могут использоваться разные версии IP (например, IPv6 через туннель IPv4 или IPv4 через туннель IPv6).

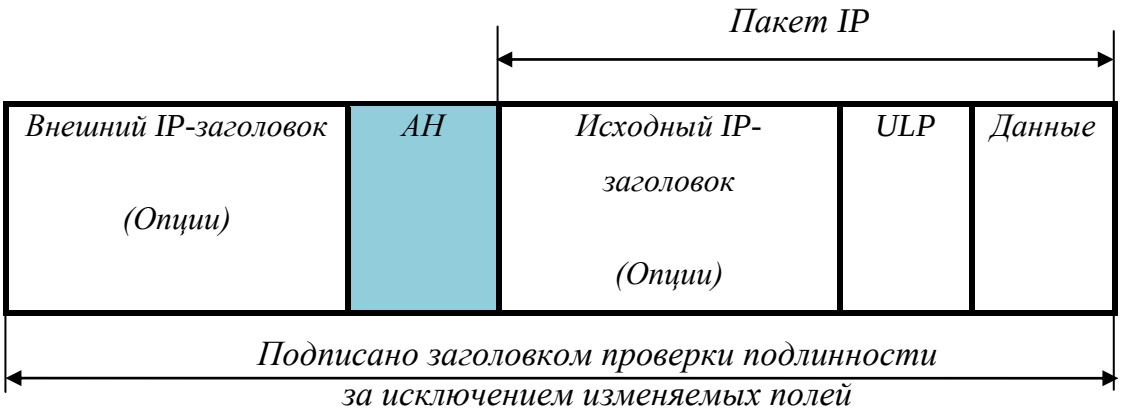


Рис. 3.16. Защита AH в случае IPv4 в туннельном режиме

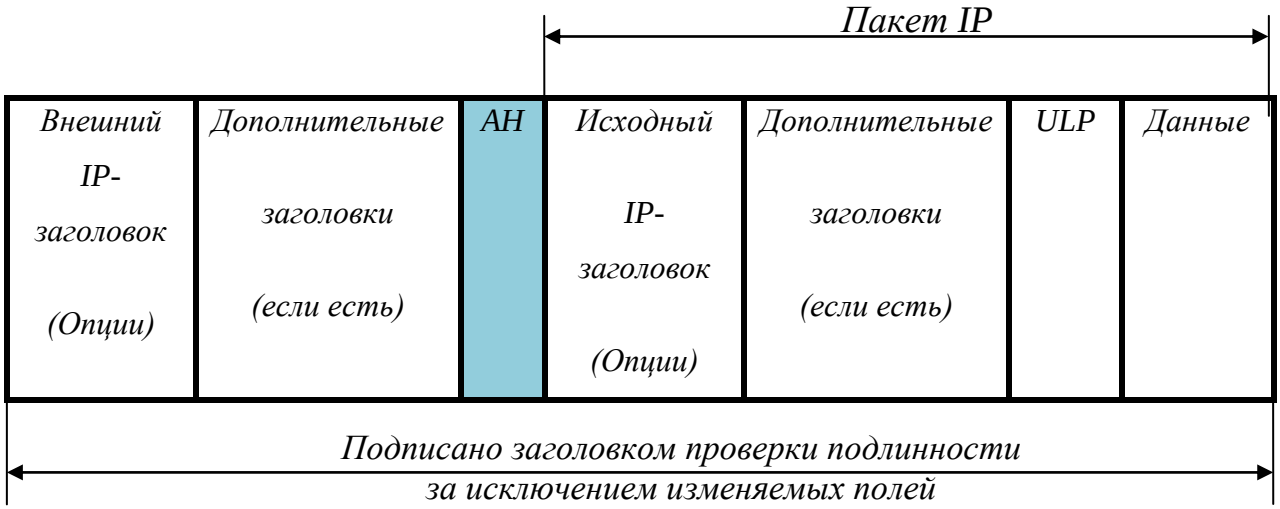


Рис. 3.17. Защита AH в случае IPv6 в туннельном режиме

Защита пакетов с помощью протокола ESP

Так же как и AH, протокол ESP может быть использован в двух режимах: транспортном и туннельном.

Протокол ESP в транспортном режиме обеспечивает конфиденциальность полезных данных IP, но не заголовка IP или заголовков расширений, идущих перед ESP-заголовком. Кроме шифрования полезных данных IP, ESP обеспечивает проверку подлинности и целостности пакета (заголовка ESP, полезных данных IP и трейлера ESP). Значение проверки целостности хранится в поле «трейлер проверки подлинности ESP» или «ESP ICV». Заголовок ESP размещается перед полезными данными IP, а трейлер ESP и трейлер проверки подлинности ESP помещаются за полезными данными IP, как показано на рис. 3.18. В случае IPv4 ESP размещается после IP-заголовка (и любых содержащихся в нем настроек), но перед заголовком протокола следующего уровня (TCP, UDP, ICMP и т.д.). «Концевик ESP» или «Трейлер ESP» содержит все заполняющие биты, их длину и поля следующего заголовка. Если для пакета используется также AH, заголовок идентификации применяется к заголовку ESP, полю Payload, трейлеру ESP и ICV.

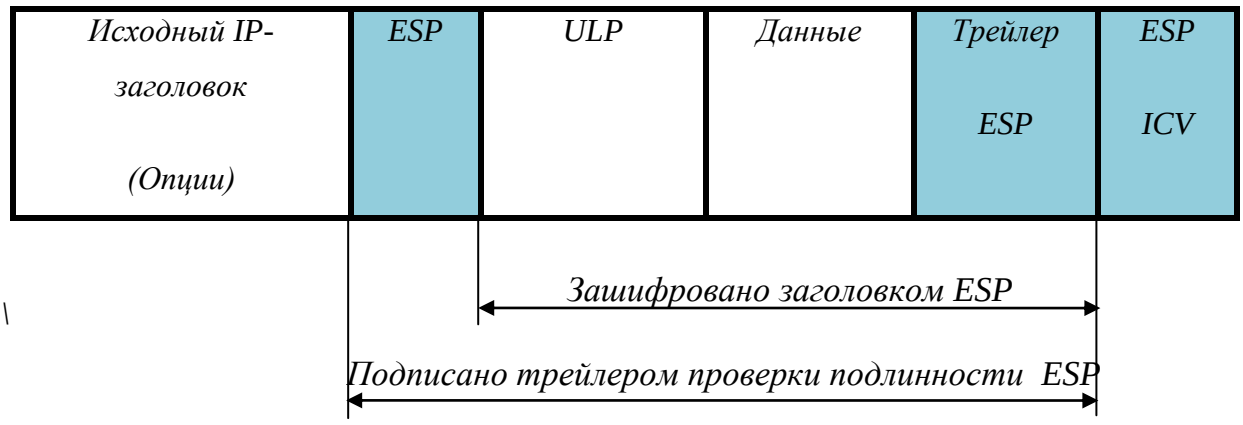
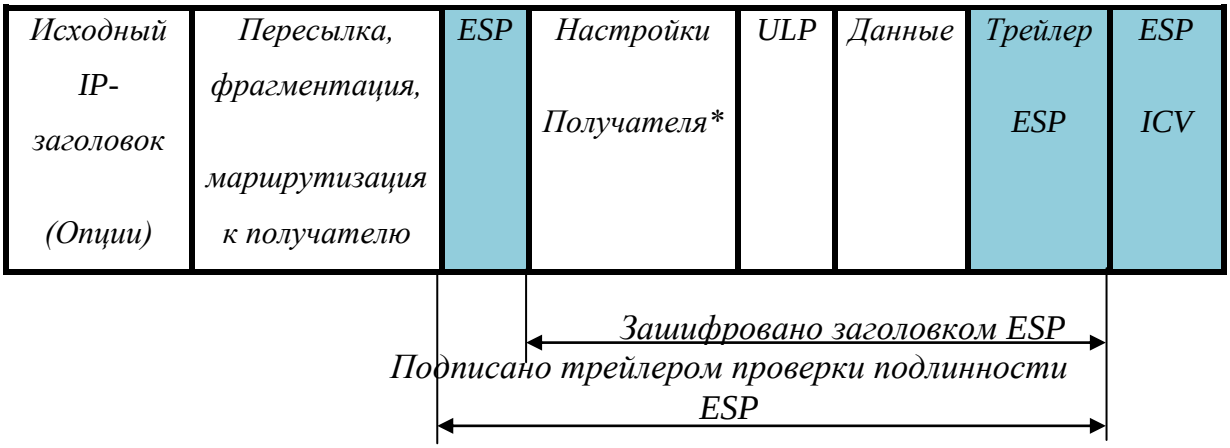


Рис. 3.18. Защита ESP в случае IPv4 в транспортном режиме

На рис. 3.19 показана защита ESP в транспортном режиме в случае IPv6. ESP рассматривается как полезная нагрузка, доставляемая из конца в конец, и должна появиться после данных о пересылках, маршрутизации и заголовков расширения фрагментации. Заголовок (заголовки) расширения настроек получателя могут появиться как до, так и после заголовка ESP, в зависимости от

необходимости. Однако в силу того, что ESP защищает только поля после заголовка ESP, то в общем случае это может быть желательным — поместить заголовки настроек получателя после заголовка ESP.



* при наличии могут находиться перед AH, после AH или на обеих позициях

Рис. 3.19. Защита ESP в случае IPv6 в транспортном режиме

Защищаемые данные в случае туннельного режима ESP показаны на рис. 3.20. и рис. 3.21. В туннельном режиме ESP защищает весь внутренний IP-пакет, включая весь внутренний IP-заголовок. ESP в туннельном режиме помещает исходный пакет целиком между заголовком ESP и трейлером проверки подлинности ESP, включая заголовок IP, и шифрует эти данные, создавая новый заголовок IP.

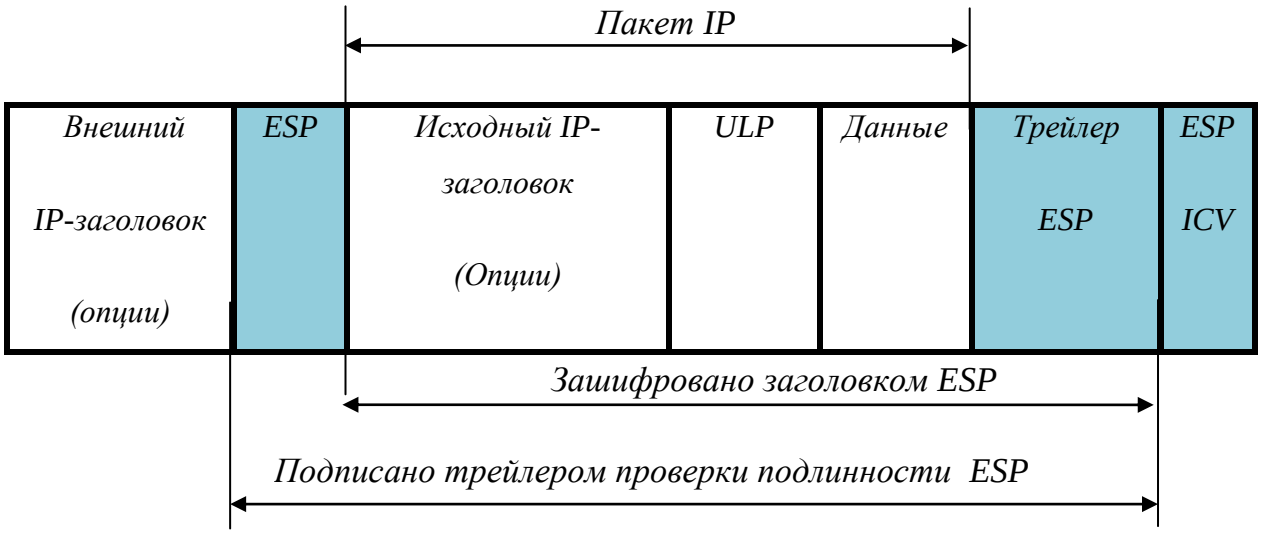


Рис. 3.20. Защита ESP в случае IPv4 в туннельном режиме

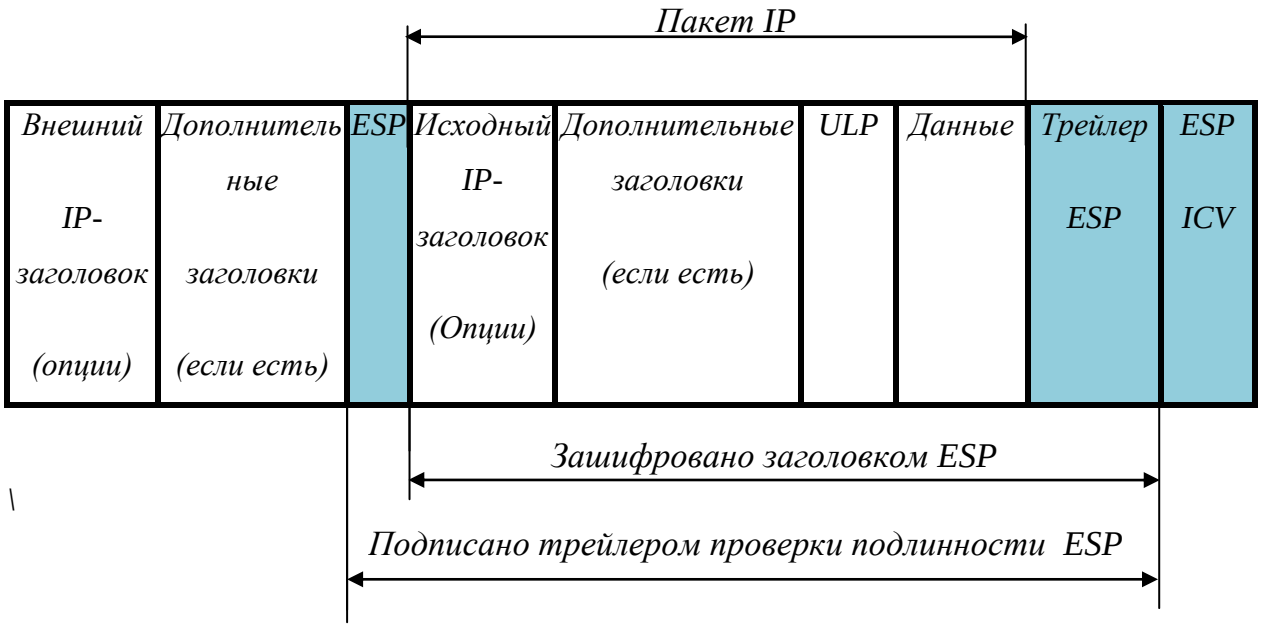


Рис. 3.21. Защита ESP в случае IPv6 в туннельном режиме

Таким образом, взаимоотношения между режимами и протоколами IPSec представлены в табл. 3.1.

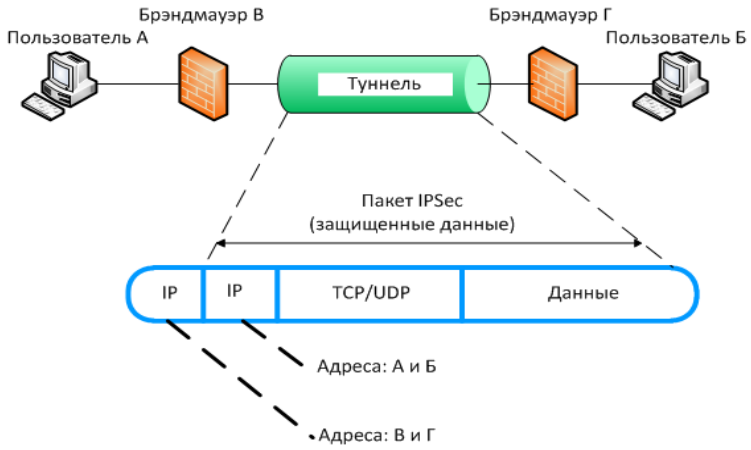
Таблица 3.1.

	Транспортный режим	Туннельный режим
AH	Идентифицирует передаваемые данные и отдельные части IP-заголовка	Идентифицирует весь внутренний IP-заголовок и передаваемые данные, а также отдельные части IP-заголовка.
ESP	Шифрует и идентифицирует данные, но не IP-заголовок	Шифрует и идентифицирует внутренний IP-заголовок и передаваемые данные

IP-адресация в заголовках

Кодирование пакетов IPSec зависит от применяемого протокола безопасности, который, в свою очередь, зависит от настроек SA.

Туннельный режим используется в том случае, когда существует туннель между двумя брандмауэрами (рис. 3.22) или между брандмауэром и удаленной системой (сервером, например).



или:

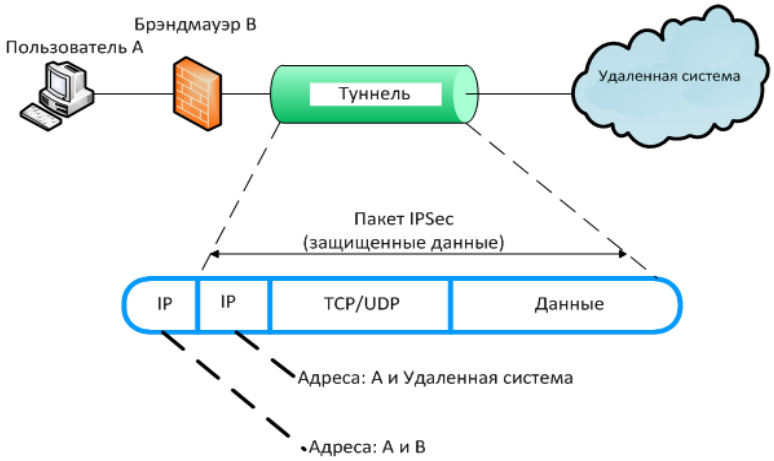


Рис. 3.22. Адресация в туннельном режиме

IP-адреса отправителя и получателя в IP-заголовке могут быть, а могут не быть теми же самыми, что и в исходной датаграмме IP, например, адреса пользователей А и Б могут находиться в защищенном IP-заголовке, тогда как IP-адреса брандмауэров В и Г могут быть во внешнем IP-заголовке. Конкретное использование адресов зависит от того, где начинается и где заканчивается туннель.

Адресация в транспортном режиме показана на рис. 3.23. Транспортный режим используется тогда, когда конечными точками туннеля безопасности являются конечные пользователи соединения.

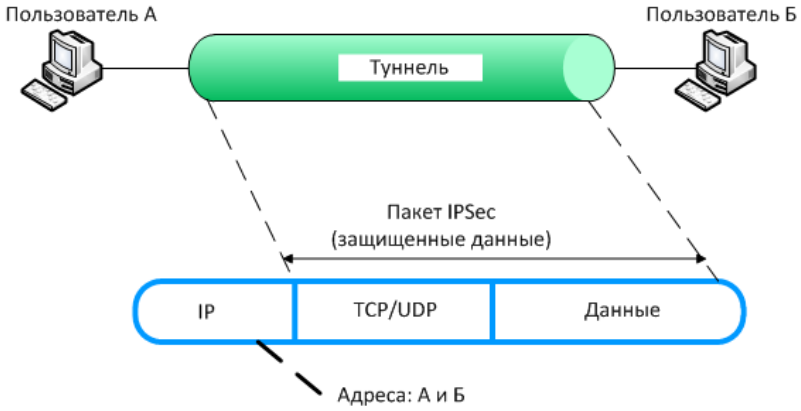


Рис. 3.23. Адресация в транспортном режиме

На рис. 3.24 дано еще одно представление пакета ESP. Он создается у отправителя следующим образом. Сначала генерируется заголовок ESP. Затем к нему добавляются пользовательские данные (полезная нагрузка). После этого создается концевик ESP и добавляется к данным. Кроме того, концевик ESP содержит блок шифра, использованного для шифрации (такой как DES) и, если необходимо, байты, дополняющие блок данных до необходимой длины. Затем блок данных и концевик ESP шифруются, образуя тем самым зашифрованную часть пакета. Если нужна проверка целостности, то на основе заголовка и зашифрованной части вычисляется значение ICV, результат помещается в конец пакета, и все это добавляется к внешнему заголовку IP.

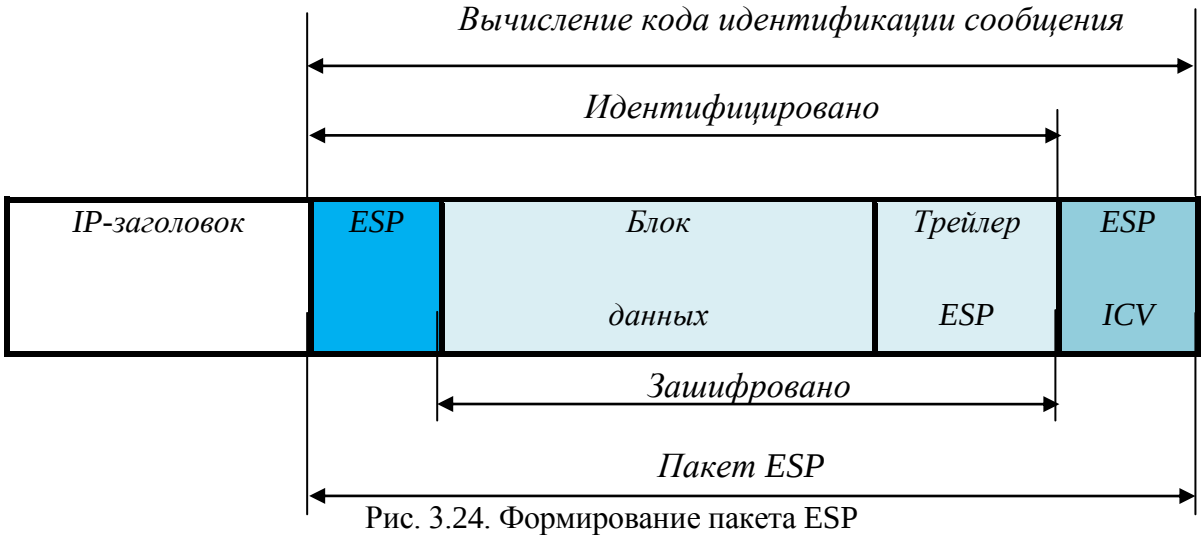


Рис. 3.24. Формирование пакета ESP

Процедура создания пакета AH сходна с процедурой создания ESP и показана на рис. 3.25. Различие заключается в том, что при создании пакета AH не применяется шифрация. Отправитель создает заголовок протокола AH, который (как и в ESP) содержит последовательный номер, SA IPSec, SPI, а также номер протокола для идентификации встроенных данных. Здесь же будет находиться значение MAC. На следующем этапе встраиваемый пакет просто добавляется к этому заголовку AH. Затем перед ним помещается IP-заголовок. Последней операцией является вычисление кода идентификации сообщения MAC для всего пакета, включая IP-заголовок, заголовок AH и передаваемые данные.

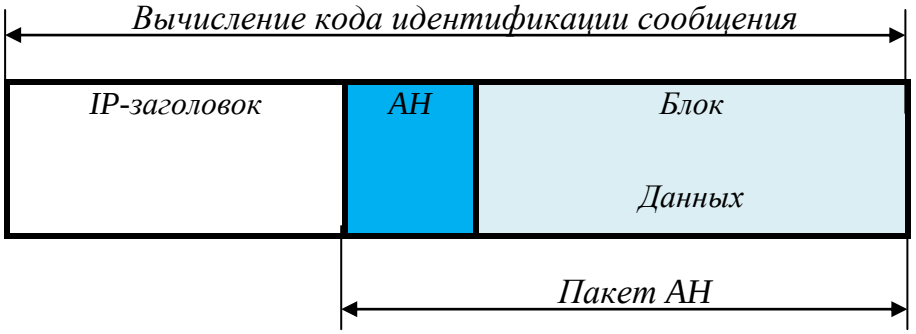


Рис. 3.25. Формирование пакета AH

Хотя ESP может обеспечить как конфиденциальность, так аутентификацию и целостность данных, AH, тем не менее, нужен для того, чтобы обеспечить следующие возможности:

Если шифрация не нужна или запрещена, AH может предоставить защиту целостности данных без затрат на шифрацию.

Защита целостности данных: в отличии от ESP, AH защищает части IP-заголовка. Необходимость такой защита, зависит от требований правил безопасности. Если нужна и шифрация, и защита IP-заголовка, в этом случае необходимо использовать AH совместно с ESP.

На рис. 3.26. показан пакет ESP, встроенный в пакет AH, а пакет AH, в свою очередь, помещен в IP-пакет. В этом варианте предполагается, что пакет ESP создается первым. Поле Последовательный Номер в заголовке AH предоставляет защиту от повторения на ранних стадиях обработки, без необходимости выполнения дешифрации.

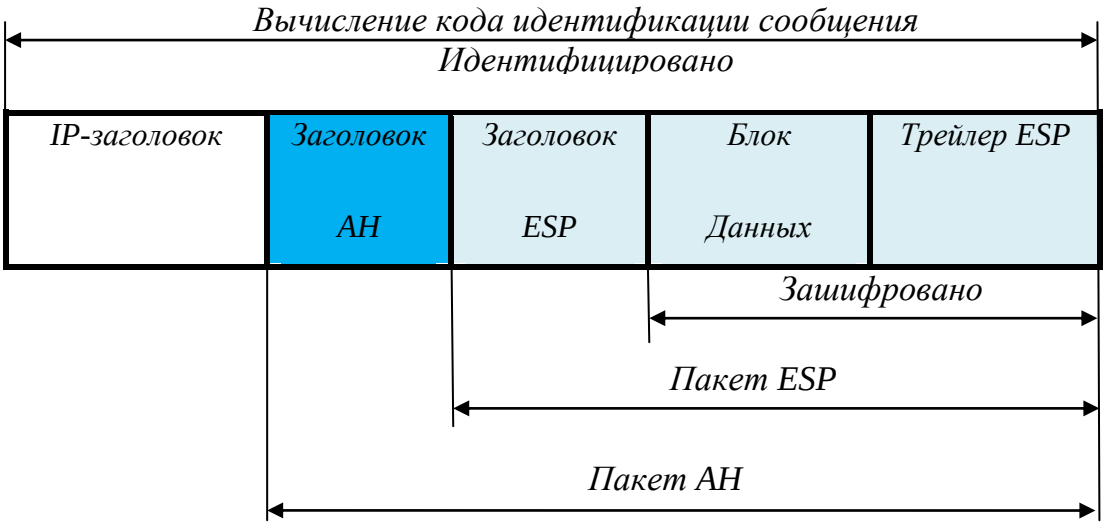


Рис. 3.26. Формирование пакета АН и ESP

3.3. Преимущества и недостатки использования IPSec

IPSec обычно применяется для создания VPN-туннелей между компьютерами либо сетями через Интернет, или другую масштабную сеть, безопасность которой невозможно контролировать, и является наиболее признанным, поддерживаемым и стандартизированным из всех протоколов виртуальных частных сетей (ВЧС, VPN). Для обеспечения совместной работы различных устройств в гетерогенной сети он подходит лучше прочих, так как основан на полностью открытых стандартах. В отличие от других ВЧС-протоколов, IPSec работает на третьем уровне и может защищать любой IP-трафик. При его применении с другими протоколами туннелирования на втором уровне, такими как L2TP, также появляется возможность защиты и не IP-трафика.

IPSec – это не жесткий протокол, диктующий тип алгоритма, ключей и используемых методов аутентификации. IPSec – это открытая модульная платформа, обеспечивающая большую гибкость для компаний, выбравших эту технологию. Большим преимуществом IPSec остается то, что он работает на любом производителе, поддерживающим IPSec RFC, следовательно, использование IPSec решает проблемы совместимости. То, что IPSec является открытым стандартом и работает на третьем уровне, позволяет ему решать более сложные задачи.

Одним из важных преимуществ IPsec является невысокая стоимость его использования, поскольку он позволяет обезопасить данные и обеспечить проверку подлинности пользователей и данных без дополнительных затрат на сетевое оборудование, так как сохраняется совместимость со всем ранее выпущенным оборудованием, а также то, что протокол является стандартным и открытым, и поставляется практически со всеми современными операционными системами.

IPsec обеспечивает высокий настраиваемый уровень безопасности с помощью служб, основанных на криптографии (*хеширование* – для защиты от повторений, обеспечения целостности данных и проверки их подлинности (проверки прав доступа), и непосредственно *шифрование,* обеспечивающее конфиденциальность данных).

Важным преимуществом IPSec, является простота использования IPSec. Для использования IPSec необходимо только настроить и запустить политику безопасности IPSec. IPSec прозрачен для конечных пользователей и приложений. Протокол IPSec интегрирован на сетевом уровне, обеспечивая безопасность для всех протоколов, основанных на IP пакетах TCP/IP, а значит, при реализации IPSec в брандмауэре или маршрутизаторе нет необходимости вносить изменения в сетевые приложения настольного ПК, а также нет необходимости переобучать конечных пользователей. Так же при использовании IPSec существует возможность централизованного управления политикой IPSec. IPSec можно настраивать через групповую политику, политику IP-безопасности или при помощи правил безопасности подключений. Данная возможность позволяет применять политики IPSec на домен, сайт или определенное подразделение, устраняя административные издержки на настройку каждого отдельного компьютера.

При помощи политики IPSec можно настроить сервер только на прием трафика определенного типа. IPSec использует методологию фильтрации для пакетов IP по диапазонам IP- адресов, протоколам IP и определенным TCP и UDP портам.

Политику IPSec можно создавать и настраивать согласно требованиям безопасности приложений, компьютеров, групп компьютеров, домена, сайта

или глобальной организации. IPSec можно настраивать для использования широкого спектра сценариев, включая пакетную фильтрацию, защиту узла трафика хоста по указанному пути, защиту трафика на серверы, туннельного протокола уровня 2 (Layer Two Tunneling Protocol, L2TP), подключений виртуальной частной сети (Virtual Private Network, VPN) и многое другое.

В настоящее время не существует таких сетевых технологий, стандартов и алгоритмов, которые были бы полностью защищены и не уязвимы для атак. Но, тем не менее, с развитием области информационных технологий способы защиты информации становятся все более и более совершенными. Ранее при передаче информации по сетям можно было с помощью несложных действий перехватывать пакеты данных и получать доступ к их содержимому, используя легкий сниффер.

Сейчас, при передаче данных применяется шифрование, которое позволяет защищать передаваемую информацию. Однако, по мнению служб информационной безопасности, вся работа по защите данных сводится к минимизации рисков её утечки и не обеспечивает полной её неприкосновенности.

Стандарт IPsec, как частный и довольно распространённый способ защиты информации, так же, прежде всего предназначен для минимизации риска расшифровывания трафика при его перехвате, поэтому при передаче информации трафик шифруется. Также, ключевой особенностью этого стандарта, является, так называемый handshake (приветствие, рукопожатие) обоих хостов, выявляющий уровень доверия между ними.

Таким образом, стандарт IPsec, как и другие стандарты и протоколы сетевой безопасности имеет свои недостатки и уязвим для атак, но только при неправильном его использовании. И это не является причиной для того чтобы отказываться от такого гибкого и отлично зарекомендовавшего себя инструмента для построения защищенных туннелей.

Некоторые меры предосторожности, которые следует соблюдать при работе с IPSec для того, чтобы максимально ограничить влияние сетевых

атак на сохранность, конфиденциальность и целостность информации приведены ниже:

1. Необходимо обеспечивать работу первой фазы IKE с более медленном, но более безопасном основном режиме и избегать работы в более быстром, но менее защищенном энергичном режиме первой фазы IKE. Оборудование многих производителей не поддерживает энергичный режим первой фазы IKE.

2. Для аутентификации сторон при выборе механизмов аутентификации следует использовать более сильный алгоритм SHA1 и избегать использования менее криптостойких MD5 хешей.

3. Для обеспечения конфиденциальности передаваемых данных следует использовать более стойкие алгоритмы шифрования 3DES.

4. Для большей безопасности следует использовать IKEv2.

5. Протоколы IPSec будут неэффективно работать с мобильными, постоянно перемещающимися между точками доступа одной сети клиентами. Это вызвано тем, что перемещающийся клиент будет слишком часто получать новый IP-адрес, что в свою очередь, потребует слишком частого согласования ассоциаций безопасности.

6. Реализация решений с помощью политик IPSec должна тщательно планироваться, а перед развертыванием - тестироваться в среде, максимально точно моделирующей реальную.

7. IPSec предусматривает исключительно взаимную аутентификацию партнеров на уровне системы - он не включает проверку идентичности пользователя этой системы. Таким образом, если злоумышленник получает доступ к системе от имени какого-либо пользователя, он может получить доступ и к данным, передаваемым с помощью IPSec. Данная проблема конечно же может быть решена многими стандартными способами идентификации пользователей системы - от смарт-карт и биометрии до различных расширений протокола IKE.

4. Установление соединения IPSEC между компьютерами Windows XP

4.1 Этапы настройки и установки соединения IPSec

Этапы настройки и установки соединения IPSec:

1. Создание политики безопасности IPSEC.
2. Добавление правила безопасности в созданную политику.
3. Добавление фильтра для трафика, который будет шифроваться.
4. Определение действий фильтра (Filter Action).
5. Заключительная настройка IPSEC.
6. Запуск и проверка работы IPSEC соединения.

Общий набор параметров безопасности IPSec называется **политикой IPSec.** Политика состоит из набора правил, определяющих обработку сетевого трафика. Каждое правило содержит относящиеся к нему набор фильтров и действия, которые данное правило будет производить с пакетом, соответствующим условиям фильтра. В качестве параметров фильтров могут быть заданы IP-адреса, адреса сети или полное доменное имя отправителя и получателя пакета, тип IP-протокола (ICMP, TCP, UDP и т.д.), номера TCP и UDP портов отправителя и получателя.

В ОС Windows XP настройку IPsec можно выполнить посредством функции «Локальные параметры безопасности». Запуск может быть произведен из меню «Администрирование» «Панели управления», или с помощью команды «Выполнить» «secpol.msc». При работе с IPSec есть возможность использования созданных по умолчанию политик, либо создания новой.

1. Создание новой политики безопасности

Для создания новой политики безопасности IP необходимо выбрать из списка пункт «Политики безопасности IP» и в меню при нажатии правой кнопки мыши выбрать действие «Создать политику безопасности IP» или в меню «Действие» выбрать «Создать политику безопасности IP» (рис. 4.1).

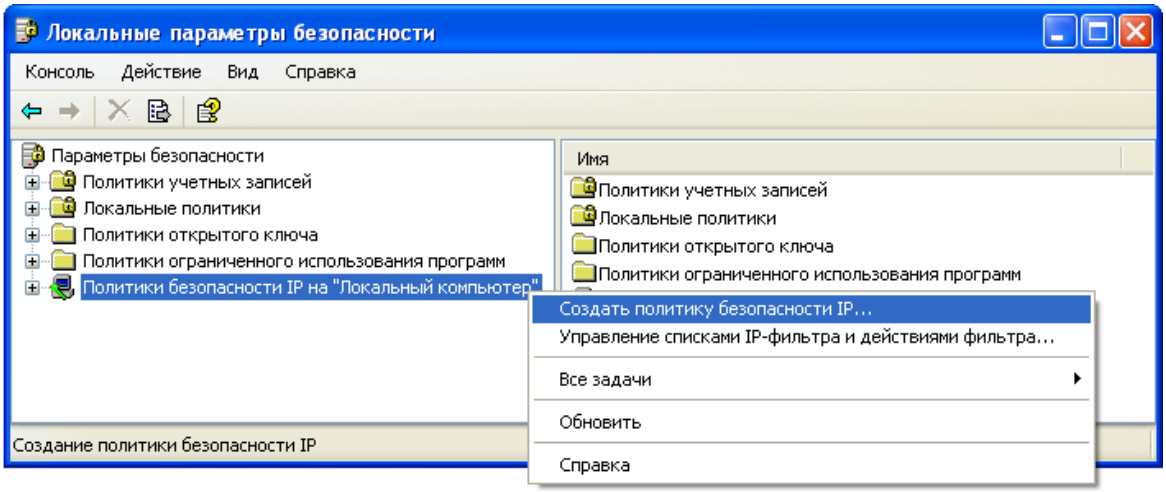


Рис. 4.1

После этого откроется «Мастер политики IP-безопасности». Для продолжения следует нажать кнопку «Далее», в результате чего откроется окно, где нужно ввести имя новой политики, и нажать кнопку «Далее» (рис. 4.2).

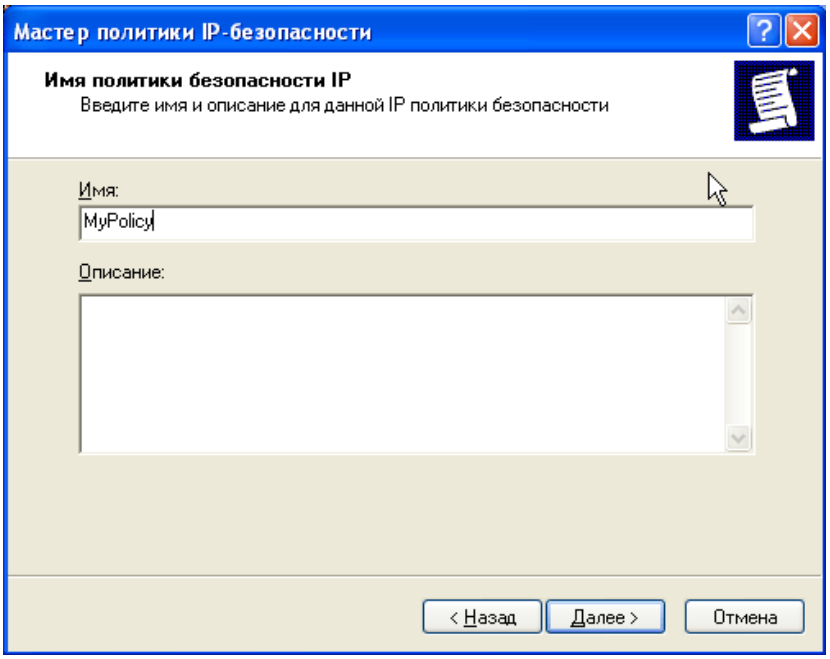


Рис. 4.2

В следующем окне «Мастер» предложит принять решение об использовании правила по умолчанию. Использование правила по умолчанию можно отменить после создания политики, если возникнет такая необходимость (рис. 4.3).

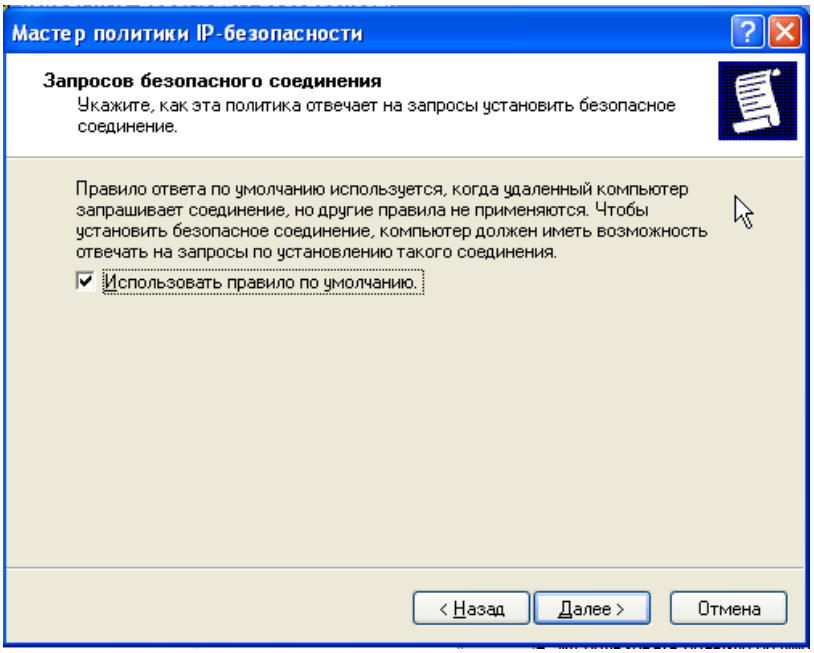


Рис. 4.3

Далее «Мастер» предлагает несколько способов проверки подлинности пользователя, которые поддерживает IPsec: посредством протокола Kerberos (стандартный протокол аутентификации в доменах Windows 2000 и Windows 2003), с помощью сертификата пользователя, либо на основании строки защиты (предварительного ключа). Если в сети нет контроллеров домена, и пользователи сети не обладают действительными сертификатами, следует выбрать проверку подлинности с помощью предварительного ключа (рис. 4.4).

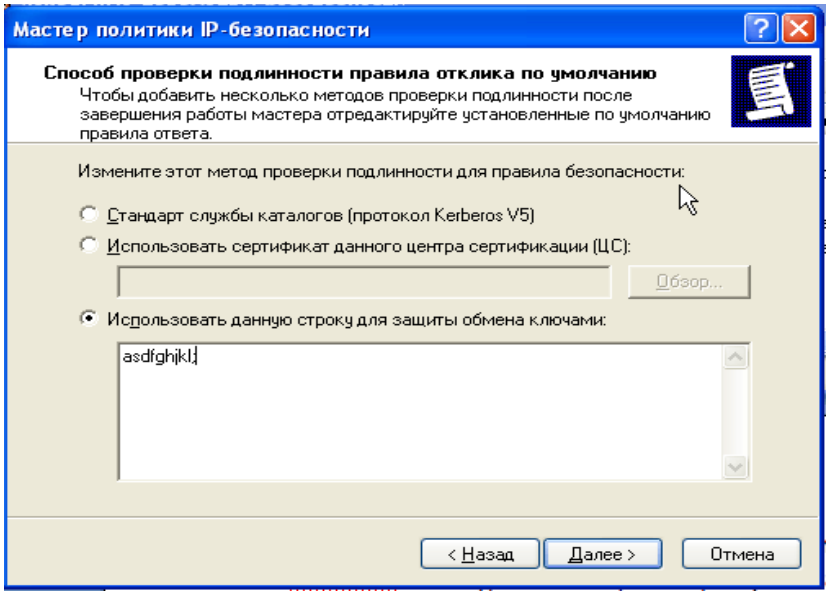


Рис. 4.4

Таким образом, создание политики практически завершено (рис. 4.5). Изменить свойства можно при завершении работы мастера (окно свойств откроется автоматически), либо позже, выделив нужную политику и выбрав из контекстного меню пункт «Свойства».

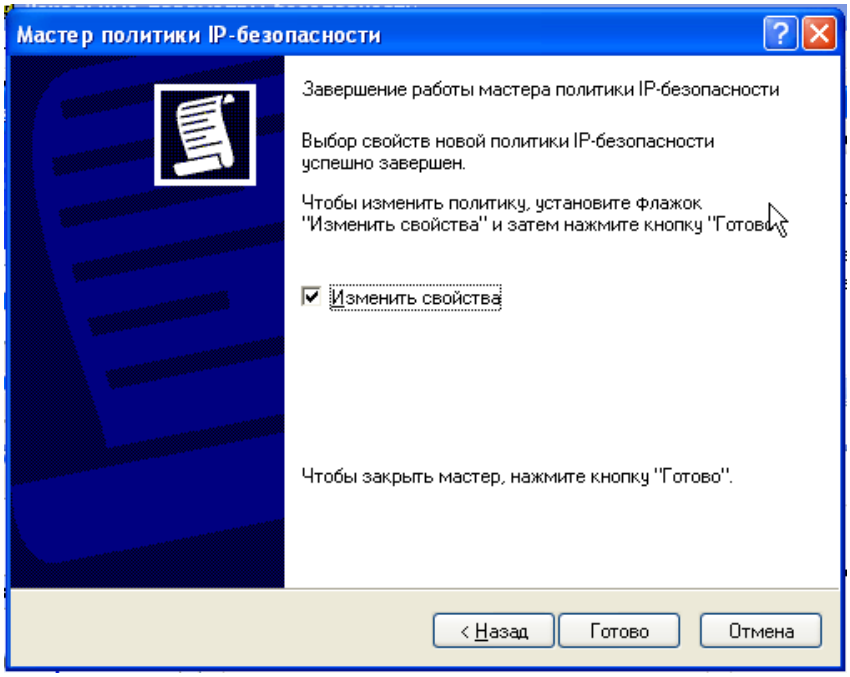


Рис. 4.5

Далее необходимо изменить свойства политики таким образом, чтобы они соответствовали требованиям, а следовательно необходимо создать правила безопасности IP, фильтр и определить действие фильтра.

2. Добавление правила безопасности для созданной политики

Для создания правила безопасности следует открыть свойства созданной политики безопасности IP и на вкладке «Правила» нажать кнопку «Добавить», предварительно сняв флажок «Использовать мастер» (рис. 4.6).

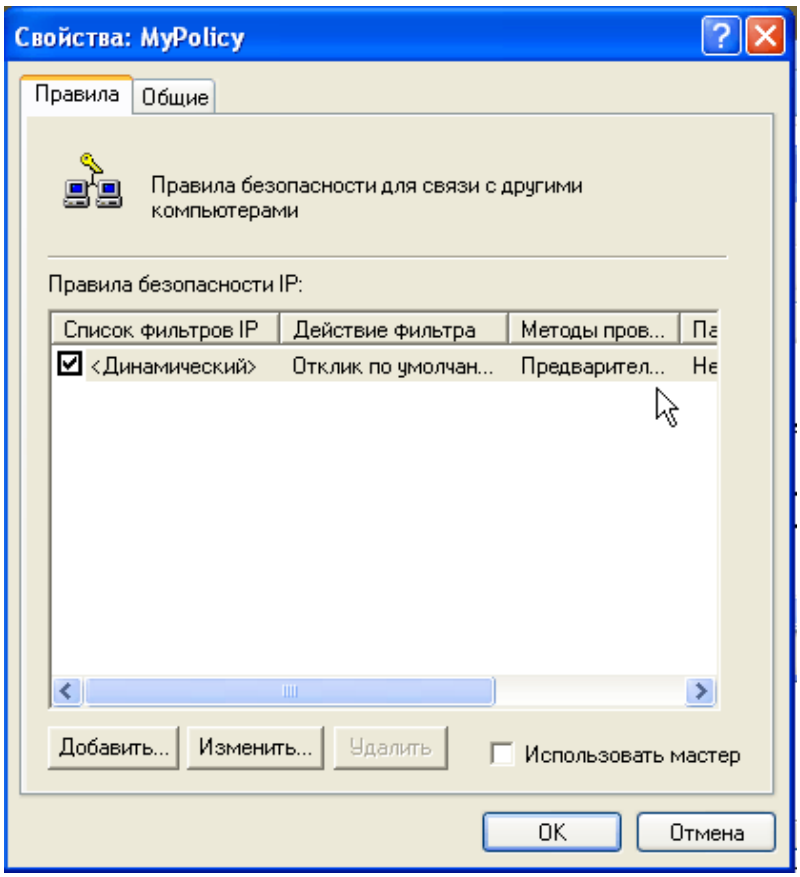


Рис. 4.6

Так как соединение IPSec настраивается для транспортного режима, на закладке «Параметры туннеля» нет необходимости что-либо изменять. На закладке «Тип подключения» можно выбрать сетевые подключения, для которых будет применяться создаваемое правило – все подключения, только локальные подключения, только удаленные подключения. Таким образом, предоставляется возможность создания различных правил для сетевых подключений с различной скоростью передачи данных, что позволяет для более медленных и, как правило, менее защищенных удаленных подключений установить другие параметры аутентификации, проверки целостности и шифрования (рис. 4.7).

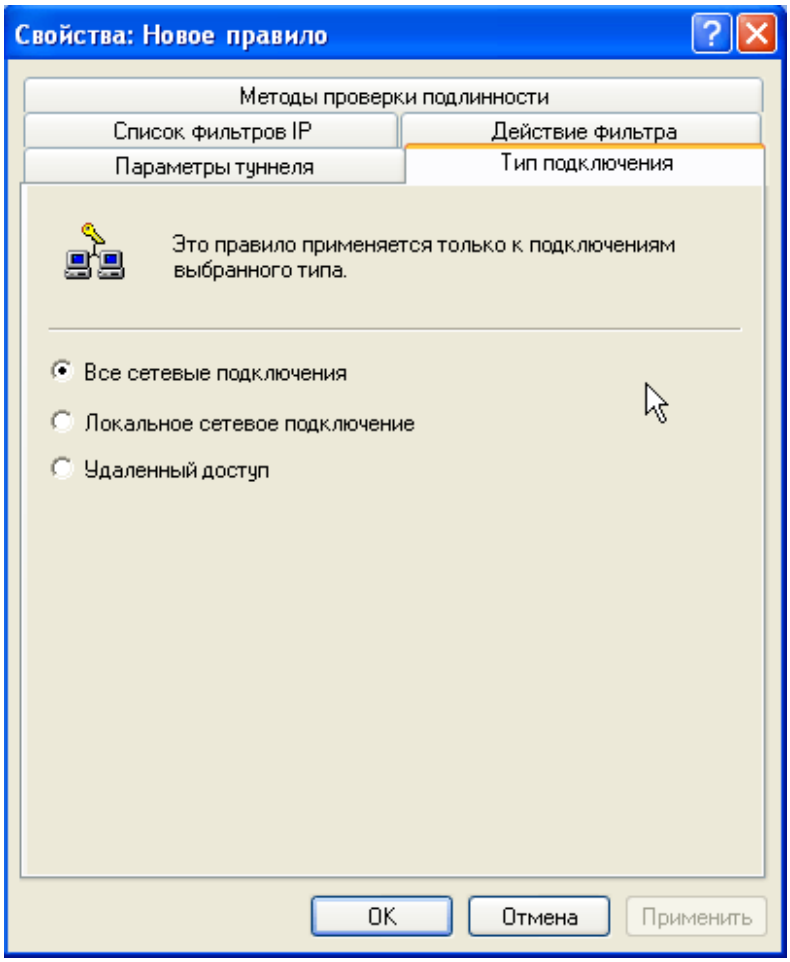


Рис. 4.7

На закладке «Методы проверки подлинности» есть возможность добавить несколько методов проверки и изменить порядок их предпочтения, что позволяет более гибко настроить правило для связи с различными узлами, поддерживающими различные способы аутентификации (рис. 4.8).

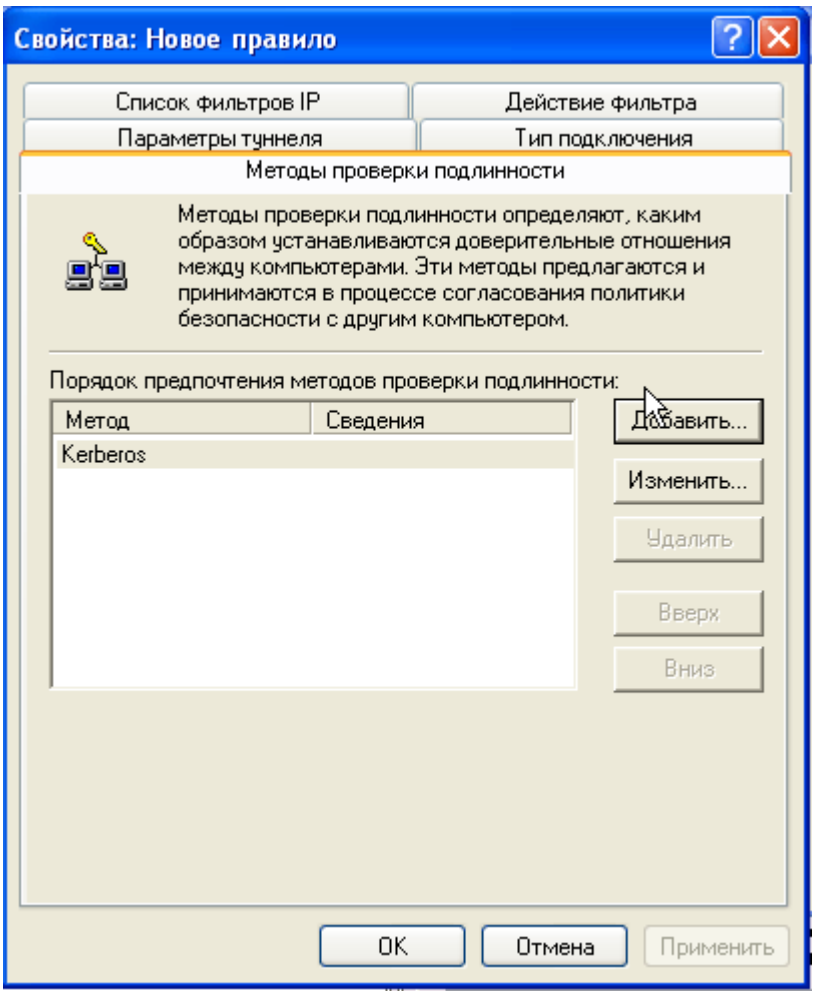


Рис. 4.8

3. Добавление фильтра

Далее на закладке «Список фильтров IP» необходимо выбрать фильтр IP и действие фильтра, либо создать новый (рис. 4.9).

Фильтры, созданные по умолчанию:

- Полный IP-трафик, который применяется ко всему IP-трафику, независимо от используемого протокола более высокого уровня;
- Полный ICMP-трафик, который применяется ко всему ICMP-трафику.

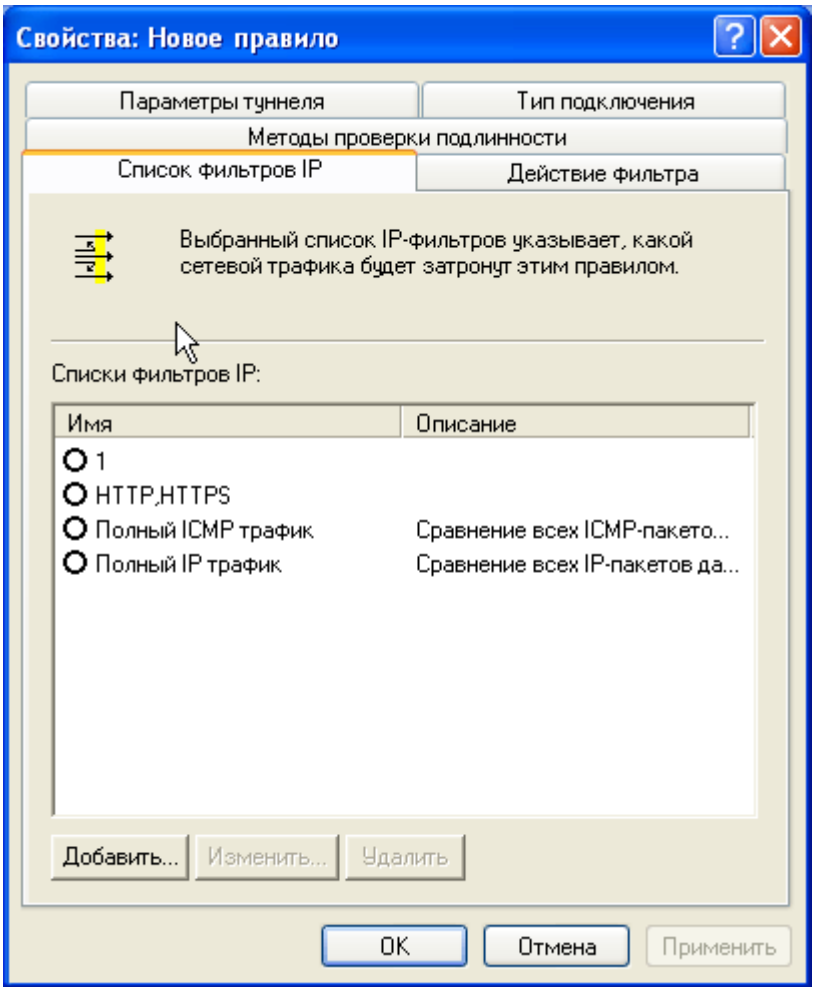


Рис. 4.9

Для создания нового фильтра необходимо нажать кнопку «Добавить», в результате чего откроется окно «Список фильтров IP», где необходимо снять галочку «Использовать мастер» и, после ввода имени списка фильтров, нажать кнопку «Добавить» (рис. 4.10).

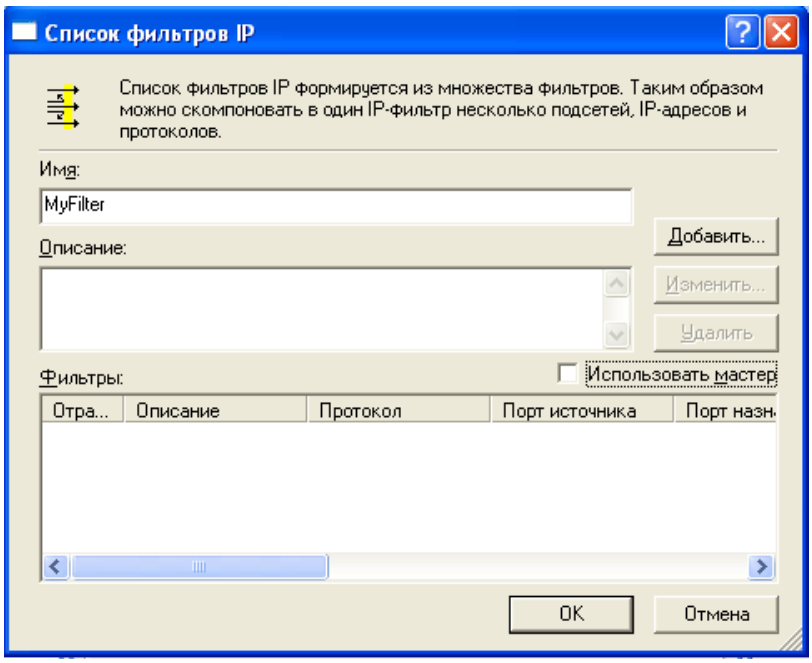


Рис. 4.10

Далее откроется окно «Свойства: Фильтр», где необходимо указать адреса источника и получателя пакетов, к которым будет применяться фильтр, а также, при необходимости, протокол и порты источника и получателя (рис. 4.11).

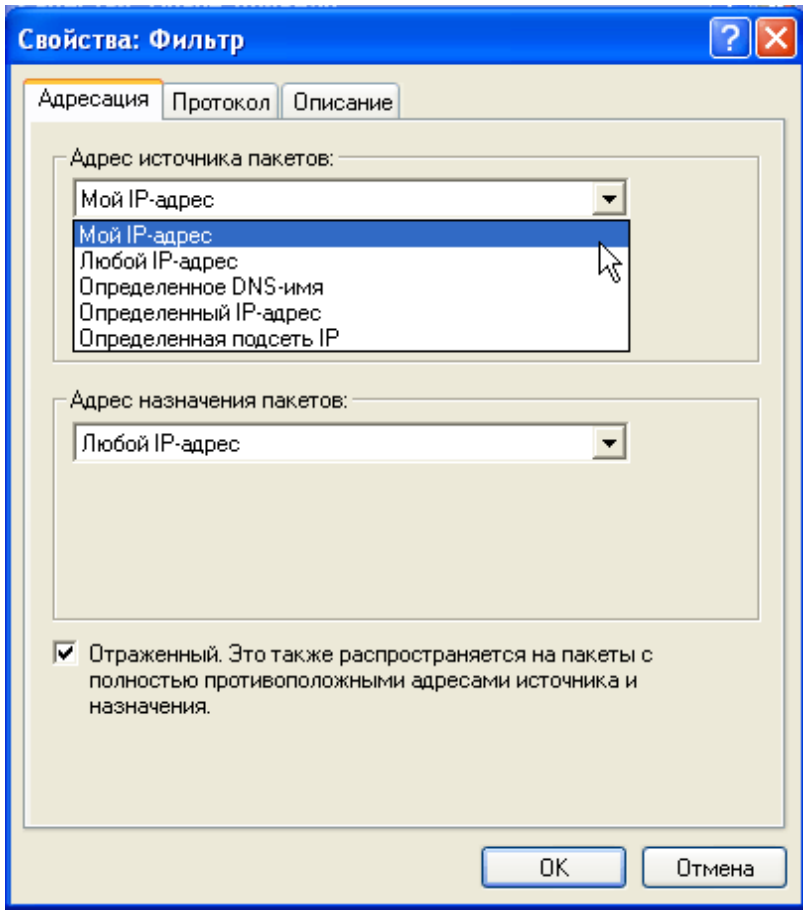


Рис. 4.11

4. Определение действия фильтра

Далее необходимо определить действие фильтра. На закладке «Действие фильтра» можно выбрать действия по умолчанию или создать новое. Созданные по умолчанию действия (рис. 4.12):

- ***Запрос безопасности*** – принимать небезопасную связь, но требовать от клиентов применения методов доверия и безопасности. Будет поддерживаться небезопасная связь с ненадежными клиентами, если клиенты выполнят требования безопасности.
- ***Разрешить*** – разрешает прохождение небезопасных IP-пакетов (без использования IPsec).
- ***Требуется безопасность***, что определяет разрыв связи с клиентами, не поддерживающими IPsec, а с клиентами, поддерживающими IPsec будет производиться обмен данными с применением проверки целостности ESP, но без AH и без шифрования данных.

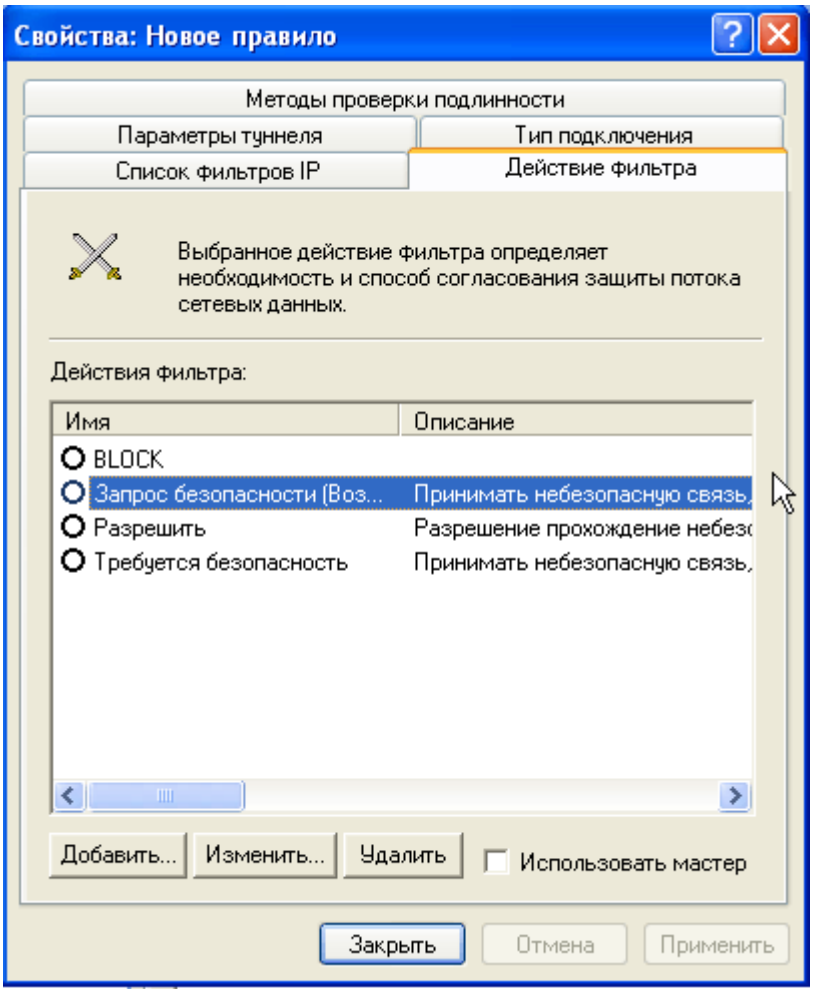


Рис. 4.12

Новое действие можно создать, сняв флажок «Использовать мастер» и нажав на кнопку «Добавить». На вкладке «Методы безопасности» открывшегося окна «Свойства: создание действия фильтра», необходимо выбрать: нужно ли разрешить прохождение данных, заблокировать их, либо согласовать безопасность (рис. 4.13).

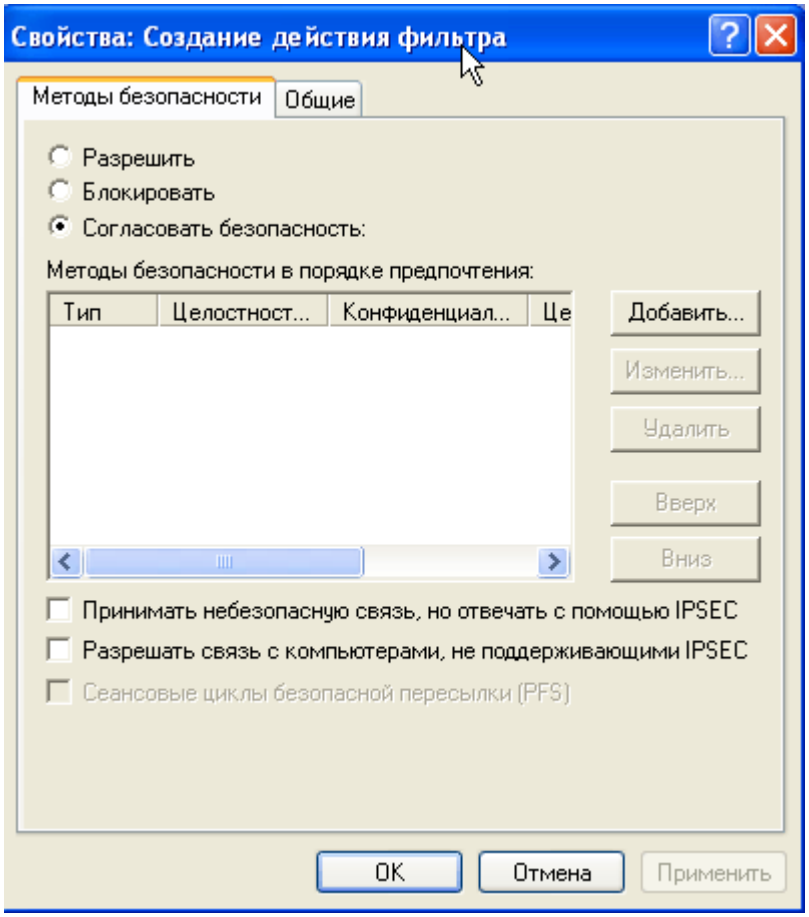


Рис. 4.13

При выборе пункта «Согласовать безопасность», можно добавить методы безопасности и изменить порядок их предпочтения. При добавлении методов безопасности следует выбрать, будет ли использоваться AH, ESP, либо настроить безопасность вручную, выбрав пункт «Настраиваемая безопасность» (рис. 4.14).

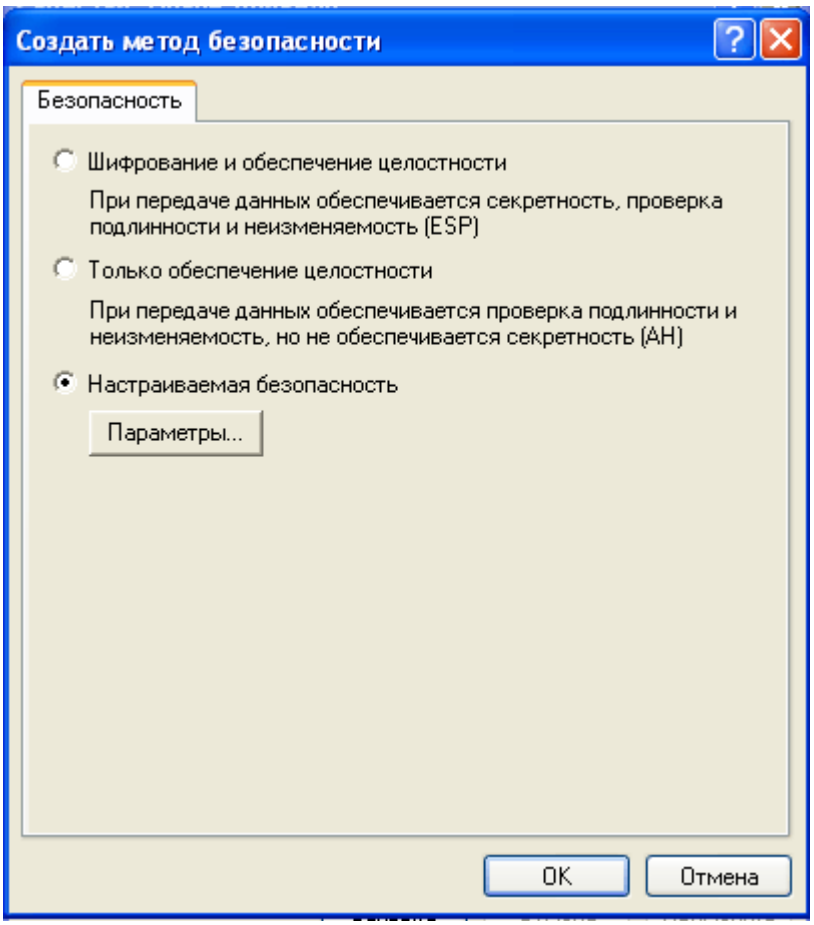


Рис. 4.14

В параметрах настраиваемой безопасности устанавливаются требуемые протоколы (AH и ESP), а также предоставлена возможность вручную выбрать алгоритмы проверки целостности и шифрования, параметры смены ключей сеанса (рис. 4.15). По умолчанию ключи изменяются каждый час либо через каждые 100Mb переданной информации.

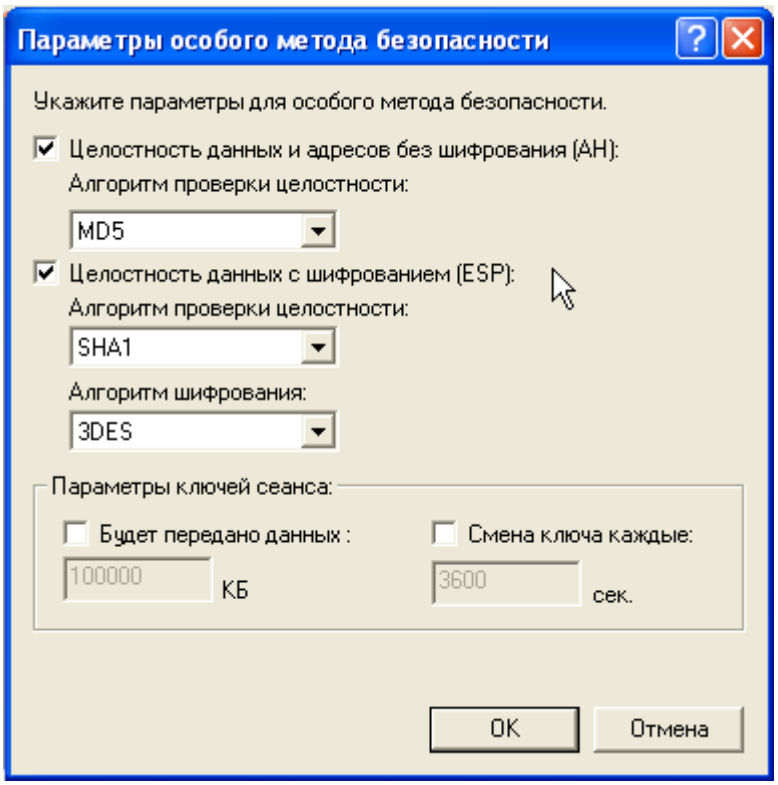


Рис. 4.15

5. Заключительная настройка IPSec

После выбора действий фильтров настройку политики безопасности IP можно считать завершенной. С помощью нажатия кнопок «OK» и «Применить» необходимо завершить работу с «Мастером настройки».

Далее необходимо назначить созданную политику безопасности (рис. 4.16).

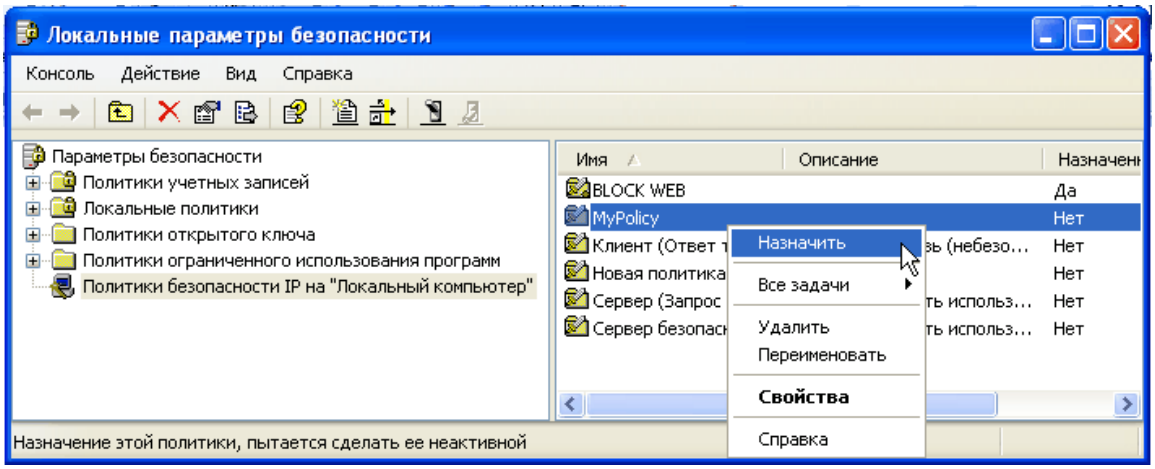


Рис. 4.16

Если настройка производилась в Windows XP, для транспортного режима IPsec, то такую же операцию следует произвести на каждом

компьютере. Средства автоматизации в Windows Server позволяют централизовано развернуть политику IP на всех рабочих станциях домена.

6. Запуск и проверка IPSec соединения

Проверить, установилось ли соединение IPSec, можно с помощью утилиты ping в командной строке. Строки «Согласование используемого уровня безопасности IP» означают, что системы выбирают общие типы шифрования (рис. 4.17).

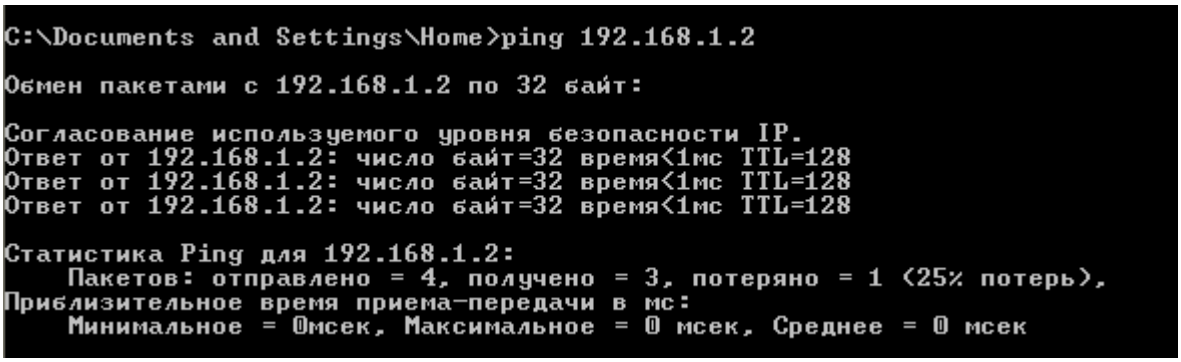


Рис. 4.17

4.2 Тестирование производительности протокола IPSec

В ходе дипломной работы было проведено тестирование производительности протокола IPsec, для того, чтобы выявить уровень нагрузки на центральный процессор во время передачи данных по сети с использованием различных криптографических алгоритмов.

Тестирование производилось на компьютерах, имеющих следующие технические характеристики:

	Компьютер 1	Компьютер 2
Процессор	Intel Mobile Core 2 Duo T8300 @ 2400МГ	Intel Pentium 4 @ 2266МГц
Материнская плата	Apple Inc. Mac-F22788A9	MSI MS-6580
Память	2048Мб (2x1024 DDR2-SDRAM)	1024Мб (2x512 DDR-SDRAM)
Жесткий диск	FUJITSU MHY2160BH (160Гб)	Western Digital WD5000AAKB-00H8A0 (500Гб)
Сетевой адаптер	Marvell Semiconductor (Was: Galileo Technology Yukon 88E8058 PCIe Gigabit Ethernet Controller	Realtek Semiconductor RTL8139/810x Fast Ethernet Adapter

Файл, объем которого составлял 105 Мб, передавался по сети между двумя компьютерами с различными настройками IPsec в транспортном режиме (Transport Mode), а также без использования рассматриваемого протокола.

Необходимо помнить, что в транспортном режиме протоколы AH и ESP шифруют и хешируют только полезные данные, а не весь пакет, как это происходит при инкапсуляции в туннельном режиме.

В измерениях возможна некоторая погрешность, так как измерения загруженности процессора и времени передачи файла проводились с помощью часов и диспетчера задач Windows.

1. Передача файла по сети без использования IPsec. Время передачи файла составило 9 с и 11 с, а средняя скорость передачи данных достигла 11,67 Мбит/с и 9,55 Мбит/с на компьютере 1 и 2 соответственно. При этом загруженность процессоров на обоих компьютерах составила 42% и 44%, как показано на рис. 4.18 и рис. 4.19.

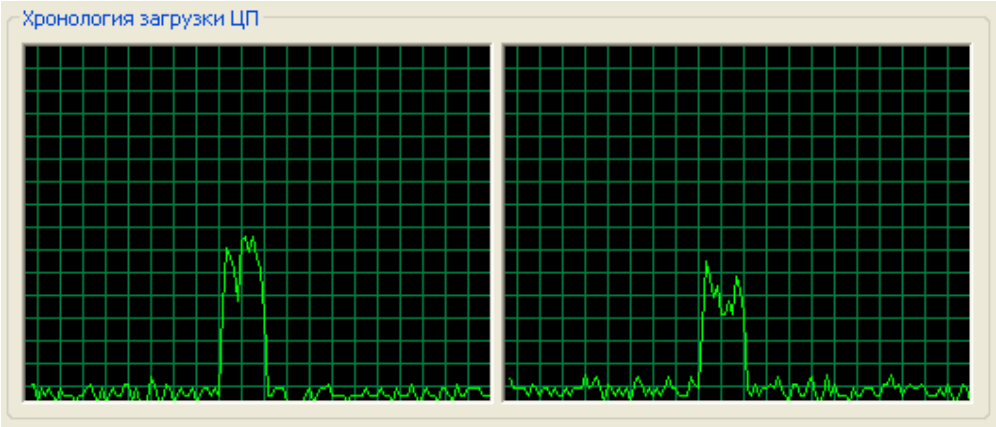


Рис. 4.18. Загрузка процессора на компьютере 1

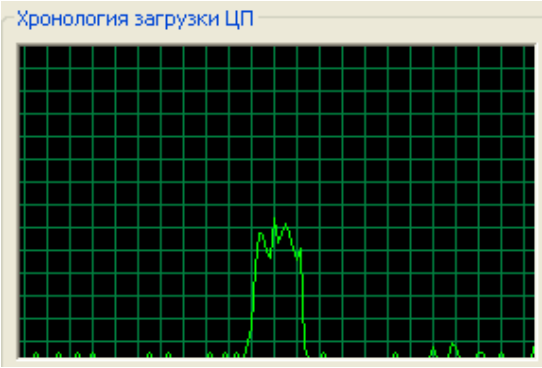


Рис. 4.19. Загрузка процессора на компьютере 2

2. Передача файла по сети с настроенной политикой IPsec, с использованием фильтра для обеспечения целостности передаваемых данных (протокол AH с использованием SHA-1). При этом время передачи данных возросло незначительно, до 12 с и 13 с, а скорость незначительно изменилась, до 8,75 Мбит/с и 8,08 Мбит/с на компьютерах 1 и 2 соответственно. При этом также незначительно возросла загрузка процессоров до 47% и 55% соответственно, как показано на рис. 4.20 и рис. 4.21.

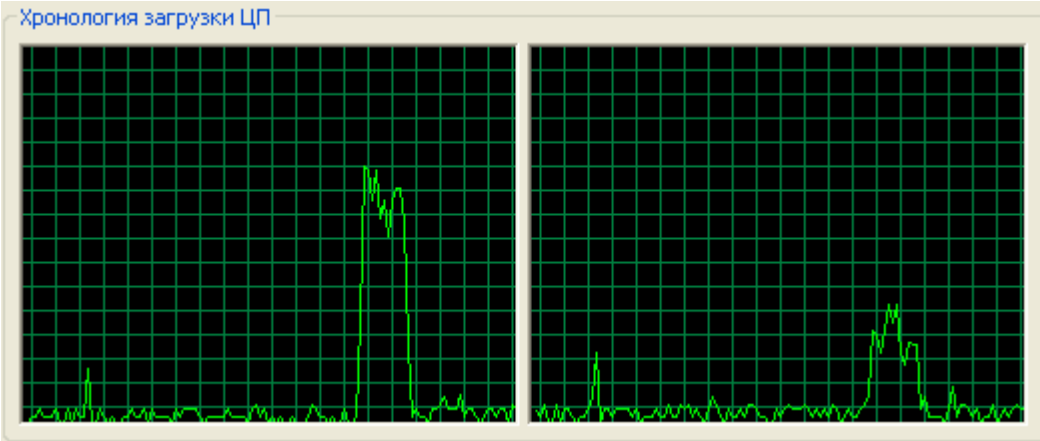


Рис. 4.20. Загрузка процессора на компьютере 1. AH (SHA1)

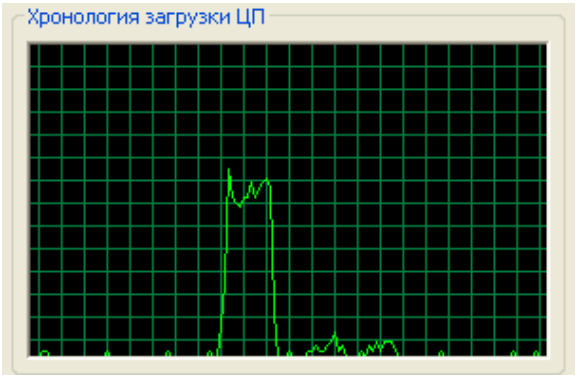


Рис. 4.21. Загрузка процессора на компьютере 2 AH (SHA1)

3. Передача файла по сети с настроенной политикой IPsec, с применением фильтра ESP без использования AH, с шифрованием при помощи алгоритма DES и хешированием MD5. Значительных изменений в производительности в этой конфигурации по сравнению с предыдущими не произошло. Время передачи файла возросло до 15 с и 16 с, а скорость передачи составила 7 Мбит/с и 6,56 Мбит/с на компьютерах 1 и 2

соответственно. Загрузка процессоров составила 50% и 65% соответственно, и показана на рис. 4.22 и рис.4.23.

Рис. 4.22. Загрузка процессора на компьютере 1. ESP (DES, MD5)

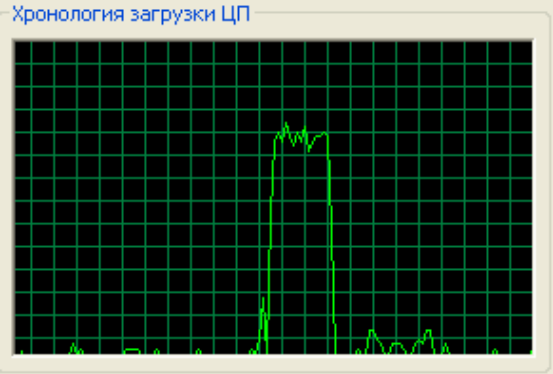


Рис. 4.23. Загрузка процессора на компьютере 2 ESP (DES, MD5)

DES является устаревшим алгоритмом и не рекомендуется к использованию там, где защищаемые данные имеют большую ценность, но стойкость этого алгоритма может быть значительно улучшена благодаря более частой смене ключа.

4. Передача файла по сети с настроенной политикой безопасности IPsec, с применением фильтра ESP, использующего шифрование при помощи алгоритма 3DES, вместо алгоритма DES, и хеширование MD5. При этом время передачи файла значительно возросло и составило 19 с и 29 с, а скорость передачи файла соответственно 5,53 Мбит/с и 3,62 Мбит/с. Уровень загрузки процессоров при этом составил 47% и 74% на 1 и 2 компьютере соответственно, и показан на рис. 4.24 и рис. 4.25.

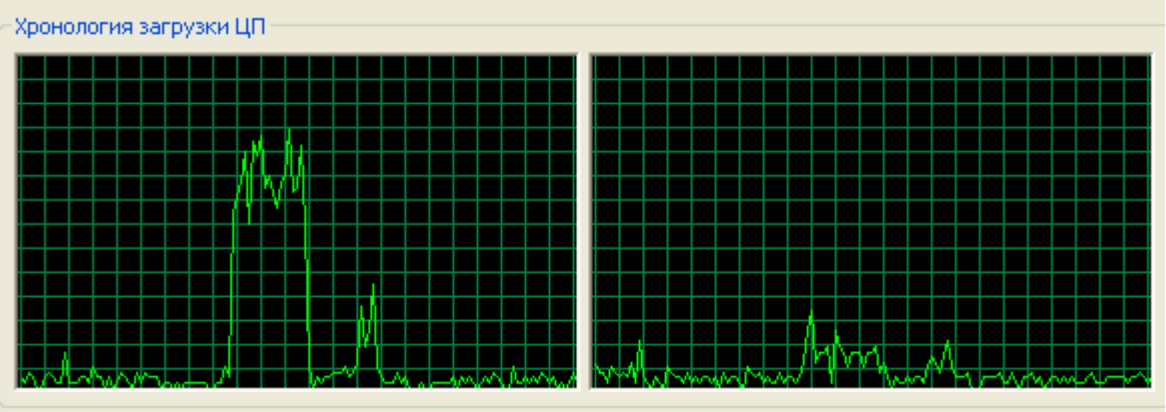


Рис. 4.24. Загрузка процессора на компьютере 1. ESP (3DES, MD5).

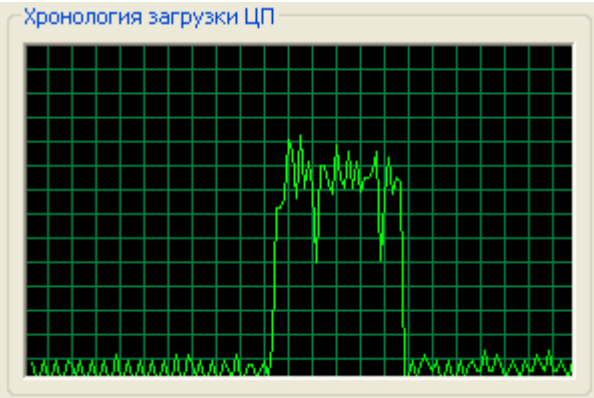


Рис. 4.25. Загрузка процессора на компьютере 2 ESP (3DES, MD5)

5. Передача файла по сети с настроенной политикой безопасности IPsec, с применением фильтра ESP с 3DES и SHA1. При этом время передачи файла составило 20 с и 31 с, а скорость передачи файла 5,25 Мбит/с и 3,39 Мбит/с соответственно. Уровень загрузки процессоров при этом составил 45% и 75%, как показано на рис. 4.26 и рис. 4.27.

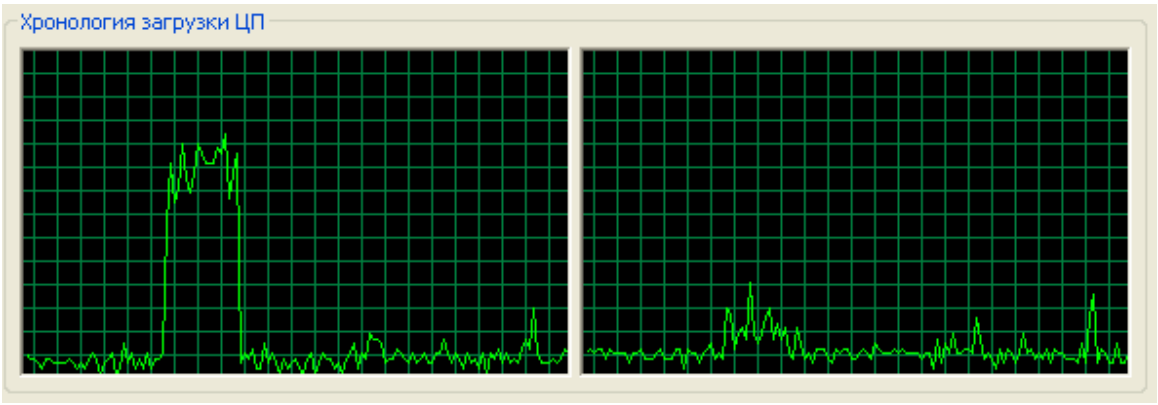


Рис. 4.26. Загрузка процессора на компьютере 1. ESP (3DES, SHA1)

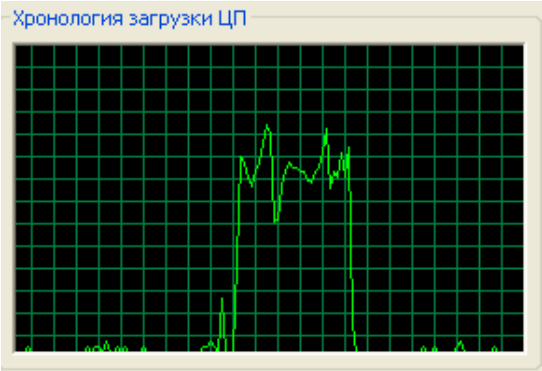


Рис. 4.27. Загрузка процессора на компьютере 2 ESP (3DES, SHA1)

6. Передача файла по сети с настроенной политикой безопасности IPsec, с использлванием протокола ESP совместно с протоколом AH. При этой наиболее безопасной, а следовательно, наиболее ресурсоемкой конфигурации, доступной в Windows XP, получены следующие результаты: время передачи увеличилось до 25с и 38 с, скорость упала до 4,20 Мбит/с и 2,76 Мбит/с на компьютере 1 и 2 соответственно. Загрузка процессоров составила 55% и 79% соответственно, и показана на рис. 4.28 и рис. 4.29.

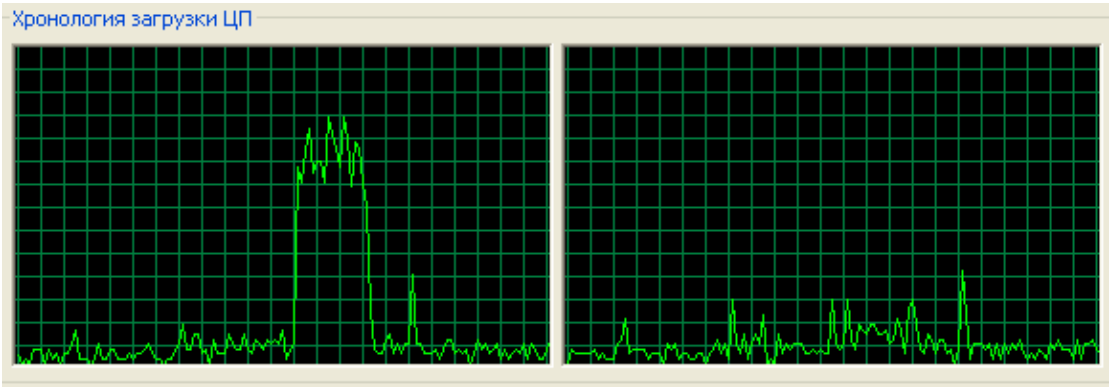


Рис. 4.28. Загрузка процессора на компьютере 1. ESP (3DES, SHA1) и AH(SHA1)

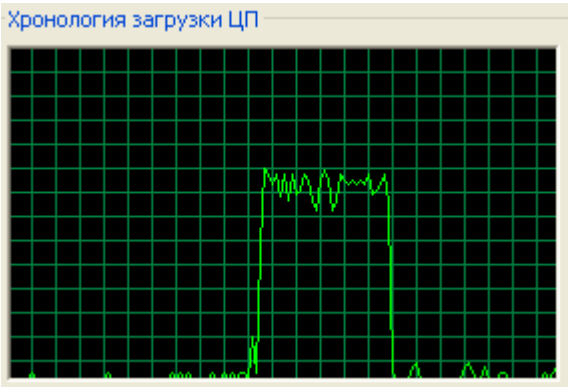
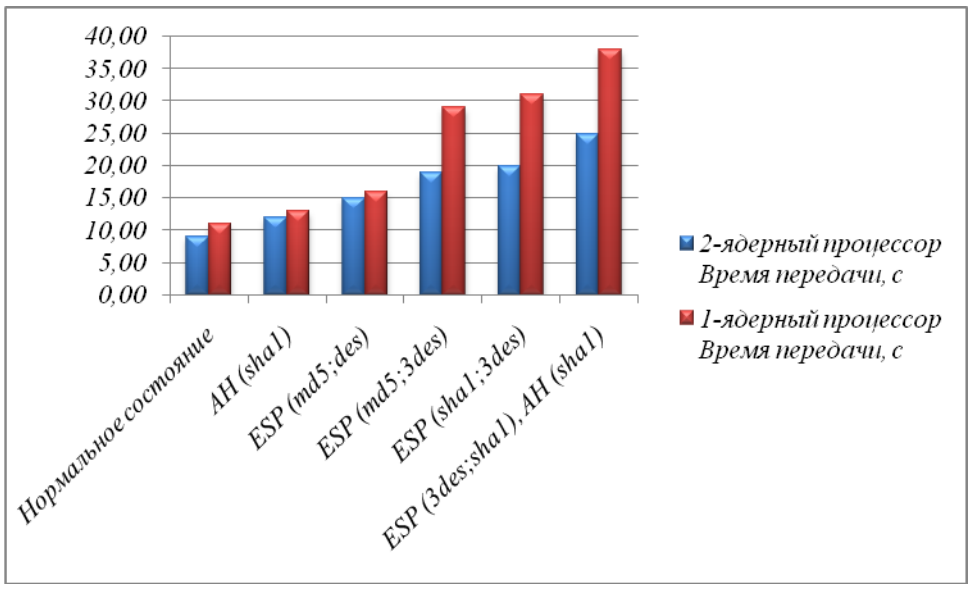
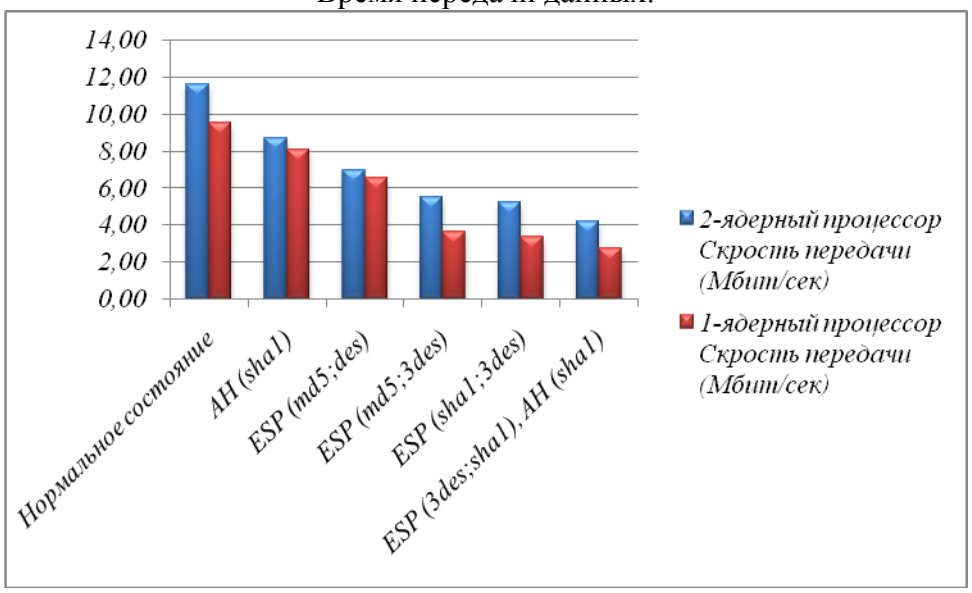


Рис. 4.29. Загрузка процессора на компьютере 2 ESP (3DES, SHA1) и AH(SHA1)



Время передачи данных.



Скорость передачи данных.

Рис. 4.30. Время и скорость передачи файла
в зависимости от используемых криптографических алгоритмов

В ходе тестирования можно было наблюдать, как изменяются время и скорость передачи от класса процессоров. Результаты тестирования (рис. 4.30) показывают, что ресурсоемкость IPsec невысока только при использовании протокола AH и при использовании протокола ESP с алгоритмом шифрования DES. При использовании протокола ESP с более сильным алгоритмом шифрования 3DES производительность значительно снижается, но, тем не менее, при низких скоростях передачи данных производительности даже устаревших процессоров будет достаточно. В

случаях, где требуется высокая скорость обмена данными, может оказаться достаточным использование алгоритма DES с частой сменой ключа.

Таким образом, IPsec может быть рекомендован для использования во многих сетях в целях повышения безопасности.

4.3 Настройка политики безопасности IPSec для работы в качестве межсетевого экрана

Протокол IPsec используется, в основном, для организации VPN-туннелей. В этом случае протоколы ESP и AH работают в режиме туннелирования. Кроме того, настраивая политики безопасности определенным образом, протокол можно использовать для создания межсетевого экрана.

Основным назначением межсетевого экрана является осуществление контроля и фильтрация проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. В общем случае, устанавливается набор правил (формируется фильтр), используя которые, экран просматривает все передаваемые и принятые системой пакеты. С пакетами, которые подпадают под критерии отбора, заданные в фильтре, экран производит необходимые действия.

Существует возможность использования IPSec, позволяющая реализовать подобие межсетевого экрана. Использование IPSec не является полноценной заменой файервола, однако позволяет реализовать множество сходных задач с использованием штатных средств ОС Windows.

Рассмотрим пример, в котором IPSec используется для того, чтобы запретить весь Интернет-трафик на локальной машине.

Для того, чтобы запретить весь обмен Интернет-трафиком на компьютере, необходимо настроить политику IPSec, запрещающую весь обмен данными по протоколам **HTTP** и **HTTPS**. Изображения диалоговых окон и последовательность действий будет показана ниже на примере использования ОС Windows XP.

Создать новую политику IPSec также возможно, используя консоль **MMC** (Пуск - Выполнить - mmc). В меню открывшегося окна консоли необходимо выбрать команду **Консоль**, затем пункт **Добавить или удалить оснастку** (рис. 4.31).

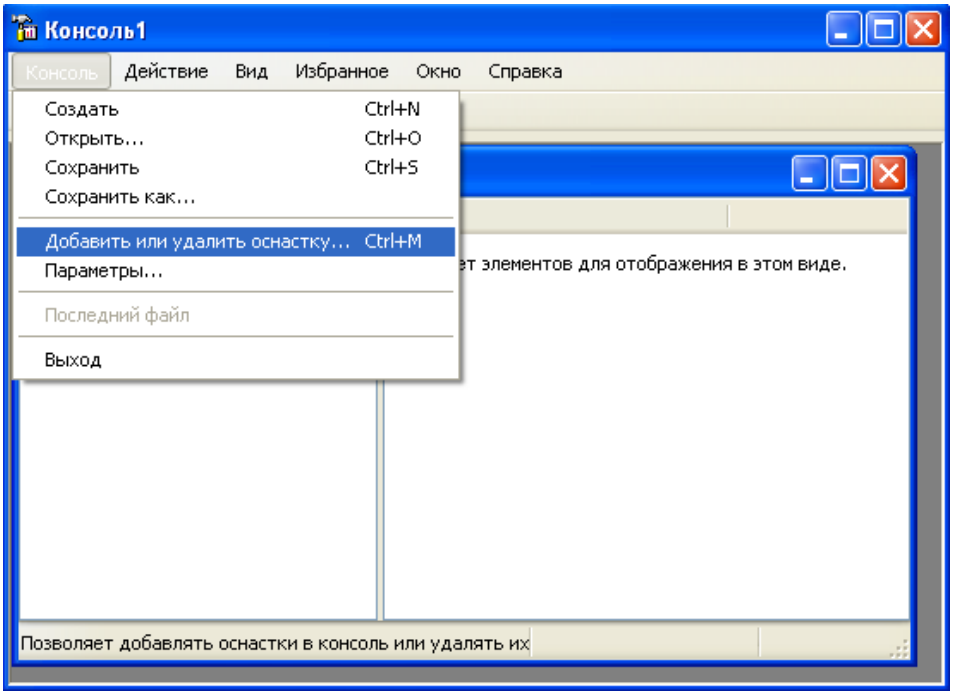


Рис. 4.31

Для управления IPSEC соединениями в Windows XP необходимо добавить оснастку «Управление политикой безопасности IP» (рис. 4.32).

После нажатия кнопки «Добавить», нужно указать, что политика безопасности применяется на локальном компьютере (рис. 4.33).

Далее необходимо последовательно закрыть окна, нажимая кнопки **Готово**, **Закрыть**, **ОК**. После чего на появившемся узле **Политики безопасности IP на «Локальный компьютер»** в левой панели консоли необходимо сделать щелчок правой кнопкой мыши и выбрать команду **Управление списками IP-фильтра** (рис. 4.34)**.**

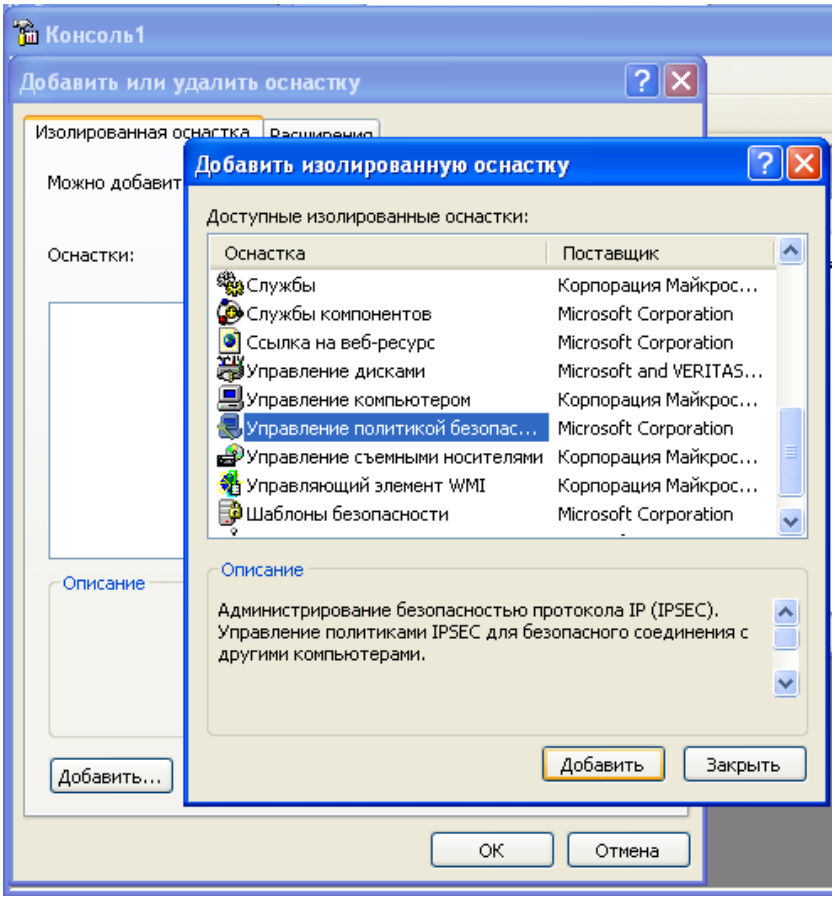


Рис. 4.32

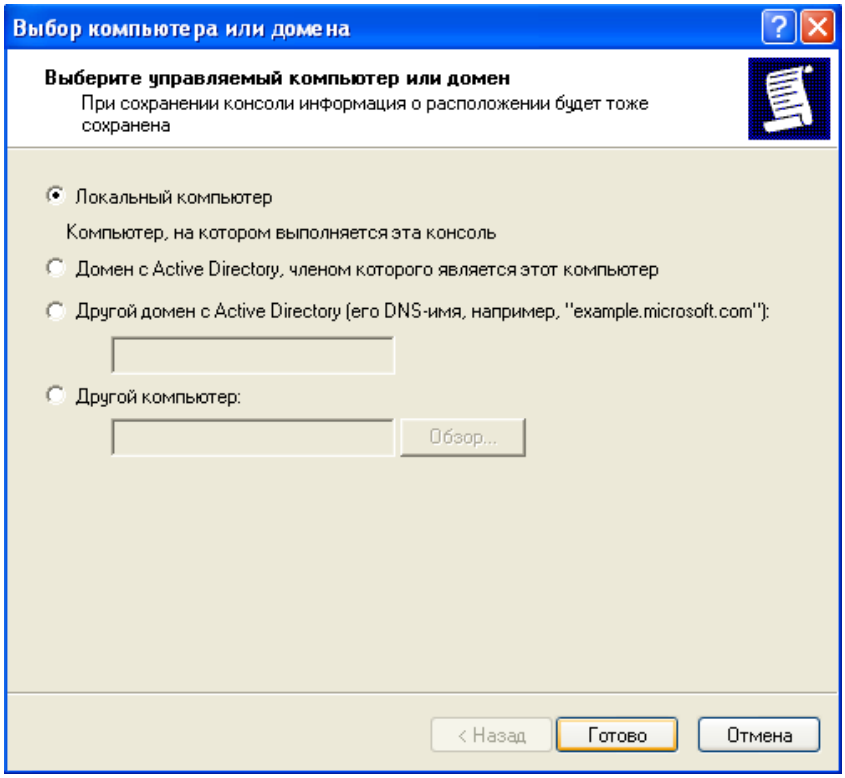


Рис. 4.33

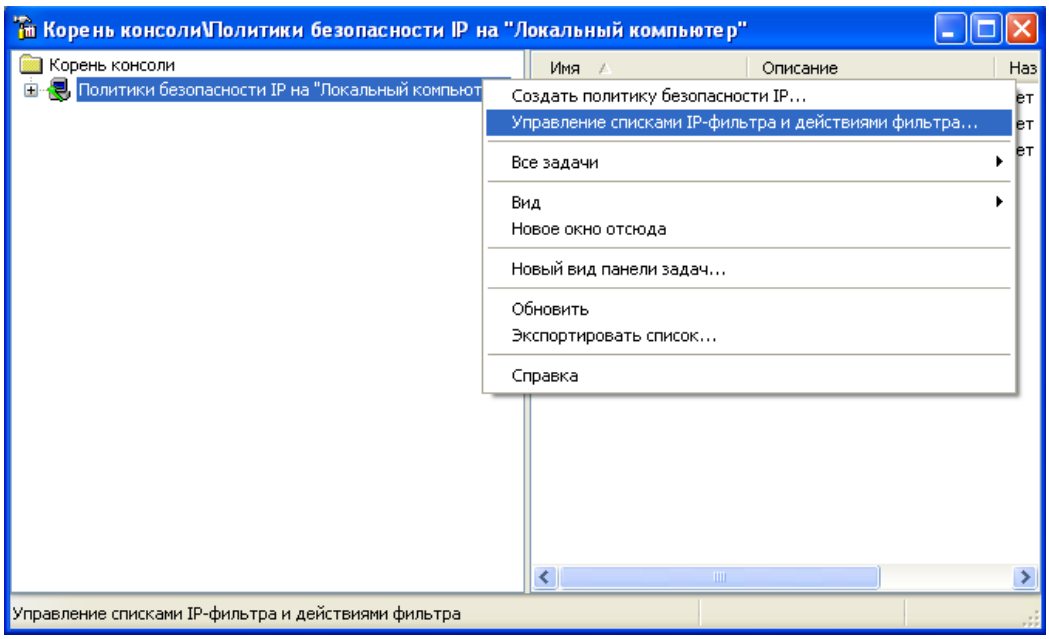


Рис. 4.34

В открывшемся диалоге при нажатии кнопки **Добавить** откроется окно **Список фильтров**. Необходимо задать название для нового фильтра, например, **HTTP, HTTPS,** и приступить к созданию фильтра, нажав кнопку **Добавить** (рис. 4.35)**.**

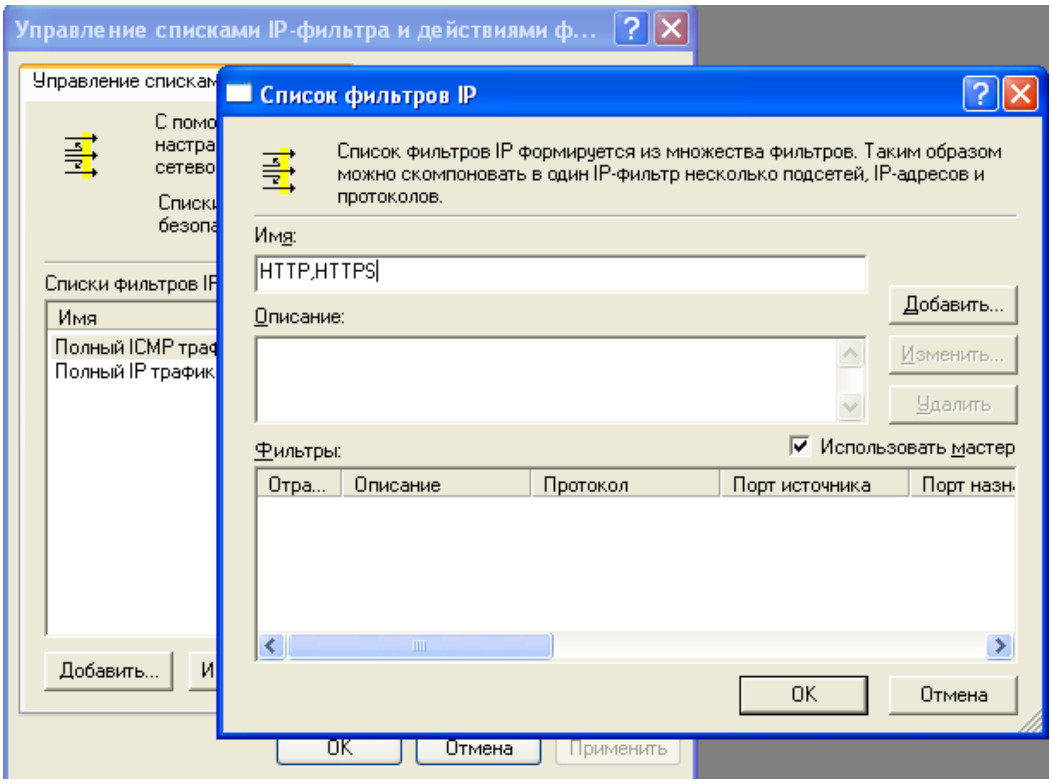


Рис. 4.35

Далее нужно указать адрес источника IP-пакетов, в данном примере необходимо указать **Мой IP-адрес** и нажать кнопку **Далее** (рис. 4.36)**.**

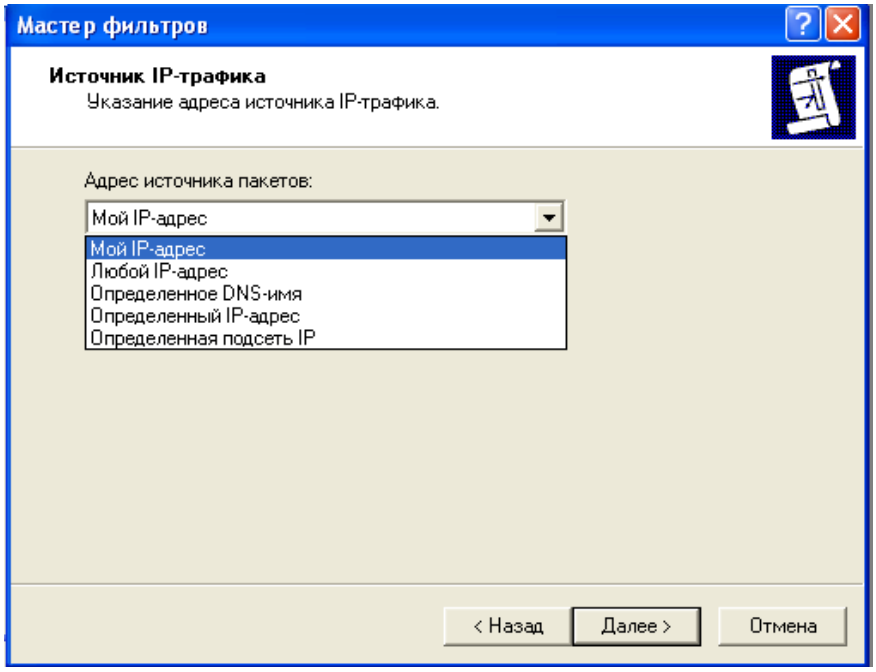


Рис. 4.36

В следующем окне также нужно задать адрес назначения, выбрав **Любой IP-адрес** (рис. 4.37)**.**

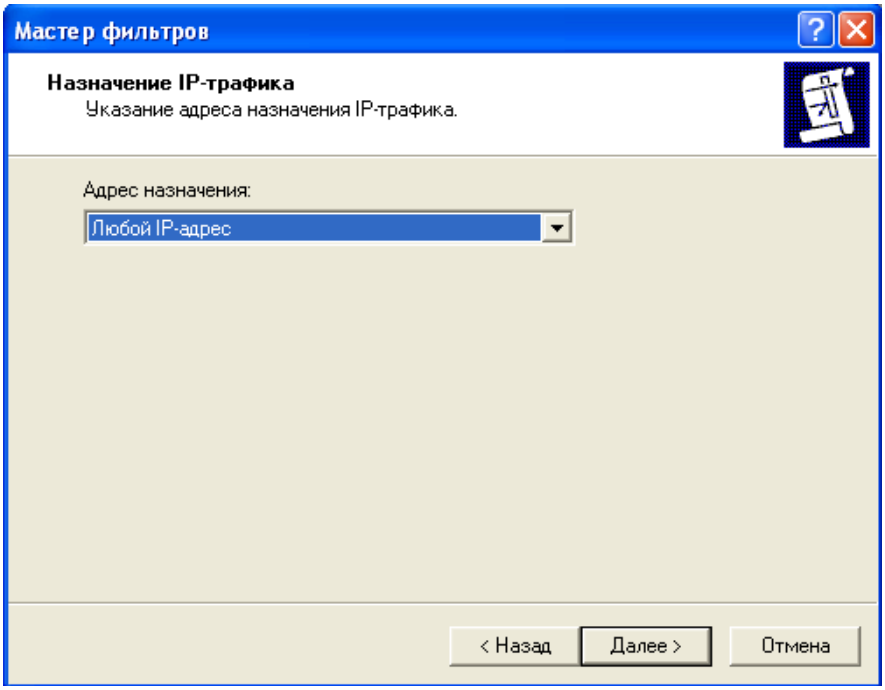


Рис. 4.37

Далее следует указать тип протокола. Для данной задачи необходимо выбрать протокол **TCP** (рис. 4.38) и далее задать номера портов (рис. 4.39)**.**

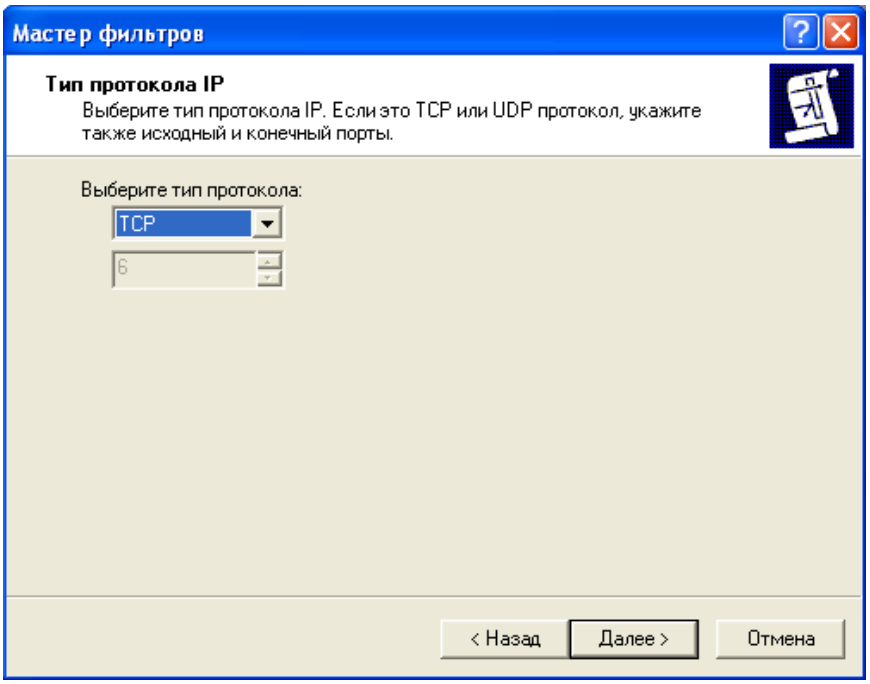


Рис. 4.38

Верхний переключатель следует оставить в положении **Пакеты из любого порта**, а нижний переключить в положение **Пакеты на этот порт** и ввести значение HTTP-порта **– 80** (рис. 4.39)**.**

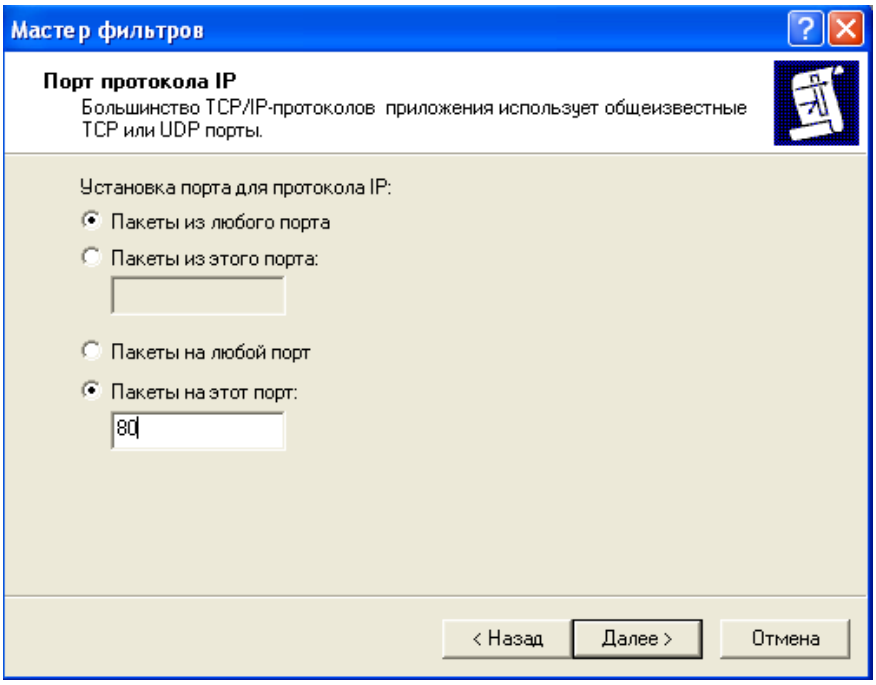


Рис. 4.39

После нажатия кнопки **Готово**, в нижнем окне списка появится созданный фильтр.

Далее, нажав кнопку **Добавить**, следует проделать все предыдущие операции еще раз, но уже указав значение порта **443** (для HTTPS). В списке нижнего окна должны находиться оба созданных правила фильтрации пакетов (рис. 4.40)**.**

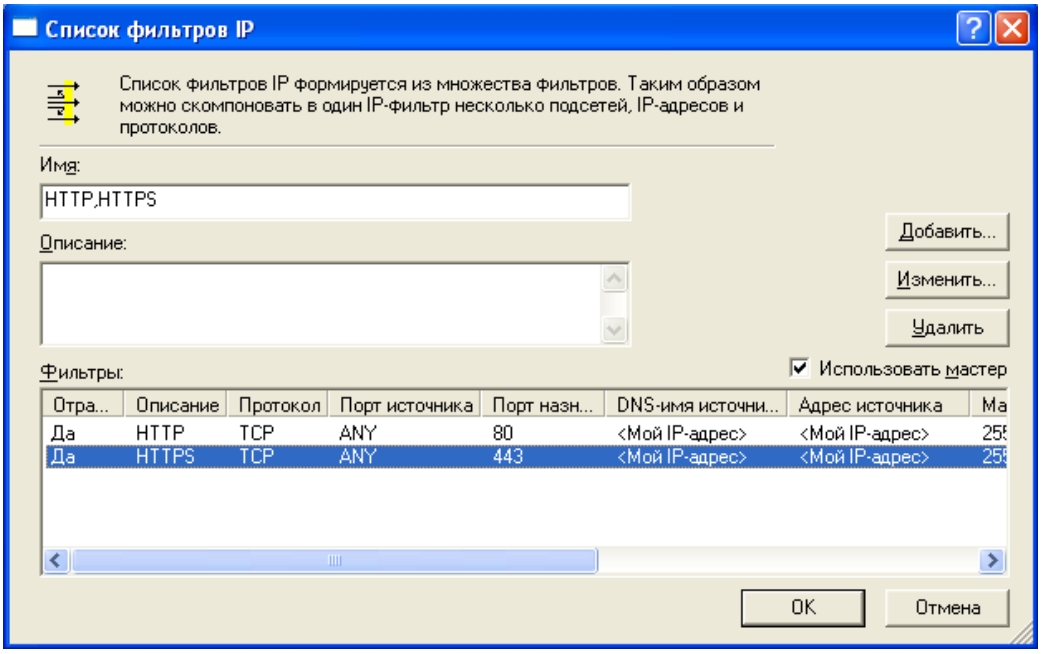


Рис. 4.40

Теперь необходимо определить действия, которые будет производить созданный фильтр. Для этого необходимо переключиться на закладку **Управление действиями фильтра** и нажать кнопку **Добавить** (рис. 4.41)**.**

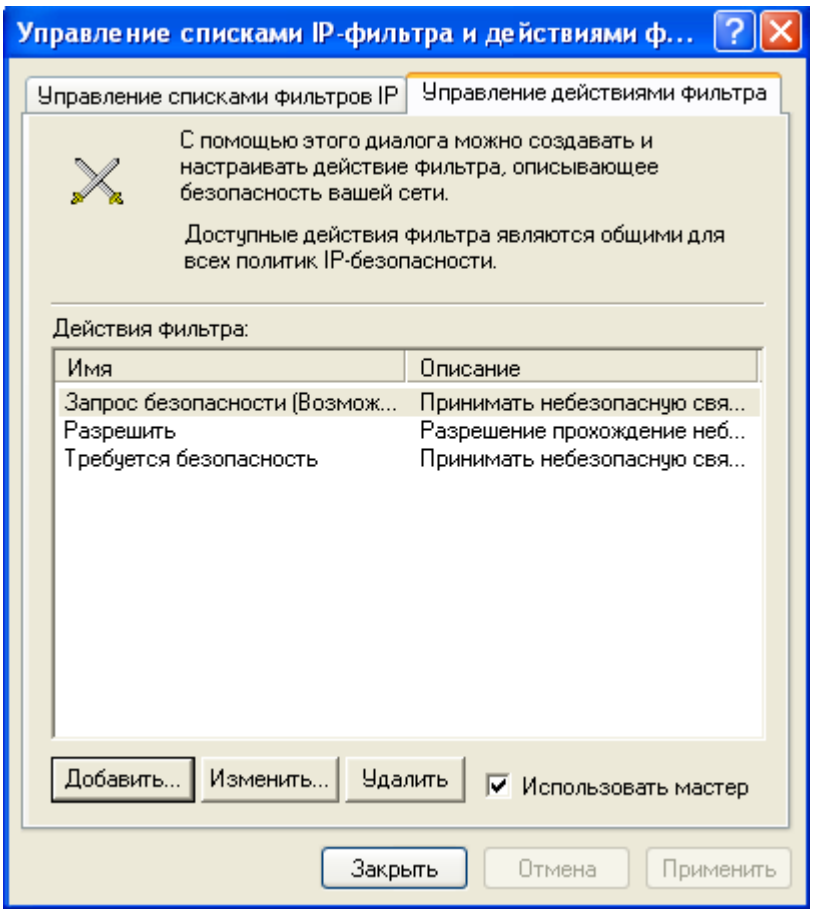


Рис. 4.41

После этого следует указать название действия, например, **Block, и нажать кнопку Далее** (рис. 4.42)**.**

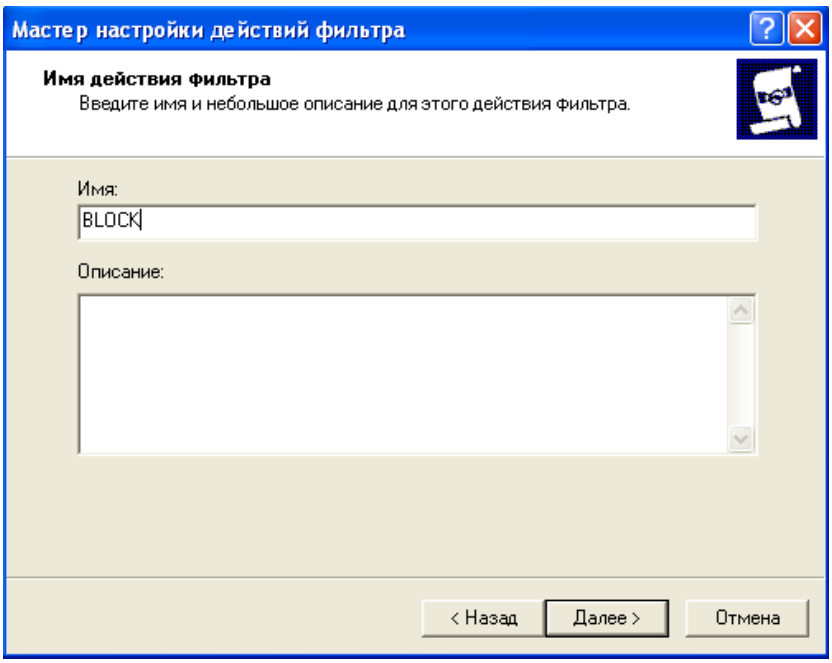


Рис. 4.42

В качестве действия нужно выбрать переключатель **Блокировать,** нажать **Далее** и **Готово** (рис. 4.43)**.**

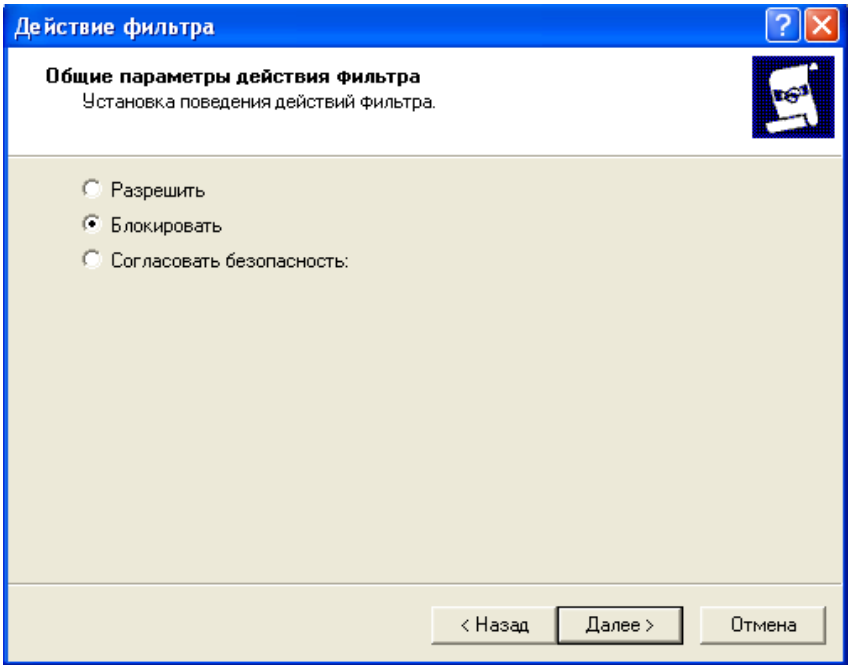


Рис. 4.43

Таким образом, фильтр создан, действие для него определено, осталось создать политику и назначить ее. В окне консоли MMC, нажать правой кнопкой мыши на узел **Политики безопасности IP** и выбрать команду **Создать политику безопасности IP** (рис. 4.44)**.**

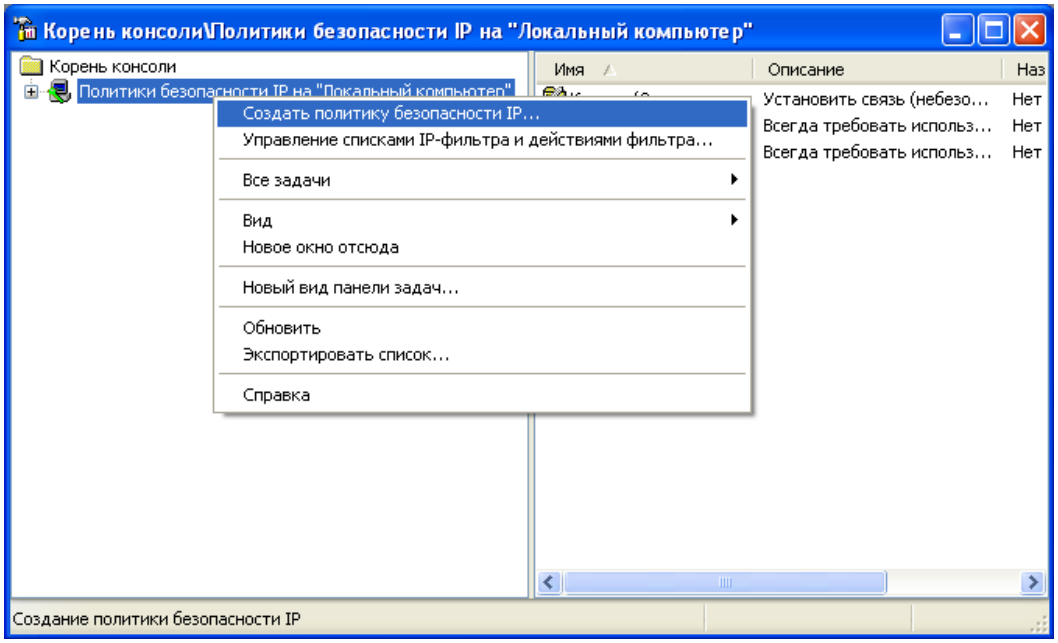


Рис. 4.44

В открывшемся окне мастера нужно указать политики, например, **Block Web** и нажать **Далее** (рис. 4.45)**.**

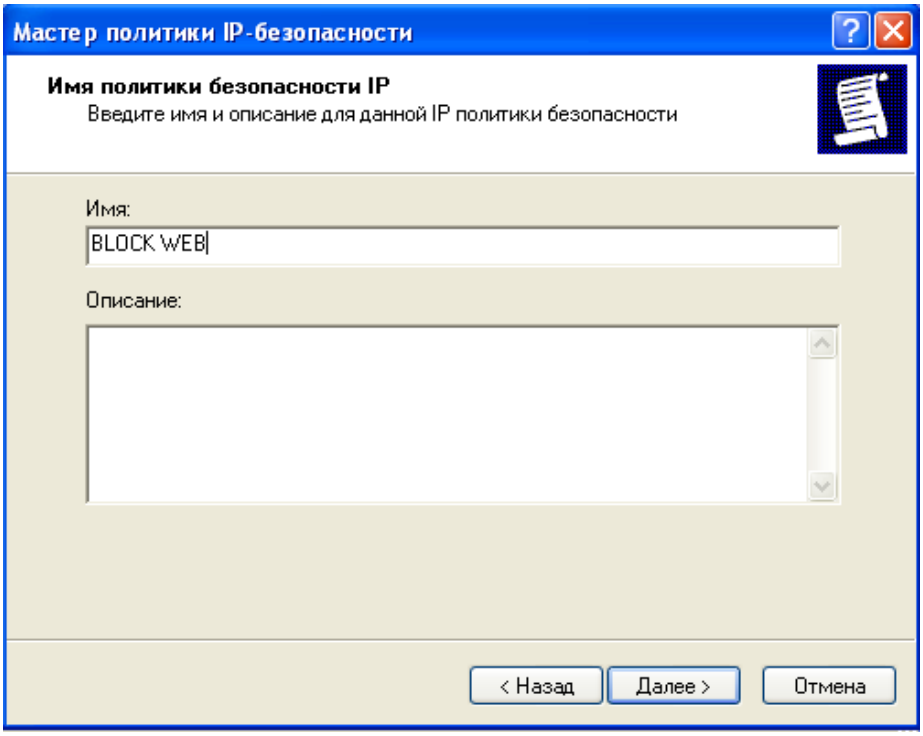


Рис. 4.45

В окне свойств политики необходимо нажать кнопку **Добавить** (рис. 4.46)**.**

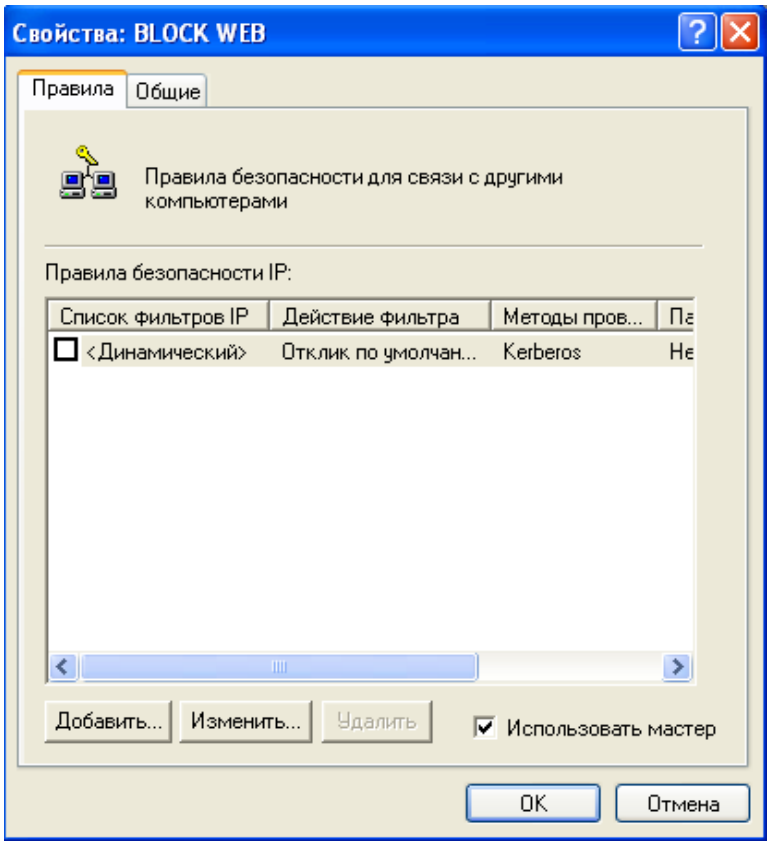


Рис. 4.46

После этого следует нажать **Далее**, оставив переключатель в положении **Это правило не определяет туннель**. Тип сети – следует указать **Все сетевые подключения**, нажать **Далее**. Теперь нужно выбрать созданный фильтр из списка (рис. 4.47)**.**

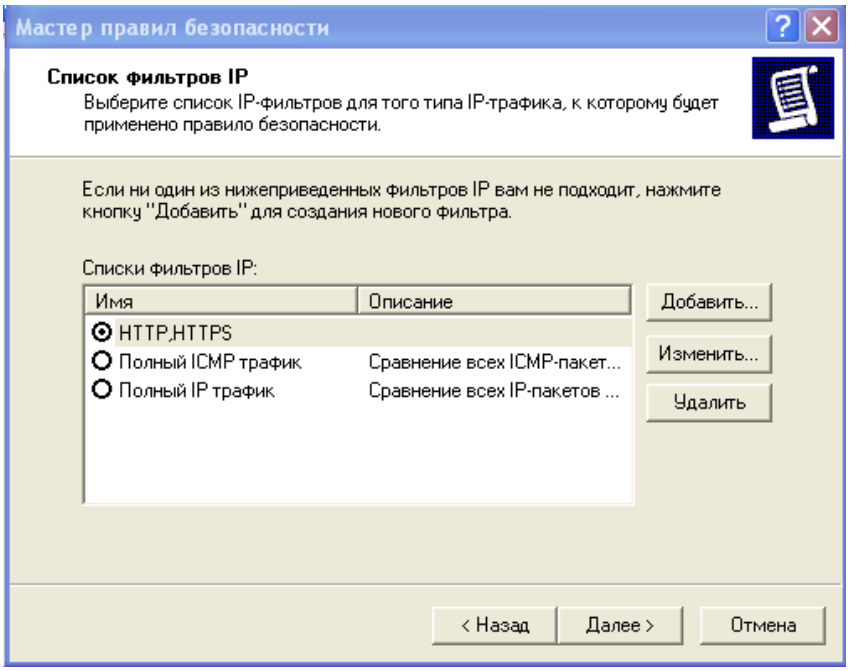


Рис. 4.47

Таким же образом следует выбрать созданное действие для фильтра – **BLOCK WEB**, нажать **Далее** и **Готово** (рис. 4.48)**.**

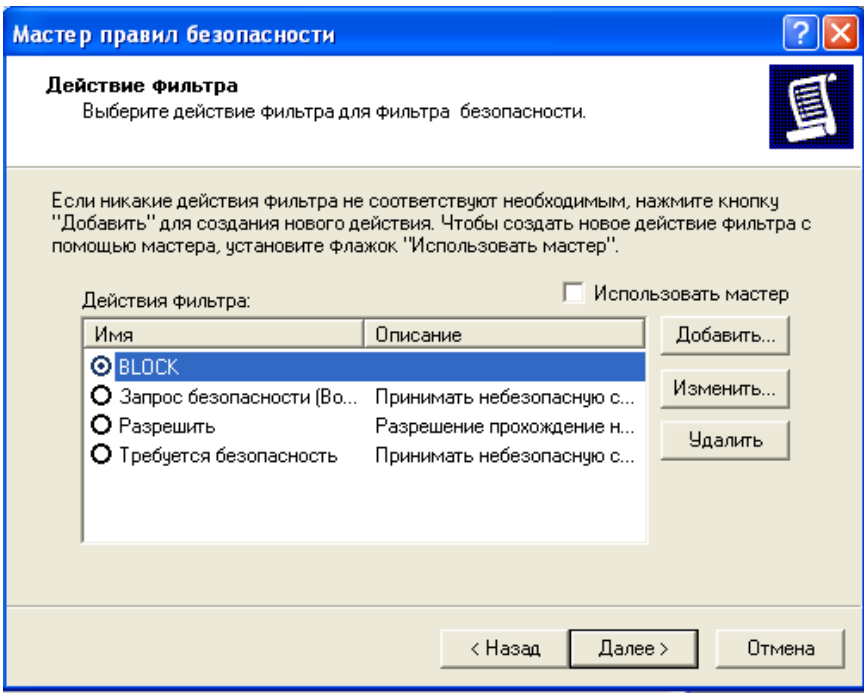


Рис. 4.48

Теперь в правой панели консоли MMC появится созданная политика с именем **BLOCK WEB**. Все, что осталось сделать – назначить ее. Для этого правый кнопкой мыши нужно вызвать меню и выбрать команду **Назначить** (рис. 4.49)**.**

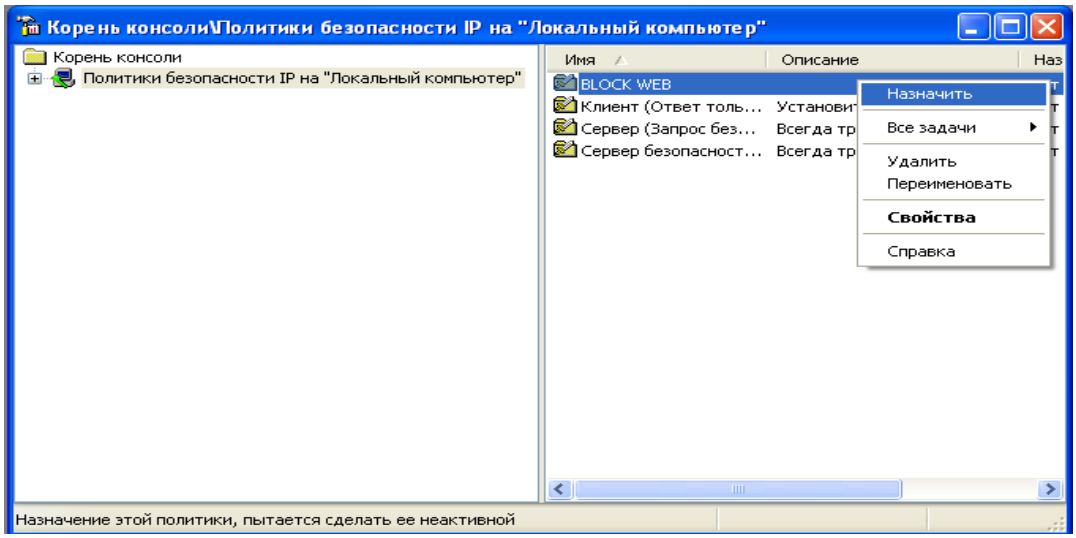


Рис. 4.49

Для проверки работы созданной политики IPSec следует запустить браузер. Если политика работает правильно, то страница браузера должна выглядеть следующим образом (рис. 4.50)**:**

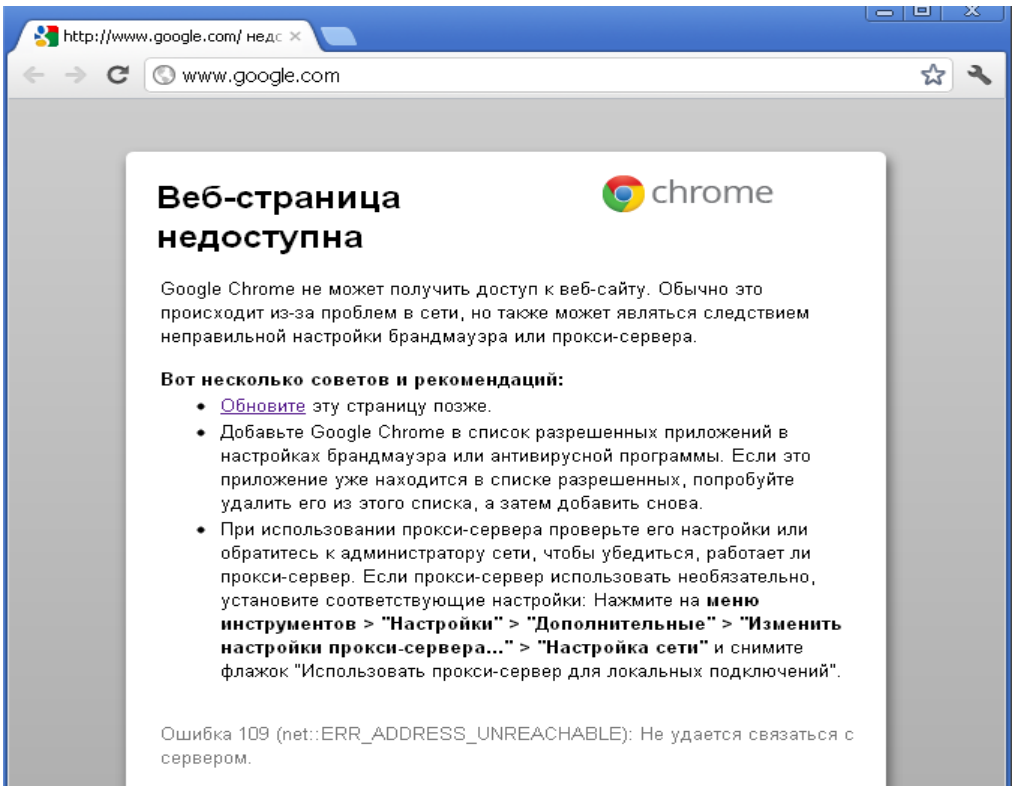


Рис. 4.50

Также можно добавить фильтр, который будет разрешать подключение только к определенным узлам Интернет. Для этого в консоли MMC необходимо дважды щелкнуть на название политики **BLOCK WEB**. В окне свойств нажать кнопку **Добавить**, затем двойным щелчком выбрать фильтр **HTTP, HTTPS**. На вкладке **Список фильтров добавить новый фильтр,** указав для него имя, нажать **Добавить**, **Далее**, в качестве источника пакетов выбрать вариант **Мой IP-адрес**, а в качестве адреса назначения выбрать строку **Определенное DNS-имя**, а в поле **Имя узла** указать имя определенного узла, к которому будет разрешено подключение. Теперь фильтр будет содержать два фильтра, один из которых запрещает весь http-трафик, а другой разрешает соединения с определенным IP-адресом.

Теперь, при переходе на разрешенный узел браузер должен отобразить содержание этого узла, ресурсы, расположенные на другом хосте (например, рекламные баннеры), не будут отображаться – они также будут фильтроваться примененной политикой IPSec.

5. Разработка видеоурока для изучения протоколов IPSec

5.1 Реализация учебного видео-пособия по настройке политики безопасности IPSec в ОС Windows XP

Учебное пособие реализовано как обучающий видео-курс. Представляет собой руководство по настройке брандмауэра в ОС Windows XP. Видео-курс может быть рекомендован как новая форма учебного пособия для студентов. В файле IPSecPolicy.Avi предоставлена пошаговая иллюстрация с голосовым сопровождением, записаны изображения, показывающее в точности то, что видит пользователь на экране монитора при настройке брандмауэра. Смена изображений отражает пошаговые действия, выполняемые при настройке. Голосовое сопровождение синхронизировано со сменой изображений и с движением курсора на экране компьютера. Запись данного курса выполнена с помощью программы UVScreen Camera version 4.4.0.97. Воспроизведение данного файла можно осуществить посредством различных проигрывателей, поддерживающих такой мультимедийный формат как AVI (проигрыватель Windows Media, Media Player Classic, AIMP, KMPlayer, RealPlayer, Amaroc, Beep Media Player, QuickTime Player и др.).

5.2 Тест для проверки знаний, полученных при обучении с помощью разработанного видеоурока

После работы с видеоуроком обучаемому предлагается пройти тест и проверить уровень усвоения материала. Разработанный тест целесообразно включить в тестовую систему, которая имеется на сайте кафедры ОПДС.

Тест «Протоколы IPSec»

1. На каком уровне модели OSI работает протокол IPSec?
    1. Прикладной
    2. Транспортный
    3. Сетевой
    4. Канальный

2. Какие алгоритмы IPSec использует для шифрования трафика?

1. HMAC-MD5, HMAC-SHA1
2. DES, 3DES
3. IKE
4. DH

3. Какие алгоритмы IPSec использует для проверки целостности передаваемых данных?

1. IKE
2. DH1, DH2, DH5
3. HMAC-MD5, HMAC-SHA1
4. DES, 3DES

4. Какой тип соединения поддерживает применение и транспортного, и туннельного режима?

1. Хост – Шлюз безопасности
2. Хост – Хост
3. Шлюз безопасности – Шлюз безопасности
4. Любое из перечисленных соединений может поддерживать только один из названных режимов

5. Выберете правильное утверждение:

1. Заголовок AH в туннельном режиме защищает только полезные данные и внутренний IP-заголовок
2. Заголовок AH в транспортном режиме защищает только полезные данные, но не IP-заголовок
3. Заголовок ESP в транспортном режиме защищает полезные данные и неизменяемые поля IP-заголовка
4. Заголовок ESP в туннельном режиме защищает весь исходный IP-пакет, включая внутренний IP-заголовок, но не защищает внешний IP-заголовок (правильный ответ)

6. Ассоциация безопасности однозначно задается тремя параметрами. Какой из перечисленных параметров не определяет SA?

1. Индекс параметров безопасности (SPI)
2. IP-адрес назначения
3. Версия протокола IP
4. Идентификатор протокола безопасности (AH или ESP)

7. Какую из служб безопасности не обеспечивает протокол AH?

1. Аутентификация

2. Конфиденциальность
3. Целостность данных
4. Защита от replay-атак

8. Какой из протоколов IPSec определяет процедуры обмена и управления секретными ключами соединения?

1. IKE
2. ESP
3. Kerberos v5
4. AH

9. Какой из перечисленных способов не используются в IPSec для проверки подлинности правил безопасности?

1. Использование протокола Kerberos v5
2. Использование цифровых сертификатов
3. Использование предварительного ключа
4. Использование фильтров

10. Что происходит во время первой фазы согласования IKE?

1. Происходит обмен данными между сообщающимися сторонами IPSec, который основывается на параметрах IPSec и ключах, хранимых в базе данных ассоциаций защиты

2. IKE-процесс выполняет аутентификацию сторон IPSec и ведет переговоры о параметрах ассоциаций безопасности IKE, в результате чего создается защищенный канал для ведения переговоров о параметрах ассоциаций безопасности IPSec в ходе второй фазы IKE

3. IKE-процесс ведет согласование параметров ассоциации безопасности IPSec, устанавливает соответствующие ассоциации безопасности IPSec для устройств сообщающихся сторон с целью создания туннеля IPSec

4. Трафик, которому требуется шифрование в соответствии с политикой защиты IPSec, согласованной сторонами IPSec, начинает IKE-процесс

11. Что происходит в результате второй фазы согласования IKE?

1. Происходит обмен данными между сообщающимися сторонами IPSec, который основывается на параметрах IPSec и ключах, хранимых в базе данных ассоциаций защиты.

2. IKE-процесс ведет согласование параметров ассоциации безопасности IPSec, устанавливает соответствующие ассоциации безопасности IPSec для устройств сообщающихся сторон с целью создания туннеля IPSec

3. IKE-процесс выполняет аутентификацию сторон IPSec и ведет переговоры о параметрах ассоциаций безопасности IKE, в результате чего создается защищенный канал для ведения переговоров о параметрах ассоциаций безопасности IPSec в ходе второй фазы IKE.

4. Трафик, которому требуется шифрование в соответствии с политикой защиты IPSec, согласованной сторонами IPSec, начинает IKE-процесс.

12. В каком режиме может происходить согласование параметров во время первой фазы согласования IKE?

1. Основной
2. Быстрый
3. Туннельный
4. Транспортный

13. В каком режиме происходит согласование параметров во время второй фазы согласования IKE?

1. Основной режим
2. Туннельный режим
3. Транспортный режим
4. Быстрый режим (правильный ответ)

14. Где располагаются заголовки протоколов безопасности AH или ESP при защите данных с помощью IPSec в транспортном режиме?

1. После IP-заголовка и всех настроек и перед заголовками протоколов верхних уровней
2. Перед IP-заголовком
3. Между внешним и исходным внутренним IP-заголовком
4. После всех полей защищаемого пакета IP

15. Где располагаются заголовки протоколов безопасности при защите данных с помощью IPSec в туннельном режиме?

1. После IP-заголовка и всех настроек и перед заголовками протоколов верхних уровней
2. Перед IP-заголовком.
3. Между внешним и исходным внутренним IP-заголовком.
4. После всех полей защищаемого пакета IP.

Далее приведены номера вопросов и соответствующие им правильные варианты ответов: 1 – 3, 2 – 2, 3 – 3, 4 – 2, 5 – 4, 6 – 3, 7 – 2, 8 – 1, 9 – 4, 10 – 2, 11 – 2, 12 – 1, 13 – 4, 14 – 1, 15 – 3.

5.3 Мероприятия по обеспечению безопасности жизнедеятельности при работе с персональным компьютером

В ходе дипломной работы был разработан видеоурок, представляющий собой электронное пособие, содержащее текстовое описание с иллюстрациями, презентацию и видеокурс. Разработанный видеоурок предполагает работу с компьютером.

При работе с компьютером для обеспечения безопасности и сохранения работоспособности необходимо соблюдать следующие рекомендации и меры предосторожности.

1. Обеспечение безопасности рабочего места.

1.1 Расположение оргтехники.

Дисплеи (мониторы) *с электронно-лучевой трубкой* являются источниками электромагнитного излучения. Рекомендуется устанавливать защитный экран для снижения воздействия электромагнитного излучения от задней части другого дисплея, при этом недопустимо устанавливать рабочие компьютеры близко друг от друга. Недопустимо работать напротив боковой или задней части другого дисплея, если расстояние до него менее 2 м.

Размещать компьютер необходимо вдали от отопительных приборов и исключать попадания на него прямых солнечных лучей. Системный блок для настольного компьютера помещается на крепкую надежную поверхность, чтобы исключить даже случайное сотрясение.

Центр экрана должен быть расположен на 15-20 см ниже уровня глаз. Расстояние от глаз до экрана должно составлять не менее 50 см. Клавиатура располагается на расстоянии 15-30 см от края столешницы или на специальной выдвижной доске. Необходимо следить, чтобы бумаги, какие-либо предметы не закрывали вентиляционные отверстия работающих аппаратов.

1.2. Рабочая мебель.

Кресло – ширина и глубина сиденья не менее 40 см.; спинка: высота опорной поверхности 30±2 см; ширина не менее 38 см.; подлокотники: длина не менее 25 см; ширина 5-7 см., высота над сиденьем 23+3 см.

Стол – размеры рабочей поверхности (столешницы): длина – 80-120 см; ширина – 80-100 см.; высота (расстояние от пола до рабочей поверхности) 68-85 см; оптимальная высота 72,5 см.;

1.3 Помещение.

В рабочем помещении освещение должно быть естественным и искусственным. Освещение не должно создавать блики на поверхности экрана дисплея. Сдерживать поток избыточного света от окон следует с помощью жалюзи (или тканевых штор);

При работе за компьютером обязательно соблюдение чистоты. Влажную уборку помещения следует проводить ежедневно. Недопустима запыленность воздуха, пола, рабочей поверхности стола и техники.

1.4 Микроклимат.

Температура воздуха – от 21 до 25°С (в холодное время года); от 23 до 25˚С (в теплое время года); влажность воздуха (относительная) – от 40 до 60%. Недопустимы резкие перепады температуры и влажность воздуха более 75%.

Ионизация воздуха – образующиеся в помещении положительно заряженные ионы очень вредны для здоровья, вызывают быстрое утомление, головную боль, учащение пульса и дыхания (из-за недостаточного поступления кислорода в кровь). Специальные устройства – аэроионизаторы – нормализуют аэроионный режим, увеличивая концентрацию легких отрицательно заряженных ионов.

Необходимо в начале работы включать общее питание, периферийные устройства, системный блок, в конце работы наоборот – выключать системный блок, периферийные устройства, общее питание. Не обязательно выключать компьютер на время небольших перерывов в работе.

Перед подсоединением/отсоединением устройств ввода-вывода требуется полностью отключать эту технику и компьютер от электросети.

При появлении запаха гари или при обнаружении повреждения изоляции, обрыва провода следует немедленно отключить устройства от электросети.

Недопустимо попадание влаги на системный блок, дисплей, клавиатуру и другие устройства.

При интенсивной работе резко возрастает напряженность электрического поля на клавиатуре и «мыши». От трения рук о них через 0,5-1 час работы электростатический потенциал достигает 10-20 кВ/м, что оказывает на организм вредное воздействие. Работать с «мышью» нужно на специальном коврике. Рекомендуется регулярно проводить влажную антистатическую обработку помещения, ежедневно протирать влажной салфеткой экран дисплея, клавиатуру, «мышь» для снятия статического электричества.

6. Рабочая поза.

Правильная рабочая поза позволяет избегать перенапряжения мышц, способствует лучшему кровотоку и дыханию. Следует сидеть прямо (не сутулясь) и опираться спиной о спинку кресла. Недопустимо работать, развалившись в кресле. Такая поза вызывает быстрое утомление, снижение работоспособности. Необходимо найти такое положение головы, при котором меньше напрягаются мышцы шеи. Рекомендуемый угол наклона головы – до 20°. В этом случае значительно снижается нагрузка на шейные позвонки и на глаза.

Во время работы за компьютером необходимо расслабить руки, держать предплечья параллельно полу, на подлокотниках кресла, кисти рук – на уровне локтей или немного ниже, запястья – на опорной планке. Необходимо сохранять прямой угол (90°) в области локтевых, тазобедренных, коленных и голеностопных суставов. Также следует чаще моргать и смотреть вдаль. Моргание способствует не только увлажнению и очищению поверхности глаз, но и расслаблению лицевых, лобных мышц. Малая подвижность и длительное напряжение глазных мышц могут стать причиной нарушения аккомодации. При ощущении усталости глаз нужно в течение 2-3 минут окинуть взглядом комнату, устремлять взгляд на разные предметы, смотреть вдаль.

Заключение

В дипломной работе отражена история возникновения сети Интернет, возможности и услуги, предоставляемые пользователям Сети. Рассмотрена актуальная для пользователей проблема – обеспечение информационной безопасности в сети Интернет. Классифицированы основные угрозы информационной безопасности и способы борьбы с ними, названы основные и наиболее распространенные в настоящее время системы и протоколы безопасности, обеспечивающие защиту пользователей от несанкционированного доступа и вирусных атак.

Основное внимание уделено протоколам открытой структуры IPSec. Раскрыты принципы работы протоколов IPSec при передаче данных по сети с использованием механизмов защиты, реализованных этими протоколами.
Рассмотрены режимы работы ассоциаций безопасности, случаи, для которых необходимо применение того или иного режима, а также рассмотрена защита данных с помощью IPSec для IPv4 и IPv6.

Приведены результаты анализа работы компьютера и скорости передачи данных при использовании протоколов безопасности IPSec с различными комбинациями алгоритмов шифрования, способов аутентификации и механизмов обеспечения целостности передаваемых данных. Проведенный анализ показал, что для использования более мощных и стойких алгоритмов защиты информации требуются более производительные процессоры. В противном случае время передачи данных будет увеличиваться, что может отрицательно сказаться на производительности работы сети.

В дипломной работе также рассмотрены преимущества и недостатки использования протоколов IPSec для обеспечения безопасности передаваемых данных, и даны рекомендации по наиболее эффективному использованию этих протоколов.
Также разработаны рекомендации для пользователей услуг сети Интернет по настройке политики IPSec на персональных компьютерах, представлен обучающий видеоурок по настройке политики безопасности IPSec в ОС Microsoft Windows XP. Для оценки знаний, полученных с помощью видео-курса, составлен тест с контрольными вопросами.

Список используемой литературы

1. RFC 4302
2. RFC 4303
3. У. Блэк «Интернет: протоколы безопасности. Учебный курс». – СПб: Питер, 2001. – 288с.:ил.
4. Олифер В.Г., Олифер Н.А. «Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов», 2006.
5. Крейг Хант «TCP/IP. Сетевое администрирование». Третье издание. СПб, 2008.
6. Казарин О.В. «Безопасность программного обеспечения компьютерных систем», Москва, МГУЛ, 2003. – 212 с.
7. W. Odom. CCNA ICND2 Official Exam Certification Guide, 2nd Edirion. Cisco Press. Aug 30, 2007.
8. Журнал "Information Security/ Информационная безопасность" #6, 2009.
9. Виктор Сердюк, "Бухгалтер и компьютер", №1, 2007.
10. ГОСТ Р ИСО/МЭК 13335-1 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
11. http://www.opennet.ru
12. http://www.internetworldstats.com
13. Официальный сайт Cisco http://www.cisco.com
14. http://technet.microsoft.com
15. http://www.ietf.org