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

Факультет СС, СК и ВТ

Дипломная работа

на тему

«Анализ способов и средств обеспечения информационной безопасности пользователей услуг Интернет»

Дипломник Володченко М. А.

Руководитель работы Доронин Е. М.

Санкт-Петербург

2011 г.

РЕФЕРАТ

Тема дипломной работы: «Анализ способов и средств обеспечения информационной безопасности пользователей услуг Интернет».

Пояснительная записка включает в себя: 98 страниц текста, 42 рисунка, 8 таблиц.

Ключевые слова: Интернет, услуги, информационная безопасность, угрозы, вирус, спам, атаки, несанкционированный доступ (НСД), антивирусные программы, брандмауэр, шифрование, электронная цифровая подпись (ЭЦП), прокси-сервер, протоколы, «облачные» технологии.

Цель работы: провести анализ имеющихся на сегодняшний день типов угроз информационной безопасности пользователей услуг сети Интернет, оказать помощь в обоснованном подборе и результативном использовании необходимых способов и средств защиты персонального компьютера и локальных сетей в борьбе с различного рода атаками.

В ходе дипломной работы рассмотрены основные услуги сети Интернет, а также деструктивные факторы, существующие в Сети, и последствия их разрушительного воздействия. Проведен анализ способов и средств защиты информации пользователей услуг Интернет от НСД, вирусных атак и других негативных факторов. Приведены результаты сравнительного анализа последних версий современных антивирусных программ. Даны описания и схемы подключения межсетевых экранов. Разработан обучающий видео-курс по настройке брандмауэра в ОС Microsoft Windows XP. Составлены рекомендации пользователям услуг Интернет.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Новые информационные технологии успешно внедряются во все сферы человеческой деятельности. Появление глобальных и локальных сетей передачи данных предоставило новые возможности быстрого обмена информацией. Благодаря всемирной сети Интернет с помощью стека протоколов TCP/IP и единого адресного пространства объединяются не только корпоративные и ведомственные сети, но и обычные пользователи, которые имеют прямой доступ в Интернет со своих домашних компьютеров. При этом естественное желание пользователей, иметь постоянный доступ к своей персональной информации и информации для домашней и служебной деятельности и быть уверенными, в невозможности ее неправомерного использования. Проблема обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных систем и хранящейся и обрабатываемой ими информации требует постоянного внимания и поиска рациональных путей ее решения.

Сегодня термин «информация» часто используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость вычислительной системы, в пределах которой он существует. При появлении угроз, связанных с возможностью потери, искажения, раскрытия конфиденциальных данных и утечке определенной информации, организация или государство в целом может потерять не только большие суммы денег, но и репутацию на политическом и экономическом уровне.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается и уровень угроз для используемых информационных технологий. Именно поэтому посредством использования современных способов и средств защиты целостности и конфиденциальности информации (антивирусных программ, межсетевых экранов, программных и аппаратных продуктов для защиты

информации от НСД и 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 предлагаемой дипломной работе рассмотрены возможные виды атак персонального компьютера и локальной сети, как со стороны локальных сетей, так и со стороны сети Интернет. Предложены способы и средства обеспечения информационной безопасности, разработаны руководства по настройке и работе аппаратных и программных средств защиты ПК, для обоснования выбора приведены результаты исследований средств защиты.

1. ИНТЕРНЕТ. ОБЩИЕ СВЕДЕНИЯ

Интернет – это информационно-коммуникационная инфраструктура открытого доступа, образующая виртуальную интерактивную информационную среду, в которой в интересах неограниченного круга пользователей обеспечивается глобальный оборот информации в различных режимах доступа, представленной в электронно-цифровой форме.

Это глобальная информационная система, которая логически соединена посредством адресного пространства, основанного на протоколе IP (Internet Protocol - протокол Интернета) или заменяющих его протоколах, поддерживает передачу данных, используя протокол TCP (Transmission Control Protocol - протокол управления передачей) или заменяющие его протоколы, предоставляет и использует прикладные сервисы, основанные на коммуникациях и связанной с ними инфраструктуре. Это определение было дано Федеральным советом США по компьютерным сетям (FNC - Federal Networking Couneil) 24.10.1995 г.

1.1. История создания сети Интернет

В 1958 году в Вашингтоне в Агентстве передовых оборонных исследовательских проектов (ARPA - Advanced Research Projects Agency), созданном под эгидой Министерства обороны США, были начаты работы по созданию специальной компьютерной сети. В это же время проблемами связи между удаленными компьютерами занимались ученые и специалисты из Английской Национальной физической лаборатории (NPL – National Physical Laboratory). Совместно коллективы ARPA и NPL пришли к результатам формы представления сообщений при передаче их между компьютерами: «…сообщения разделяются на блоки определенного формата, которые включают в себя заголовок и признак конца блока».

2 сентября 1969 года был осуществлен обмен сообщениями между двумя узлами сети, названной ARPANET (Advanced Research Projects Agency

Network), находящимися на расстоянии в 640 км. Один компьютер был установлен в Калифорнийском университете Лос-Анджелеса, а второй - в Стенфордском исследовательском институте. Эту дату считают днём рождения Интернета.

К концу 1969 года четыре компьютера были объединены каналами со скоростью 56 кбит/с.

К 1971 году была разработана первая программа для отправки электронной почты по сети.

В 1973 году, когда к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной.

В 1974 году в статье В. Серфа и Р. Кана, которая была посвящена протоколу транспортного уровня TCP, впервые был использован термин «Internet». В 1975 году группа этих ученых разработала спецификации стека протокола TCP/IP.

1 января 1983 года сеть ARPANET перешла с протокола NCP (Network Control Protocol – протокол управления сетью), который был первым стандартом сетевого протокола в ARPANET, на TCP/IP, который успешно применяется до сих пор.

В 1984 году была разработана система доменных имён (DNS –Domain Name System).

В 1989 году в Европейском совете по ядерным исследованиям (CERN - фр. Conseil Européen pour la Recherche Nucléaire) была предложена концепция Всемирной паутины (WWW - World Wide Web). Её предложил британский физик Томас Бернерс-Ли, он же в течение двух лет разработал протокол HTTP (Hypertext Transfer Protocol – протокол передачи гипертекстовых файлов), язык гипертекстовой разметки web-страниц - HTML (Hypertext Markup Language) и единообразные идентификаторы ресурсов URI (Uniform Resource Identifier).

На протяжении 70-х и начала 80-х годов прошлого века, сеть Интернет использовалась преимущественно американским правительством, академическими, исследовательскими и военными организациями.

Начиная с 90-х годов, с появлением ОС Windows 95 с интегрированным стеком TCP/IP, услуги Интернет стали доступны миллионам пользователей, и развитие Интернет началось с огромной скоростью. Сегодня сеть Интернет представляет собой всемирную систему объединенных между собой компьютерных сетей, построенных на стеке протоколов TCP/IP.

С 22 января 2010 года прямой доступ в Интернет получил экипаж Международной космической станции.

Сегодня по сети Интернет передаются не только данные, но и речевая информация и видео. Сотни миллионов пользователей знают и используют приложения, реализуемые в сети Интернет (WWW, e-mail, ICQ, Skype и др.).

1982 год можно считать началом развития сети Интернет в России. В этом году в Институте атомной энергии им. И. В. Курчатова были начаты работы по созданию отечественной UNIX-подобной ОС. В 1990 году была основана компьютерная сеть РЕЛКОМ, которая базировалась на технологии электронной почты, с возможностью переписки на русском языке. В этом же году был осуществлен первый сеанс связи с Финляндией по международному телефону и зарегистрирован домен верхнего уровня SU. В 1992 году сеть РЕЛКОМ была официально зарегистрирована как часть панъевропейской сети EUnet, которая стала крупнейшей в Европе. Тогда же была начата реализация проекта создания научной некоммерческой сети RELARN, головной организацией которой стал РосНИИРОС. Было организовано оперативное распространение по сети электронных версий газеты «Известия» и других отечественных периодических изданий.

В 1993 году сеть РЕЛКОМ была официально подключена к сети Интернет и зарегистрирован домен RU; этот факт можно считать началом присутствия России в Интернет, поскольку легальными признаются только

IP-сети, зарегистрированные в NSFnet (National Science Foundation Network - компьютерная сеть Национального фонда науки США).

В 1995 году в России начато распространение IP-доступа и WWW-технологий. В том же году по инициативе ФАПСИ была начата работа по проекту «Деловая сеть России», который предусматривал создание сети для коммерческих применений, включая решение проблемы обеспечения сохранности информации. Участниками осуществления проекта стали ФАПСИ, «Ростелеком», «Релком», «Роспак» и ряд других организаций. В 1996 году появилась российская ассоциация RINET, призванная исполнять роль регионального отделения Internet Society [1].

На сегодняшний день количество пользователей Интернет в России составляет более 60 миллионов человек. Такие данные приводит в своем блоге мониторинговая компания Pingdom со ссылкой на Internet World Stats (рис. 1.1) [2].

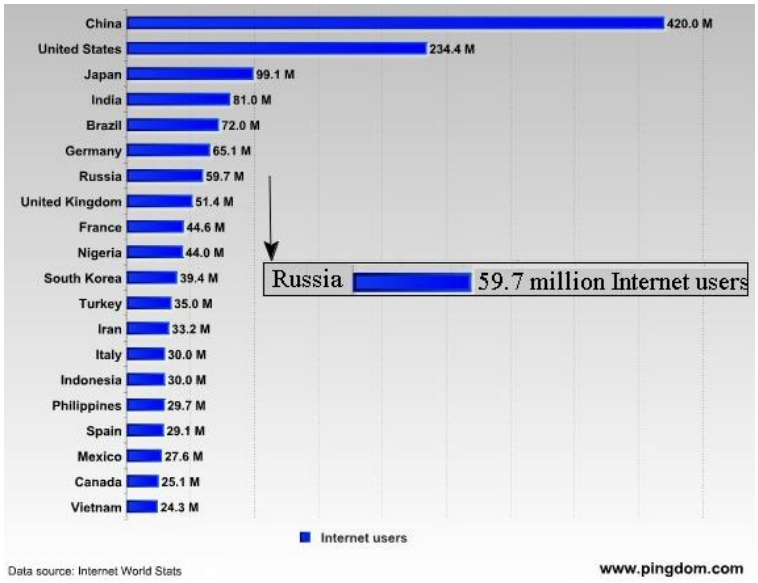

Рис.1.1. Количество пользователей сети Интернет в мире по странам

Общемировая аудитория Всемирной паутины составляет почти два миллиарда человек. При этом с 2000 года она увеличилась более чем в пять раз.

1.2. Обобщенная структура сети Интернет

В архитектуре Интернет отдельные сети соединяются друг с другом специальными устройствами – маршрутизаторами IP-пакетов (IP-шлюзами или IP-маршрутизаторами, или Router).

Шлюз подключается к двум или более сетям, каждая из которых воспринимает этот шлюз как хост-ЭВМ (узловая машина, компьютер, который подключен к сети в качестве узла). Поэтому шлюз имеет физический интерфейс и специальный IP-адрес в каждой из подключаемых сетей.

Передача пакетов требует от шлюза определение IP-адреса следующего шлюза или, на последнем участке, IP-адреса хост-машины, к которой направляется IP-пакет. Пример фрагмента сети Интернет приведен на рис.1.2.

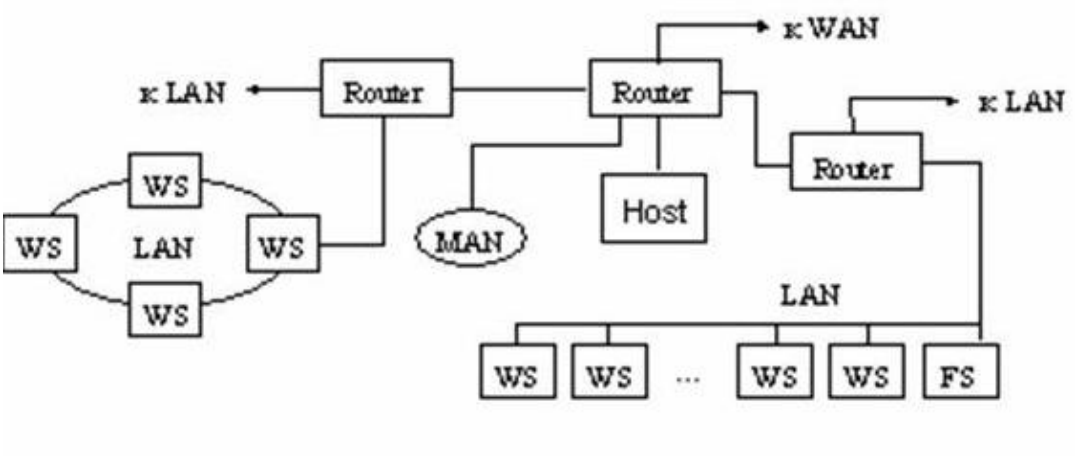

Рис. 1.2. Пример фрагмента сети Интернет

- WS (Work Station) – рабочая станция;
- LAN (Local Access Network) – локальная вычислительная сеть;
- WAN (Wide Area Network) – глобальная сеть;
- FS (File Server) – файл-сервер;
- MAN – региональная ИВС;
- Host – узловая машина (компьютер, который подключен к сети в качестве узла);
- Router – IP-маршрутизатор.

Функция шлюза, которая обычно называется маршрутизацией, основана на анализе специальных маршрутных таблиц (матриц маршрутов), которые находятся в специальной базе данных. База данных в каждом из

шлюзов должна постоянно обновляться, чтобы отражать текущую топологию сети Интернет.

Маршрут – это последовательность маршрутизаторов, через которые проходит пакет от отправителя до пункта назначения.

Данные передаются в пакетах. Пакеты имеют заголовок, который содержит служебную информацию. Данные верхних уровней вставляются в пакеты нижних уровней. На рис.1.3 показана передача сообщений в сети Интернет на основе механизма инкапсуляции (encapsulation) [3].

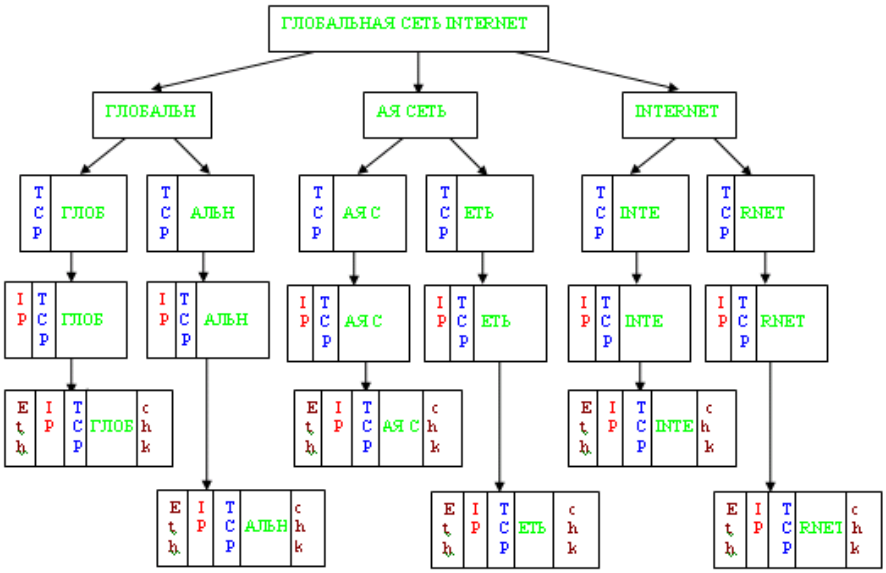

Рис. 1.3. Передача сообщений в сети Интернет на основе механизма инкапсуляции

В основе функционирования сети Интернет заложены протоколы TCP/IP.

TCP/IP – собирательное название для набора (стека) сетевых протоколов разных уровней, используемых в Интернет. Особенности TCP/IP:

- открытые стандарты протоколов, разрабатываемые независимо от программного и аппаратного обеспечения;
- независимость от физической среды передачи;
- система уникальной адресации;
- стандартизованные протоколы высокого уровня для распространенных пользовательских сервисов.

Стек протоколов TCP/IP делится на 4 уровня (рис.1.4):

- прикладной (объединяет сеансовый, представления данных и

прикладной уровни модели OSI);

- транспортный (совпадающий с моделью OSI);
- межсетевой (соответствующий сетевому уровню моделиOSI);
- уровень сетевого интерфейса (объединяет канальный и физический уровни модели OSI).

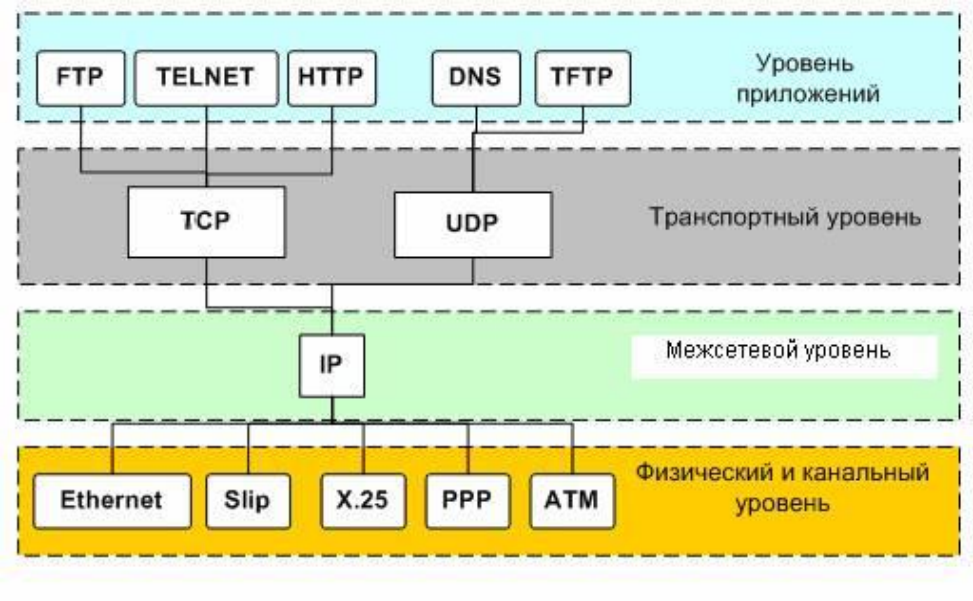

Рис. 1.4. Пример стека протоколов TCP/IP

Каким образом пакеты попадает с локального компьютера на удаленный сервер?

Все компьютеры объединены в локальную сеть, и имеют локальную IP-адресацию. Пакеты с такой адресацией «путешествовать» в глобальной сети не смогут, т.к. маршрутизаторы их не пропустят.

Поэтому существует шлюз, который преобразовывает пакеты с локальными IP-адресами, давая им свой внешний адрес. И дальше пакеты путешествуют с адресом шлюза (рис. 1.5).

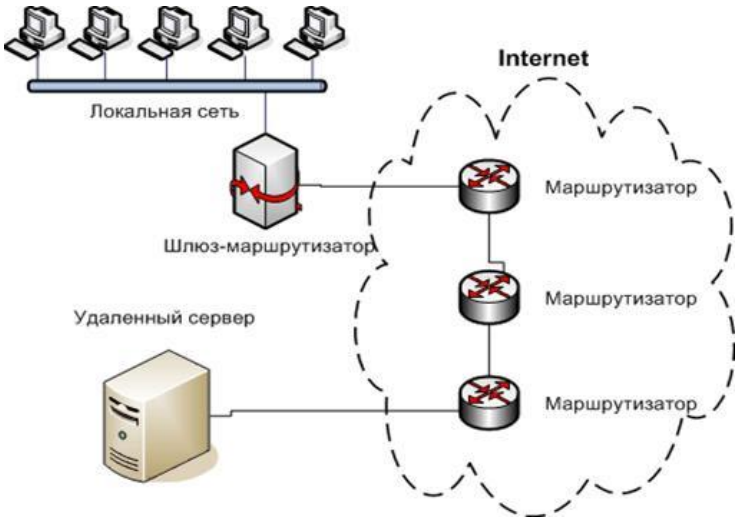

Рис. 1.5. Схема прохождения пакетов из локальной сети к серверу

Локальных сетей слишком много, поэтому реально объединяют автономные системы.

Автономная система (AS – autonomous system) – сеть, находящаяся под одним административным контролем, это может быть несколько компьютеров или большая сеть.

Схема объединения таких автономных систем в общую сеть показана на рис.1.6.

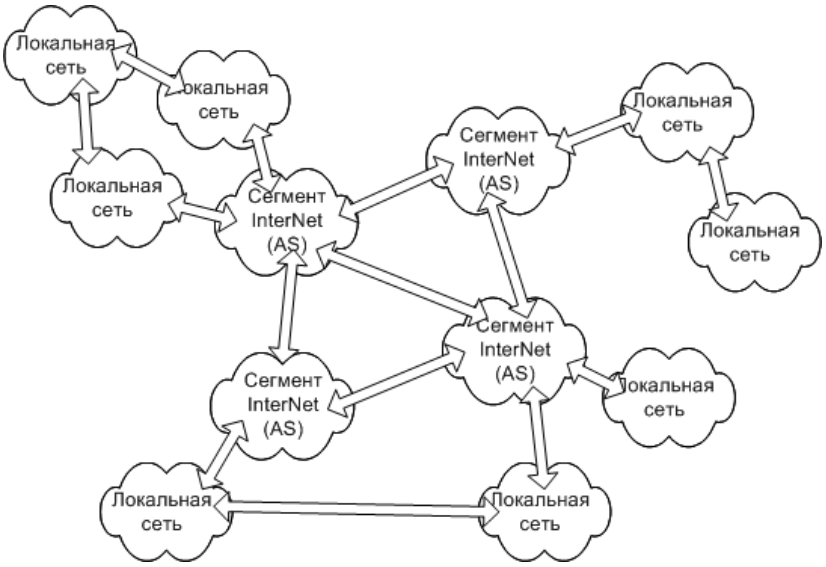

Рис. 1.6. Схема объединения отдельных сетей в общую составную сеть

За развитие Интернет и стандартизацию средств Интернет отвечают следующие организации Internet Society (ISOC) – профессиональное сообщество, которое занимается общими вопросами эволюции и роста Интернет как глобальной коммуникационной инфраструктуры.

Под управлением ISOC работает IAB (Internet Architecture Board) - организация, под ведомством которой находится технический контроль и координация работ в Интернет. IAB координирует направление исследований и новых разработок для стека TCP/IP и является конечной инстанцией при определении новых стандартов Интернет.

В IAB входят две основные группы:

- Internet Engineering Task Force (IETF). Это инженерная группа, которая занимается решением ближайших технических проблем Интернет. Именно IETF определяет спецификации, которые затем становятся стандартами Интернет;
- Internet Research Task Force (IRTF). Координирует долгосрочные исследовательские проекты по протоколам TCP/IP.

Все стандарты Интернет носят название RFC с соответствующим порядковым номером, но не все RFC являются стандартами Интернет - часто эти документы представляют собой комментарии к какому-либо стандарту или просто описания некоторой проблемы Интернет. RFC-документы можно найти по адресу http://www.rfc-editor.org/ или http://www.ietf.org/rfc.html.

1.3. Основные услуги сети Интернет

Для пользователя сеть Интернет предлагает различные средства коммуникаций и способы доступа к информации. Кроме услуг передачи данных сеть Интернет предоставляет широкий набор высокоуровневых информационных услуг. Эти услуги оказываются посредством многочисленных служб сети Интернет, таких как:

- Электронная почта (e-mail);
- Служба гипертекстовой информации World Wide Web;
- Служба передачи файлов (FTP-File Transfer Protocol);
- Служба организации чат-конференций (IRC – Internet Relay Chart);
- Служба телеконференций (Usenet);
- Служба имен доменов (DNS-Domain Name System);

- Служба удаленного управления компьютером (Telnet) и др.

Ниже будут рассмотрены подробнее некоторые из них.

Электронная почта

Электронная почта (от англ. «e-mail»), является одной из самых первых, широко распространенной и интенсивно используемой службой сети Интернет. С ее помощью любой пользователь, имеющий выход в Интернет, может пересылать или получать электронные послания. Работа электронной почты регламентируется набором таких почтовых протоколов, как: SMTP (Simple Mail Transfer Protocol- простой протокол передачи почты), POP (Post Office Protocol- протокол почтового отделения), IMAP (Internet Message Access Protocol- протокол доступа к сообщениям в сети Интернет). Программа, обеспечивающая передачу сообщений между почтовыми серверами, называется SMTP-сервером, а программа, принимающая сообщения от пользователей, - POP-сервером (или IMAP-сервером) [4]. Условная схема работы электронной почты показана на рис. 1.7.

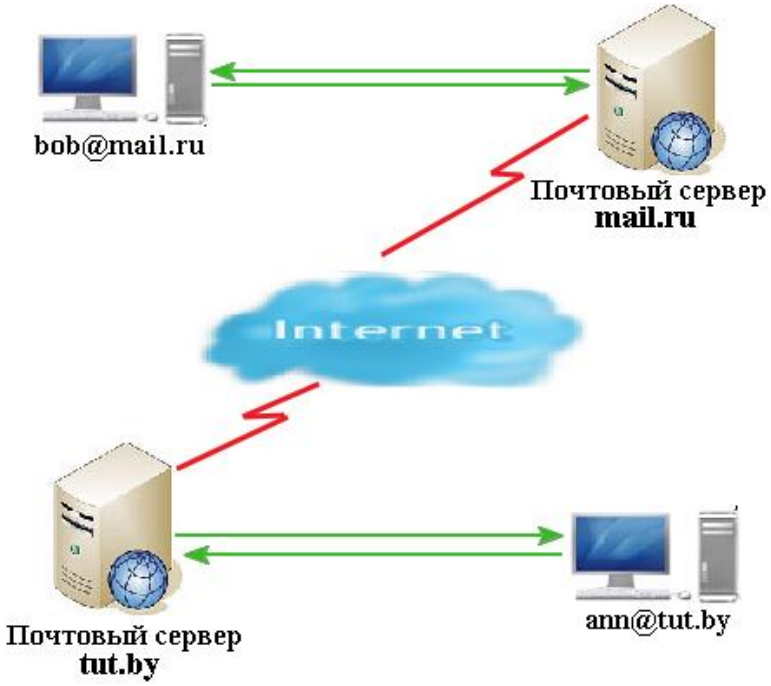

Рис. 1.7. Схема работы электронной почты

Для маршрутизации электронной почты в Интернет, как и для установления соответствия между доменными именами узлов сети и их адресами IP, используется система доменных имен DNS (Domain Name

System). Получив сообщение, предназначенное для отправки, почтовый сервер посылает запрос DNS с указанием имени почтового домена получателя. В ответ почтовый сервер получает список узлов, принимающих почту для данного домена. Список представляется в виде записей MX (Mail eXchange). Одному имени почтового домена могут соответствовать несколько записей MX с различными приоритетами. Приоритеты обозначаются целыми числами, с их помощью определяется, в каком порядке почтовому серверу следует обращаться к узлам, принимающим почту для данного домена. Меньшему числу соответствует больший приоритет.

На рис. 1.8 показан процесс доставки почтового сообщения, последовательность событий пронумерована.

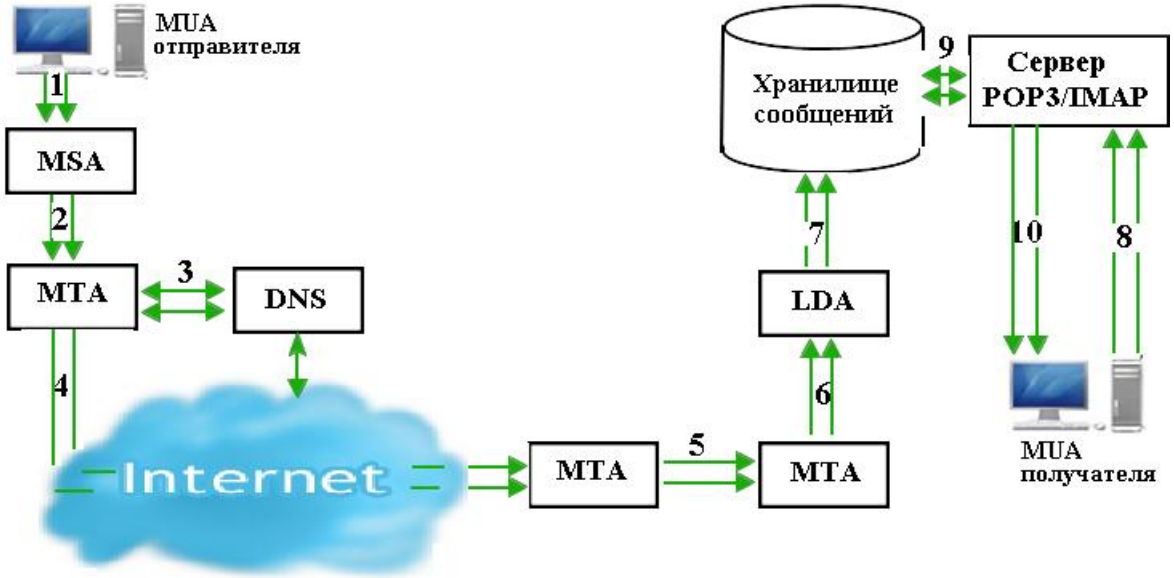

Рис. 1.8. Процесс доставки электронного сообщения от отправителя к получателю

- MUA (Mail User Agent) – пользовательский агент, или клиентская почтовая программа;
- MTA (Mail Transfer Agent) – транспортный агент, или почтовый сервер;
- LDA (Local Delivery Agent) – агент локальной доставки;
- MSA (Message Submission Agent) – агент подачи сообщения.

1. Сообщение, сформированное MUA отправителя, по протоколу SMTP посылается MSA. MSA проверяет, имеет ли данный MUA или пользователь право посылать почту из этой почтовой системы. В случае положительного результата, сообщение принимается для дальнейшей доставки.

2. MSA проверяет заголовок сообщения и, при необходимости, исправляет его. Готовое к отправке сообщение по протоколу SMTP отправляется на MTA исходящей почты.

3. MTA исходящей почты анализирует адрес получателя. Если сообщение предназначено для получателя домена, обслуживаемого данной почтовой системой, то оно доставляется получателю (см. пункты 6 – 10), в противном случае MTA запрашивает информацию о почтовом домене, указанном в адресе получателя, сервер DNS. Получив запрашиваемые данные, сервер DNS сообщает MTA, какие узлы принимают почту для данного домена, их адреса IP и приоритеты.

4. MTA отправителя пытается установить соединение по протоколу с принимающими почту узлами в соответствии с приоритетами, указанными в записях MX, полученных от сервера DNS. Если соединение ни с одним узлом не удается установить, сообщение помещается в очередь, и через некоторое время попытки установить соединение повторяются. Если соединение установлено, то принимающий MTA, удостоверившись, что сообщение предназначено для пользователя его домена, и что почтовый ящик с указанным адресом действительно существует, принимает сообщение.

5. В принимающей почтовой системе сообщение может пройти через несколько промежуточных MTA, выполняющих различные виды обработки входящей почты: проверку на вирусы, фильтрацию спама, перенаправление к нужному хранилищу сообщений и пр.

6. Последний MTA передает сообщение LDA для локальной доставки.

7. LDA помещает сообщение в почтовый ящик адресата.

8. Получатель обращается к серверу POP3 или IMAP, чтобы проверить поступившую почту.

9. Сервер забирает сообщение из почтового ящика.

10. Сервер шлет сообщение пользовательскому агенту получателя [3].

Таким образом сообщение доставляется от отправителя к получателю.

Основные проблемы, связанные с электронной почтой:

- перехват паролей учетных записей. Протокол SMTP, используемый для передачи электронной почты в Интернет не предоставляет средств аутентификации отправителя;
- перехват почтовых сообщений. Электронная почта может передаваться через Интернет в незашифрованном виде и может быть перехвачена и прочитана;
- спам. Спамом называется непрошеная массовая рассылка сообщений рекламного характера;
- рассылка фальсифицированных писем. Адрес отправителя письма может быть легко подделан. Подделка электронной почты может использоваться для атак типа "social engineering". Например, пользователь получает письмо якобы от системного администратора с просьбой сменить пароль на указанный в письме;
- передача исполняемого кода в почтовых сообщениях. Электронная почта позволяет передавать данные разных типов, в том числе программы, а также документы, содержащие макросы. Вместе с подделкой адреса отправителя это может использоваться для всевозможных атак. Например, пользователь получает письмо, в котором содержится поздравление с Новым Годом и «подарок» − программа, которую предлагается запустить. Запущенная программа рисует на экране, например, новогоднюю елку с мигающей гирляндой. Пользователь пересылает это поздравление своим друзьям и знакомым. Программа, рисующая елку, помимо этого инсталлирует программу удаленного управления, и сообщает о результате своему создателю;
- ошибки в программном обеспечении почтовых серверов. Серверы электронной почты печально известны множеством

ошибок, приводившим к взлому систем. Системному администратору следует внимательно следить за сообщениями о найденных ошибках в почтовых серверах и своевременно устанавливать исправленные версии;

- и другие.

WWW

Причиной популярности World Wide Web оказалась возможность интерактивного доступа к данным разных типов (гипертексту, графике, аудио, видео и т.д.). Для обращения к ресурсам Web пользователи сети Интернет применяют браузеры, которые представляют собой сложные, многофункциональные приложения, снабженные средствами отображения форматированного текста в документах HTML, а также машинами исполнения сценариев, написанного с помощью различных языков программирования.

Для воспроизведения различных форматов данных браузеры на стороне клиента вызывают внешние приложения (например, для просмотра файла формата *.doc, браузер вызовет Microsoft Word). Многие форматы данных могут включать исполняемый код, например, макросы в документах Microsoft Word и Microsoft Excel. Простой просмотр с виду безобидных материалов может привести к исполнению произвольного кода на машине пользователя от его имени.

Следует также принимать во внимание существование «активных компонент» (active content), таких как Java-апплеты, Javascript, ActiveX и т.п., которые также содержат код, выполняемый от имени пользователя.

Ниже приведены распространенные атаки на пользователей сети Интернет, опирающиеся на уязвимости браузеров Web:

- фальсификация Web-сайтов;
- запуск программ на локальном компьютере;
- открытие доступа к ресурсам файловой системы компьютеров;

- нарушение работы браузера путем переполнения буфера;
- раскрытие конфиденциальности Web-путешествий и др.

Простого решения проблем безопасности, связанных с активными компонентами и другим исполняемым кодом, загружаемым из WWW, не существует. Методы борьбы с проблемами включают в себя обучение пользователей и объяснение им проблем безопасности, связанных с загружаемым из сети исполняемым кодом, отключение в клиентском ПО возможности исполнения загружаемых активных компонент, своевременное обновление ПО клиента для исправления замеченных в нем ошибок и т.п.

Служба доставки файлов (FTP)

В Интернете существует множество серверов, которые предоставляют открытый доступ к файлам, хранящимся в отдельных архивах. Эти архивы содержат сжатые файлы различных ресурсов, часто объединенные по тематике. Посетители таких ресурсов могут загрузить на свой компьютер эти файлы, воспользовавшись программами, опирающимися на протокол FTP. Эти программы называются FTP-клиентами, а серверы, хранящие архивы, - FTP-серверами. Протокол регламентирует обмен информацией между сервером и клиентом FTP по сети TCP/IP. Для выполнения передачи файлов FTP-клиент открывает на FTP-сервере два TCP-соединения. Первое - реализует канал передачи команд, второе- канал передачи данных. Для канала передачи данных на стороне сервера порт может быть открыт двумя способами - в активном и пассивном режимах. Протокол FTP обеспечивает два режима работы службы доставки файлов - анонимный и пользовательский.

Наибольшую угрозу службе доставки файлов по протоколу FTP предоставляет передача паролей доступа к FTP-серверу в открытом виде, а также передача данных в открытом виде [4].

2. АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Понятие информационной безопасности

Термин «информационная безопасность» появился с развитием вычислительной техники и ЭВМ. Ниже приведены два определения информационной безопасности.

Информационная безопасность - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств [5].

Информационная безопасность - защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре [6].

Информационная безопасность непосредственно связана с понятием «защита информации».

Защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [7].

Понятие информационной безопасности базируется на трех основных положениях [8]:

- конфиденциальность информации (от англ. - *confidentiality*) — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
- целостность информации (от англ. - *integrity*) — избежание несанкционированной модификации информации;
- доступность информации (от англ. - *availability*) — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Информационная безопасность включает в себя безопасность используемого ПО, безопасность аппаратных и технических средств, безопасность каналов связи и многое другое.

Обеспечение информационной безопасности включает перечень мероприятий и образует систему обеспечения информационной безопасности. Субъекты информационных отношений заинтересованы в обеспечении своей информационной безопасности, а именно:

- своевременного доступа к необходимой информации и автоматизированным службам;
- достоверности информации;
- конфиденциальности информации и ее целостности;
- защиты от дезинформации (навязывания им ложной информации);
- защиты информации от незаконного тиражирования;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации и т.д.

Ущерб субъектам информационных отношений может быть нанесен не только со стороны локальных и глобальных сетей, но и через определенную информацию с носителей. Поэтому в качестве объектов, подлежащих защите в целях обеспечения безопасности информационных отношений должны рассматриваться информация, любые носители, средства хранения и процессы ее обработки (передачи).

В области защиты информации существует большой список руководящих документов. Ниже приведены некоторые из них.

ГОСТы в области защиты информации:

- ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.
- ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

- ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
- ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации.
- Руководящий документ Гостехкоммиссии "РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" (Гостехкомиссия России, 1997).
- ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

Федеральные Законы в области защиты информации:

- Федеральный закон РФ №63-ФЗ от 06 апреля 2011 г. «Об электронной подписи»
- Федеральный закон РФ № 8-ФЗ от 09 февраля 2009 г. «Об обеспечении доступа к информации, о деятельности государственных органов и органов местного самоуправления».
- Федеральный закон РФ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации».
- Федеральный закон РФ № 98-ФЗ от 29 июля 2004 г. «О коммерческой тайне».
- Федеральный закон РФ № 126-ФЗ от 07 июля 2003 г. «О связи».
- Федеральный закон РФ № 85-ФЗ от 04 июля 1996г. «Об участии в международном информационном обмене».

2.2. Угрозы информационной безопасности

Потенциально возможное событие, явление или процесс, которое воздействуя на информацию, ее носители или процессы обработки, которое может нанести прямой или косвенный ущерб информационной безопасности носит название угроза.

Попытка реализации угрозы безопасности информации называется атакой, а субъект, предпринимающий такую попытку, - злоумышленником.

Источниками угроз информации могут быть:

- сбои и отказы оборудования (технических средств);
- преднамеренные действия злоумышленников и нарушителей;
- ошибки проектирования и разработки компонентов ИС (аппаратных средств, технологии обработки информации, программ и т.д.);
- ошибки эксплуатации (пользователей, операторов и других субъектов);
- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.).

Зачастую угроза является следствием наличия уязвимых мест в защите информационных систем (ИС), однако некоторые из них нельзя считать следствием каких-то ошибок и просчетов; они существуют в силу самой природы современных ИС (например, угроза отключения электричества или выхода его параметров за допустимые границы).

Потенциальные угрозы можно разделить на два подкласса: объективные (естественные) и субъективные (искусственные) (рис.2.1).

Рис. 2.1. Классификация угроз информационной безопасности

Объективные - это угрозы, вызванные воздействиями на ИС и ее элементы объективных физических явлений и стихийных природных процессов.

Субъективные - это угрозы ИС, вызванные деятельностью человека. Исходя их мотива действий, этот подкласс можно разделить на два: преднамеренные и непреднамеренные.

Преднамеренные – это угрозы, связанные с идейными соображениями, из мести, с корыстными целями злоумышленников и т.д.

Непреднамеренные – это угрозы, вызванные ошибками в работе и действиях с информацией и ПО, проектировании ИС ее элементов и т.д.

Среди субъективных угроз особое место занимают нелегальное использование неучтенных программ, заражение компьютера вирусами, разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.). А также игнорирование организационных ограничений (установленных правил) при работе в системе, вход в систему в обход средств защиты, некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности и др.

По типу основного средства воздействия, используемого для реализации угрозы все возможные каналы проникновения в систему и утечки информации можно разделить на три группы (рис.2.2), где такими средствами реализации являются: субъект (человек), программа, аппаратура.

Рис. 2.2. Классификация каналов проникновения атак в ИС по типу основного воздействия

Также угрозы можно классифицировать по аспекту информационной безопасности (табл. 2.1):

Таблица 2.1

Угрозы конфиденциальности	Угрозы доступности	Угрозы целостности	Угрозы раскрытия параметров защищенной компьютерной системы
Хищение (копирование) информации, средств ее обработки, носителей; утрата (неумышленная потеря, утечка) информации, средств ее обработки и носителей; несанкционированное ознакомление, распространение.	Блокирование информации; уничтожение информации и средств ее обработки (носителей); блокирование канала передачи информации и средств обработки информации.	Модификация (искажение) информации; отрицание подлинности информации; навязывание ложной информации, обман; уничтожение информации.	Появление новых угроз; выявление уязвимостей; увеличение рисков; увеличение успешности атаки.

Классификация видов нарушений работоспособности ИС и несанкционированного доступа к информации по способам нанесения ущерба безопасности и объектам воздействия приведена в табл.2.2:

Таблица 2.2

Способы нанесения ущерба	Объекты воздействий			
	Оборудование	Программы	Данные	Субъект
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов.	Несанкционированное копирование перехват.	Хищение, копирование, перехват.	Передача сведений о защите, разглашение, халатность.
Потеря целостности информации.	Подключение, модификация, спецвложения, изменение режимов работы, несанкционированное использование ресурсов.	Внедрение "троянских коней" и "жучков".	Искажение, модификация.	Вербовка субъектов, "маскарад".
Нарушение работоспособности автоматизированной системы.	Изменение режимов функционирования, вывод из строя, хищение, разрушение.	Искажение, удаление, подмена.	Искажение, удаление, навязывание ложных данных.	Уход, физическое устранение.
Незаконное тиражирование информации.	Изготовление аналогов без лицензий.	Использование незаконных копий.	Публикация без ведома авторов.	

Сети TCP/IP при отсутствии системы защиты могут быть подвергнуты многочисленным атакам, выполняемых как изнутри локальной сети, так и извне, если локальная сеть имеет соединение с глобальной сетью. Некоторые атаки носят пассивный характер и сводятся к мониторингу информации, циркулирующей в сети, другие - активный, направленный на повреждение или нарушение целостности информации или самой сети. Наиболее распространенные типы вторжения на сети TCP/IP:

- атаки DoS (Denial of Service – отказ в обслуживании);
- искажение данных - сетевые черви;
- компьютерные вирусы;
- программы «троянские кони»;
- спам - агрессивная рекламная рассылка;
- фишинг и др.

В следующем разделе рассмотрены некоторые из основных угроз подробнее.

2.3. Типы проблем в обеспечении информационной безопасности

2.3.1. Вредоносные программы

Сегодня, пожалуй, не найти пользователя Интернет, который не сталкивался бы с вирусами, поступающими в его ОС из глобальной сети. При посещении ненадежных сайтов или скачивании какой-либо информации существует большая вероятность завести злополучного «червя» у себя в компьютере, что впоследствии приведет к непредсказуемому поведению аппаратных и технических средств ПК или локальной сети в целом.

Компьютерный вирус – это разновидность программы, которая может записывать (внедрять) свои копии в программы, расположенные в исполняемых файлах, системных областях дисков, драйверах, документах и т.д. Отличительной особенностью компьютерных вирусов является их способность к размножению. Также он может повреждать или полностью

уничтожать данные пользователя, от имени которого была запущена зараженная программа.

Принято разделять вирусы:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, сетевые черви);
- по поражаемым ОС и платформам (DOS, Microsoft Windows, Unix, GNU/Linux, Java и др.);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы);
- по языку, на котором написан вирус.

Процесс внедрения вирусом своей копии в программу (системную область диска и т.д.) называется заражением, а программа или иной объект, подвергнутый заражению вирусом (содержащий вирус) — зараженным.

Когда зараженная программа начинает свою работу, то вначале управление получает вирус, находящийся внутри нее. Вирус находит и «заражает» другие программы или иные объекты, а также может выполнить какие-либо непреднамеренные действия. Затем вирус передает управление той программе, в которой он находится, и она работает так же, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Однако при каждом запуске зараженной программы в ОС пользователя размножается все больше и больше вируссодержащих программ, что приводит к сбоям в работе компьютера.

Сетевые черви

Сетевыми червями принято называть вредоносные программы, основная цель которых состоит в наибольшем распространении на разнообразные сетевые устройства. Существует разновидность сетевых червей, которые носят название безфайловых или пакетных. Они распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и там активизируют свой код. Подобные сетевые черви пользуются уязвимостями в программном обеспечении ОС.

Опасные типы файлов:

asx, bas, bat, cmd, com, crt, exe, inf, ins, js, msc, msi, pif, reg, scf, scr, vbs.

Как работает сетевой червь.

1. Сетевой червь попадает на компьютер. Для этого он использует различные компьютерные и мобильные сети: электронную почту, IRC- и файлообменные (P2P, от peer-to-peer, — равный к равному, одноранговая, децентрализованная или пиринговая сеть) сети, LAN, сети обмена данными между мобильными устройствами и т.д. Большинство сетевых червей маскируются в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях и т.д.
2. Создается и запускается копия червя.
3. Копия червя стремится перейти в следующее устройство: компьютеры в Интернет, локальной сети и т.д.

Классические компьютерные вирусы

Классическими компьютерными вирусами называются программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

Они не используют сетевые сервисы для проникновения на другие компьютеры. Копия вируса попадает на удаленные компьютеры лишь в том случае, если зараженный объект оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съемный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с прикрепленным к нему зараженным вирусом файлом.

Троянские программы

Троянская программа – это вредоносная программа, используемая злоумышленником для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблагоприятных целях.

Троянская программа не способна распространяться саморазмножением, как вирусы, она запускается пользователем вручную или автоматически – программой или частью ОС, выполняемой на компьютере-жертве.

Для этого файл программы называют служебным именем, маскирующим его под любую другую программу, файл другого типа или просто дают привлекательное для запуска название, иконку и т.п. При запуске она загружает скрытые программы, команды и скрипты с согласия или без согласия и ведома пользователя. Троянская программа может в той или иной степени имитировать задачу или файл данных, под которые она маскируется. Троянская программа может быть модулем вируса, и получив возможность, самораспространять свои копии.

Целью троянской программы может быть закачивание и скачивание файлов; копирование ложных ссылок, ведущих на поддельные веб-сайты, чаты или другие сайты с регистрацией; создание помех работе пользователя; похищение данных, представляющих ценность или тайну; шифрование файлов при вирусной атаке; распространение других вредоносных программ, таких как вирусы.

2.3.2. Атаки и контратаки

Атаки на сеть приводят к отказу в обслуживании пользователям атакуемого сетевого ресурса. Сетевой ресурс может быть выведен из строя различными вредоносными программами или перегружен в том случае, когда злоумышленник посылает на атакуемый компьютер огромное количество запросов. Такая проблема носит название - атака типа «отказ в

обслуживании» или DoS-атака (Denial of Service). Принцип действия DoS-атак показан на рис. 2.3.

Контрдействия состоят в принятии превентивных мер. Например, система отказывает атакующему злоумышленнику в доступе к сервису посредством проверки адресов входящих пакетов данных и отбрасывания пакетов с подозрительными адресами.

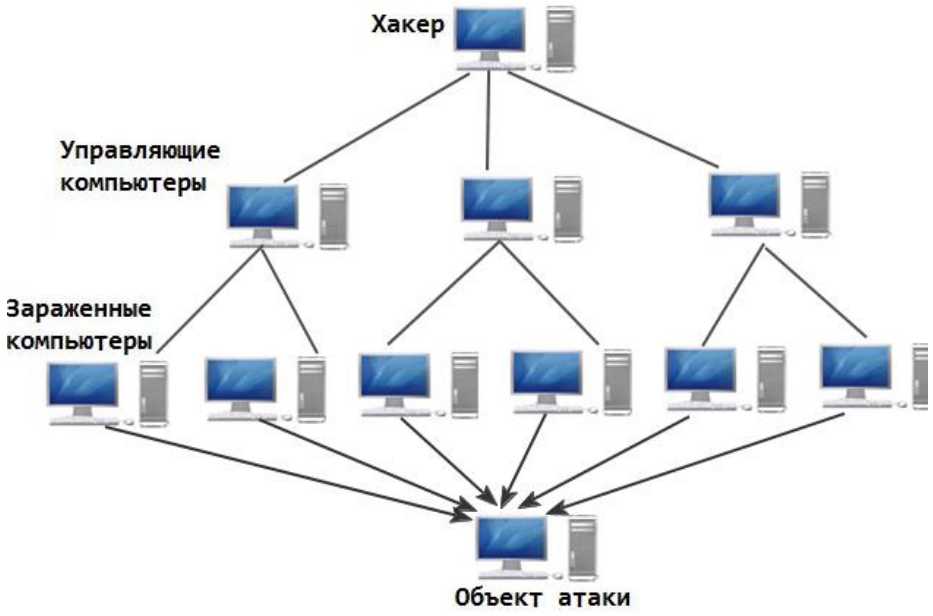

Рис. 2.3.Принцип действия DoS-атак

2.3.3. Спам и фишинг

Спамом (от англ. – «spam») называется массовая рассылка сообщений рекламного характера без согласия получателей. Термин спам появился в 1993 году. Спам в зависимости от целей и задач отправителя (спамера) может содержать коммерческую информацию или другую информацию.

Обычно спамеры используют следующую схему: устанавливается SMTP-соединение с хостом, на котором разрешена пересылка почты на любые хосты (open mail relay − открытый релей). На него посылается письмо с множеством адресатов и, как правило, с поддельным адресом отправителя. Хост, оказавшийся «жертвой», пересылает полученное сообщение всем адресатам. В результате, затраты на рассылку спама ложатся на получателей и хост, пересылающий почту. Интернет-провайдеры отрицательно относятся

к спаму, поскольку он создает весьма существенную нагрузку на их системы и неудобства их пользователям. Многие провайдеры отключают прием почты с открытых релеев, замеченных в передаче спама. Система электронной почты построена таким образом, что рассылка сразу на огромное количество адресов одного и того же сообщения стоит столько же, сколько и посылка одного-единственного письма. Получатель же оплачивает то время, которое он тратит на получение этого бесполезного письма. Подобные рассылки массового характера способны заметно загрузить почтовые серверы, из-за чего могут возникать задержки в получении важной корреспонденции.

Фишинг (от англ. phishing, от *fishing* — рыбная ловля, выуживание и password — пароль) — это вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные.

Атаки фишеров становятся все более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении. Часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить антифишинговые системы («если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»).

Для борьбы с такого рода атаками, прежде всего не стоит отвечать на письма сомнительного характера, использовать специальные программы-

фильтры, осуществляющие проверку почты на содержание спама и удаление таких писем прямо на почтовом сервере.

3. СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Существует три фундаментальных способа обеспечения информационной безопасности. Организация информационной безопасности может проводиться посредством применения организационных, аппаратных (технических) или программных способов защиты информации. Наибольшая эффективность будет получена в случае применения комплексной защиты вышеперечисленных способов. Вышеуказанные способы могут быть реализованы разнообразными средствами.

Для защиты периметра информационной системы путем применения организационных средств создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдения;
- системы контроля и управления доступом (СКУД) и др.

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладкой проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- построением экранированных помещений («капсул»);
- использованием экранированного оборудования;
- установкой активных систем зашумления;
- созданием контролируемых зон и др.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства.

К настоящему времени наибольшее распространение получили следующие аппаратные средства:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных;
- устройства для шифрования информации (криптографические методы) и др.

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 [9].

Вот некоторые из таких средств защиты информации:

- Средства защиты от НСД:
  - Системы обнаружения и предотвращения вторжений;
  - Системы предотвращения утечек конфиденциальной информации (DLP-системы).
- Анализаторы протоколов;
- Антивирусные программы;
- Межсетевые экраны (брандмауэры);
- Криптографические средства:
  - Шифрование;
  - Цифровая подпись.
- Системы резервного копирования и др.

Применение указанных способов и средств должны обеспечить пользователю уверенность в том, что:

- посторонние лица не получали доступ к его данным;
- данные отправлены именно тем, от чьего имени получены;
- принятые данные не были изменены по пути от отправителя к получателю;
- отсутствовал доступ к ресурсу без соответствующих полномочий (НСД) и др.

В дипломной работе акцент сделан на рассмотрение программных средств защиты информации, поскольку их функциональная роль в обеспечении информационной безопасности носит фундаментальный характер.

3.1. Антивирусные программы

Это программа для обнаружения компьютерных вирусов, нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или ОС вредоносным кодом.

Классификация антивирусов по принципу их действия:

- Сканеры. Принцип их работы заключается в поиске в файлах, памяти и загрузочных секторах уникального программного кода вируса - вирусных масок. Вирусные маски (описания) содержатся в антивирусной базе данных, и если сканер встречает программный код, совпадающий с одним из этих описаний, то он выдает сообщение об обнаружении соответствующего вируса.
- Ревизоры. Запоминают состояние компьютера, следят за изменениями файловой системы и извещают о важных или подозрительных изменениях пользователю.

- Мониторы. Являются разновидностью сканеров, которые постоянно находятся в памяти компьютера и осуществляют автоматическую проверку всех используемых файлов в масштабе реального времени. Современные мониторы осуществляют проверку в момент открытия и закрытия программы.
- Вакцины (иммунизаторы). Делятся на два вида: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

Классификация антивирусов по их функциональному назначению:

- Антишпион (antispyware). Антивирусная программа, предназначенная для обнаружения и удаления шпионского ПО (spyware) с компьютера пользователя.
- Онлайн-сканер. Антивирусное средство для обнаружения и удаления вирусов из файловой системы персонального компьютера, подключенного к сети Интернет. Их основным преимуществом является отсутствие необходимости инсталляции приложения. Недостатком является то, что сканер только обнаруживает вирусы, которые уже проникли в систему и не способен защитить компьютер от будущего заражения.
- Сетевой экран (firewall). Это программа, обеспечивающая безопасную работу компьютера в сети, которая позволяет блокировать нежелательный сетевой трафик, а также обеспечивает невидимость компьютера в сети, с целью предотвращения хакерских атак.
- Комплексная защита. Программные пакеты, предоставляющие в себе все перечисленные выше средства защиты компьютера плюс дополнительные функциональные компоненты. Могут содержать антивирус, сетевой экран, антишпион, защиту от фишинга, антиспам, средство резервного копирования данных.

Как антивирусная программа находит вирус в системе:

За каждым существующим вирусом закреплен уникальный для него кусок кода, так называемая сигнатура. Этот кусок кода хранится в базе

антивируса, и если такой кусок кода найден в файле, то такой файл определяется как соответствующий вирус. После нахождения подозрительного файла, в зависимости от настроек установленного на ПК антивируса, пользователь либо получает сообщение на право выбора «судьбы» данного файла, либо антивирусная программа сама решает это за него. Однако для того, чтобы в базе сигнатур антивирусной программы появился прописанный уникальный код вируса, этот вирус должен попасть на анализ вирусным аналитикам фирмы разработчика антивирусного обеспечения. Это довольно долгий путь, т.к. ежедневно появляются тысячи новых разновидностей вирусов, а программа-антивирус должна качественно защищать ПО. Для решения такой проблемы регулярно появляются обновления для антивирусов, а также определенные антивирусные программы наделены таким свойством как эвристический анализ.

Эвристический анализ работает по иному, нежели вышеизложенные базы сигнатур. Он анализирует содержимое файла и ищет в нем не сигнатуру, а последовательности операций, типичные для вирусов. Поэтому антивирусная программа имеет возможность обнаружения вирусов, которые еще не попали на исследование вирусным аналитикам. Чем более совершенный алгоритм эвристического анализа использует антивирус, тем он надежнее.

При выборе антивирусного ПО пользователи руководствуются интересующими их требованиями к нему.

Критерии оценки антивирусов:

- количество известных вирусов;
- скорость реакции на появление новых вирусов;
- степень задействования ресурсов компьютера;
- наличие эвристического анализа;
- корректное лечение вирусов;
- наличие антивирусного модуля, работающего в реальном времени.

В качестве примера ниже приведен обзор вирусной активности, полученный «Лабораторией Касперского» за март 2011 года [10].

В течение марта 2011 года на компьютерах пользователей продуктов «Лаборатории Касперского»:

- было отражено 241151171 сетевых атак;
- заблокировано 85853567 попыток заражения через веб;
- обнаружено и обезврежено 219843736 вредоносных программ (попытки локального заражения);
- отмечено 96702092 срабатываний эвристических вердиктов.

В сводной табл.3.1 приведены двадцать наиболее часто обнаруживаемых в сети Интернет вредоносных программ (по данным «Лаборатории Касперского»).

Таблица 3.1

Позиция	Изменение позиции	Вредоносная программа
1	4	AdWare.Win32.FunWeb.gq
2	New	Hoax.Win32.ArchSMS.pxm
3	3	AdWare.Win32.HotBar.dh
4	8	Trojan.HTML.Iframe.dl
5	New	Hoax.HTML.OdKlas.a
6	New	Trojan.JS.Popupper.aw
7	1	Exploit.JS.Pdfka.ddt
8	-8	Trojan.JS.Agent.btv
9	-9	Trojan-Downloader.JS.Agent.fun
10	-10	Trojan-Downloader.Java.OpenStream.bi
11	-7	Exploit.HTML.CVE-2010-1885.ad
12	New	Trojan.JS.Agent.uo
13	New	Trojan-Downloader.JS.Iframe.cdh
14	New	Packed.Win32.Katusha.o
15	New	Exploit.Java.CVE-2010-0840.d
16	1	Trojan.JS.Agent.bhr
17	New	Trojan-Clicker.JS.Agent.om
18	New	Trojan.JS.Fraud.bl
19	New	Exploit.Java.CVE-2010-0840.c
20	New	Trojan-Clicker.HTML.Iframe.aky

Быстродействие и ресурсоемкость антивируса для большинства пользователей являются одними из наиболее важных характеристик наряду с

качеством самой защиты. На эти характеристики обращают внимание в первую очередь при выборе и покупке антивируса. Никому не нужна мощная, но слишком ресурсоемкая антивирусная защита, при которой просто невозможно будет использовать компьютер для дела.

Результаты теста антивирусов на быстродействие (май 2011), поведенного информационно-аналитическим центром Anti-Malware

Цель теста - выбрать персональные антивирусные программы, которые оказывают наименьшее влияние на осуществление пользователем типовых операций на компьютере, меньше «тормозят» его работу и потребляют минимальное количество системных ресурсов.

В процессе тестирования были измерены и сравнены параметры, которые оказывают непосредственное влияние на восприятие пользователем скорости работы антивируса, а именно:

- Время загрузки операционной системы;
- Размер потребляемой антивирусом памяти и уровень загрузки процессора;
- Скорость копирования файлов (оценка быстродействия антивирусного монитора);
- Скорость сканирования (оценка быстродействия антивирусного сканера);
- Скорость запуска пяти распространенных офисных программ.

Полученные в ходе теста результаты дают ясное представление о быстродействии представленных на рынке антивирусных программ. Сопоставив эти данные, любой пользователь может сделать осознанный выбор в пользу того или иного антивирусного решения.

В тестировании участвовали следующие антивирусные программы (актуальных версий на момент начала тестирования - 05.03.2011**):**

1. Avast Internet Security 6.0.1000.0
2. AVG Internet Security 2011 10.0.0.1074

3. Avira Premium Security Suite 10.0.0.592
4. BitDefender Internet Security 2011 14.0,28,351
5. Comodo Internet Security 5.3.181415.1237
6. Dr.Web Security Space 6.00.1.01310
7. Emsisoft Anti-Malware 5.1.0.0
8. Eset Smart Security 4.2.67.10
9. F-Secure Internet Security 2011 1.30.4220.0
10. G DATA Internet Security 2011 (21.1.0.5)
11. Kaspersky Internet Security 2011 11.0.2.556
12. McAfee Internet Security 2011 4.5.147.0
13. Microsoft Security Essentials 2.0.657.0
14. Norton Internet Security 2011 18.1.0.37
15. Outpost Security Suite Pro 7.1 3415.520.1247.404
16. Panda Internet Security 2011 16.00.00
17. PC Tools Internet Security 2011 1.0.0.58
18. Trend Micro Titanium Internet Security 2011 3.0.0.1303
19. VBA32 Personal 3.12 3.12.14.1
20. ZoneAlarm Internet Security Suite 2010 9.3.37.0

Тест проводился на машине конфигурации Intel Core i5 650 3.2 ГГц / ASUS P7H55M / NVIDIA GeForse 210 / 4096 MB / WD CWD 10EARS 00Y5B1 и Hitachi HDP725040GLA360 под управлением ОС Microsoft Windows 7 x86 в период с 05 марта по 20 апреля 2011 года.

Для сохранения образов системы в состоянии до установки антивирусов и после установки каждого антивируса использовалась программа Acronis True Image, предоставленная Aflex Software, представителем компаний Acronis, Parallels и ASPLinux в России и СНГ.

Для исключения ошибок все измерения в данном тесте проводились последовательно пять раз, с возвратом в первоначальное состояние после каждого измерения. Полученные результаты усреднялись за вычетом граничных значений (максимального и минимального).

Влияние антивирусов на время загрузки операционной системы

Чем меньше влияет антивирус на загрузку ОС, тем лучше. Результаты измерения влияния антивирусной программы на время загрузки операционной системы показаны в табл. 3.2, а на рис.3.1 полученные данные сведены в график.

Таблица 3.2

Антивирус	Время загрузки, с	Задержка относительно эталона, с	Задержка относительно эталона, %
Без антивируса	30,94	-	-
Avira	33,08	2,14	6,92
Avast	34,03	3,09	9,99
Emsisoft	34,78	3,84	12,41
Trend Micro	35,30	4,36	14,09
Microsoft	35,82	4,88	15,77
ZoneAlarm	38,12	7,18	23,21
Outpost	38,19	7,25	23,43
AVG	38,64	7,70	24,89
VBA32	38,70	7,76	25,08
McAfee	39,67	8,73	28,22
G Data	39,71	8,77	28,35
Comodo	40,64	9,70	31,35
Eset	40,79	9,85	31,84
BitDefender	40,90	9,96	32,19
Kaspersky	40,99	10,05	32,48
Panda	41,51	10,57	34,16
Norton	43,21	12,27	39,66
Dr.Web	43,22	12,28	39,69
PC Tools	44,94	14,00	45,25
F-Secure	47,95	17,01	54,98

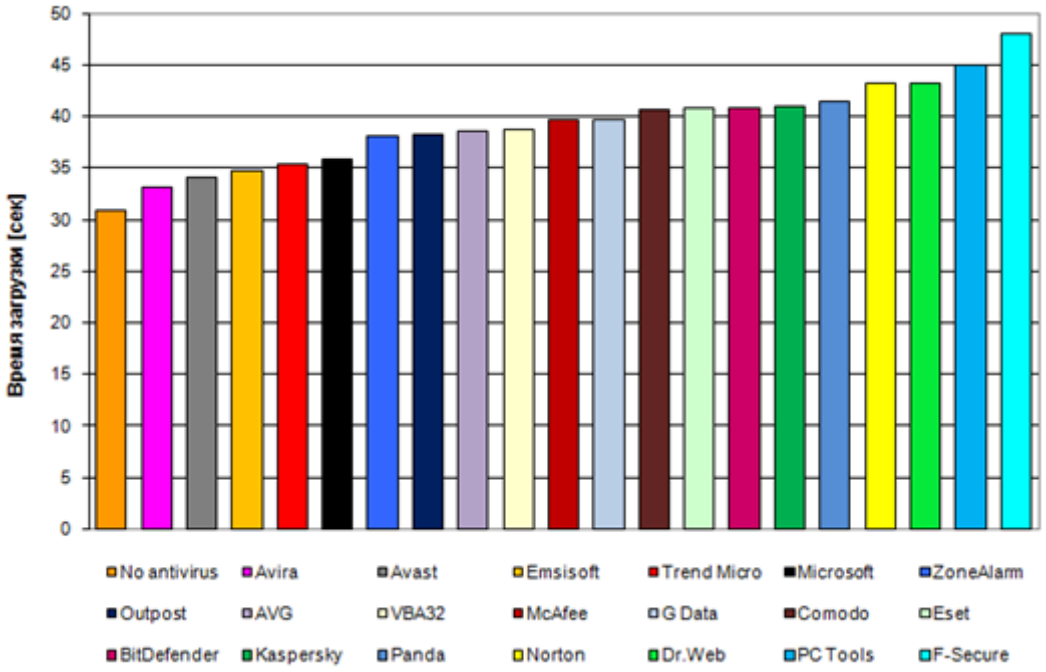

Рис. 3.1. Время загрузки операционной системы

Самые лучшие по этому показателю - антивирусы Avira, Avast, Emsisoft, Trend Micro и Microsoft. Они влияют на время загрузки операционной системы в пределах 20%. Худшие по этому показателю, антивирусы PC Tools и F-Secure, тормозят загрузку операционной системы на 45% и 55% соответственно.

Если же говорить об абсолютных значениях, то задержки в загрузке операционной системы в случае большинства антивирусов совсем небольшие – от 2 до 17 сек.

Сравнение ресурсоемкости антивирусов

Чем меньше оперативной памяти потребляет программное обеспечение и чем больше ее остается для других приложений, тем лучше. Использование антивирусами оперативной памяти в состоянии покоя может отличаться на десятки мегабайт.

Результаты измерений реально занимаемой антивирусами оперативной памяти в состоянии покоя представлены на рис. 3.2.

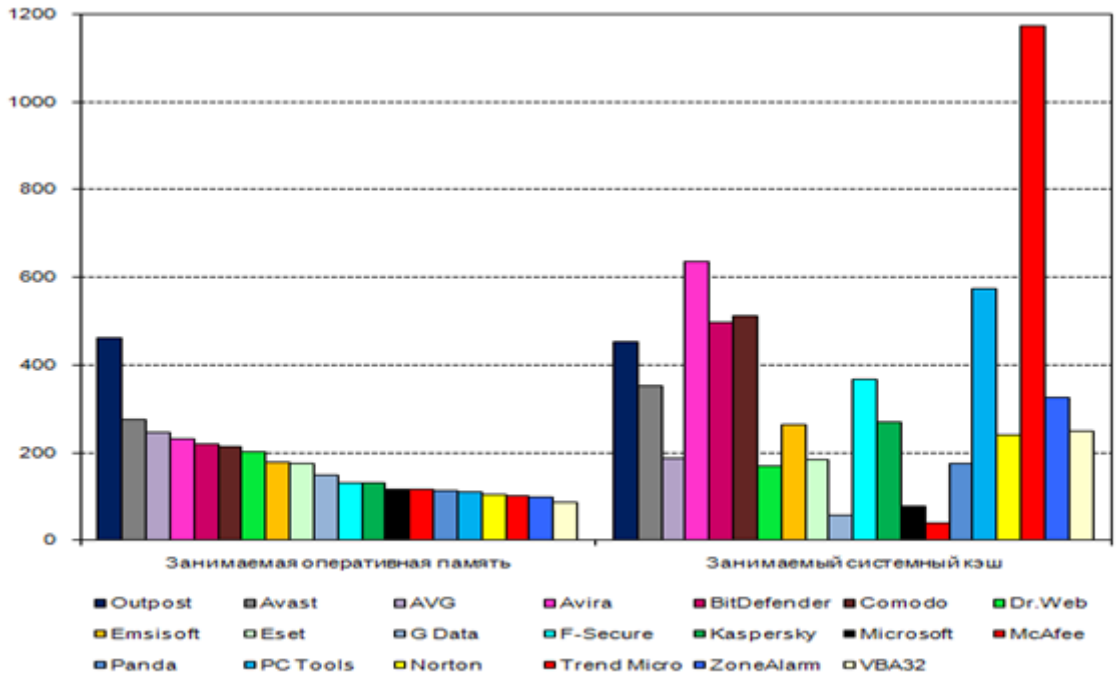

Рис. 3.2. Доступная оперативная память в состоянии покоя (Мб)

Как видно, минимальное количество оперативной памяти в состоянии покоя потребляют антивирусы VBA32, ZoneAlarm, Trend Micro, Norton, PC Tool, Panda, McAfee и Microsoft. В состоянии покоя им требуется от 87 до 120 Мб оперативной памяти. Самое большое количество оперативной памяти в состоянии покоя потребляют антивирусы Outpost, Avast, AVG, Avira, BitDefender, Comodo и Dr.Web – более 200 Мб.

Сравнение скорости работы антивирусов в режиме реального времени

Для оценки быстродействия антивируса наибольшую важность имеет скорость работы антивирусного монитора (сканера в режиме реального времени или on-access сканера). Известно, что при запуске, создании, копировании или изменении файлов на жестком диске, они подвергаются проверке антивирусным монитором. «Вмешательство» антивируса в файловые операции может заметно замедлять работу системы.

В табл. 3.3 и на рис. 3.3 представлено время копирования тестовой коллекции файлов на компьютере с различными антивирусами и задержки относительно системы без антивируса.

Таблица 3.3

Антивирус	Время копирования		
	Время [час:мин:сек]	Задержка [час:мин:сек]	Задержка [%]
Без антивируса	0:03:51	-	-
Avira	0:03:56	0:00:05	2,16
AVG	0:03:57	0:00:06	2,60
ZoneAlarm	0:04:03	0:00:12	5,19
Avast	0:04:13	0:00:22	9,52
Kaspersky	0:04:16	0:00:25	10,82
Eset	0:04:23	0:00:32	13,85
Trend Micro	0:04:27	0:00:36	15,58
Dr.Web	0:04:33	0:00:42	18,18
BitDefender	0:04:39	0:00:48	20,78
PC Tools	0:04:39	0:00:48	20,92
Outpost	0:04:41	0:00:50	21,65
F-Secure	0:05:04	0:01:13	31,60
Norton	0:05:17	0:01:26	37,09
Emsisoft	0:05:37	0:01:46	45,89
Comodo	0:06:54	0:03:03	79,22
G Data	0:08:28	0:04:37	119,91
Panda	0:12:07	0:08:16	214,72
Microsoft	0:14:03	0:10:12	264,94
McAfee	0:15:06	0:11:15	292,21
VBA32	0:25:54	0:22:03	572,73

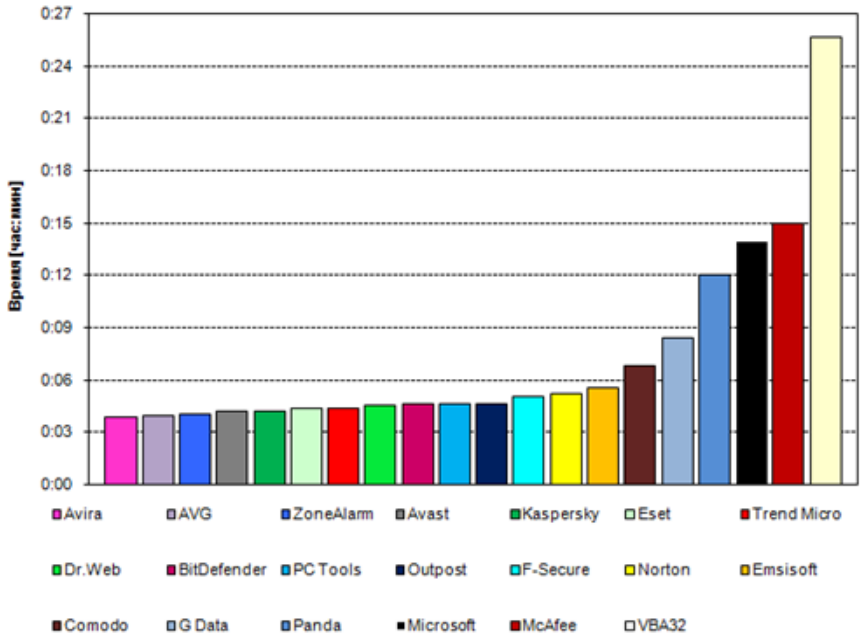

Рис. 3.3. Время копирования коллекции чистых файлов

Самым важным в выборе антивируса является уровень защиты компьютера от вирусов. Ниже приведены результаты теста на самозащиту антивирусов на платформе x64, который проведен компанией Anti-malware в январе 2011.

Изучались возможности самозащиты комплексных антивирусных продуктов класса Internet Security от возможных атак. Тест впервые проводился на операционной системе Windows 7 x64**.** Все проверки проводились с правами локального администратора на следующих уровнях:

1. Изменение разрешений на доступ к файлам и ключам реестра;
2. Модификация/удаление модулей;
3. Удаление антивирусных баз;
4. Модификация/удаление значимых ключей реестра;
5. Завершение процессов;
6. Модификация процессов/кода;
7. Выгрузка драйверов.

Дополнительно была проанализирована разница в самозащите антивирусов на операционной системе Windows 7 x86 и x64, используя для этого данные прошлого теста от сентября 2010 года.

В тестировании принимали участие двадцать наиболее популярных комплексных антивирусных продуктов класса Internet Security актуальных версий на момент начала тестирования (24 ноября 2010 года) и работающих на платформе Windows 7 x64. Среди них:

1. Avast Internet Security 5.0.477
2. AVG Internet Security 2011 (build 1170)
3. Avira AntiVir Premium Security Suite 10.0.0.565
4. BitDefender Internet Security 2011 (Build: 14.0.23.312)
5. Comodo Internet Security 5.0.32580.1142
6. Dr.Web Security Space 6.0 (12.0.0.58851)
7. Emsisoft Anti-Malware 5.0.0.0
8. Eset Smart Security 4.2.67.10
9. F-Secure Internet Security 2011 (1.30.4220.0)
10. G DATA Internet Security 2011 (21.1.0.5)
11. Kaspersky Internet Security 2011 (11.0.2.556)
12. McAfee Internet Security 2011
13. Microsoft Security Essentials 1.0.2498.0
14. Norton Internet Security 2011 (18.1.0.37)
15. Outpost Security Suite Pro 2010 (7.0)(3409.520.1244.401)
16. Panda Internet Security 2011(16.00.00)
17. PC Tools Internet Security 2011 (8.1.0.0.50)
18. Trend Micro Titanium Internet Security 2011 (3.0.0.1303)
19. VBA32 Personal 3.12.14.1
20. ZoneAlarm Security Suite 2010 (9.3.37.0)

Проверка самозащиты антивирусов

Тестирование самозащиты антивирусов проводилось по набору из 33 тестовых кейсов для каждой операционной системы отдельно.

1 балл (+) начислялся, если по одному из параметров (виду атаки) самозащита продукта сработала полностью успешно.

0.5 балла (или +/-) - если самозащита по данному параметру частично отсутствует, но основной функционал при этом сохранился (автоматически восстановился).

0 баллов - в случае полного отсутствия самозащиты и деактивации основного функционала.

Максимально возможное количество набранных баллов в тесте составило 33 балла [11].

В табл. 3.4 представлен расчет количества баллов для каждого антивирусного продукта по числу отраженных и пропущенных его самозащитой атак.

Таблица 3.4

Тестируемый продукт	Кол-во отраженных атак		Количество пропущенных атак, отсутствие самозащиты (0 баллов)	Всего баллов (максимум 33)
	Количество полностью отраженных атак (1 балл)	Количество частично отраженных атак (0.5 балла)		
Kaspersky	33	0	0	33
ZoneAlarm	32	0	1	32
Dr.Web	29	4	0	31
Comodo	30	1	2	30,5
Outpost	30	1	2	30,5
Norton	27	6	0	30
BitDefender	27	5	1	29,5
Trend Micro	27	3	3	28,5
Avast	23	9	1	27,5
AVG	20	11	2	25,5
G DATA	17	14	2	24
Avira	18	8	7	22
McAfee	12	19	2	21,5
Panda	14	15	4	21,5
F-Secure	10	22	1	21
Eset	10	19	4	19,5
PC Tools	12	15	6	19,5
Emsisoft	10	14	9	17
VBA32	11	8	14	15
Microsoft	10	0	23	10

На рис.3.4 можно наблюдать, как расположились позиции антивирусных программ в результате теста на самозащиту в процентном соотношении.

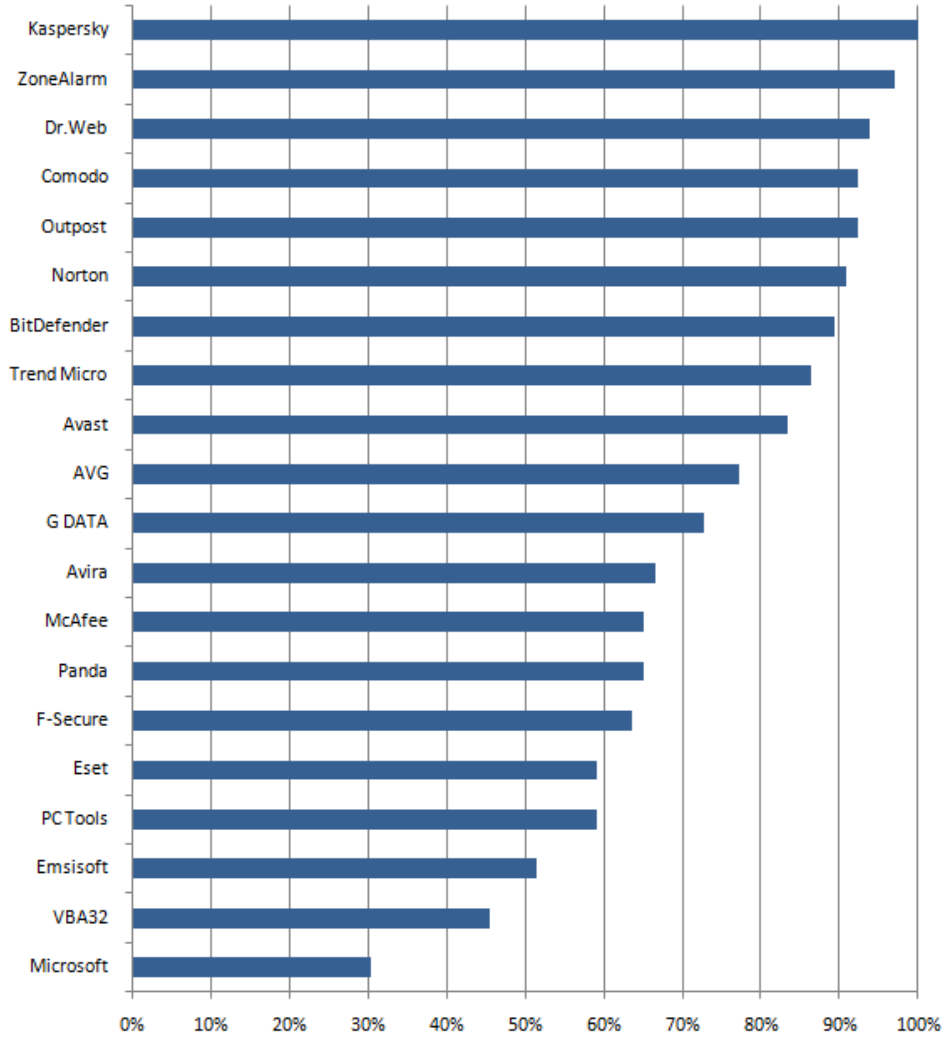

Рис. 3.4. Результаты теста самозащиты антивирусов на Windows 7 x64

Как видно, минимальный показатель в защите от разного рода вредоносных программ показал антивирус Microsoft, а лучший результат оказался у антивирусной программы Kaspersky.

3.2. Брандмауэры или межсетевые экраны

Межсетевые экраны (брандмауэры или файрволы — от нем. *brandmauer*, от англ. *firewall* — противопожарная стена).

Согласно определению Государственной технической комиссии при Президенте РФ «Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль информации, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы. Он обеспечивает защиту автоматизированной системы посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в автоматизированную систему или из нее».

Это важнейший компонент системы безопасности локальных сетей или отдельных компьютеров, подключенных к глобальной сети.

Брандмауэр необходимо использовать с целью повышения безопасности компьютера, путем ограничения информации, поступающей с других компьютеров, контролируя любые несанкционированные действия приложений и программ, пытающихся получить доступ к информационным ресурсам локального компьютера.

Для противостояния несанкционированному межсетевому доступу брандмауэр должен располагаться между защищаемой сетью и потенциально враждебной. Организационно экран входит в состав защищаемой сети. Брандмауэр не является симметричным. Для него отдельно задаются параметры, ограничивающие доступ из внутренний сети во внешнюю сеть и наоборот. Межсетевой экран должен учитывать протоколы информационного обмена, положенные в основу внутренней и внешней сетей. Если же такие протоколы различны, то брандмауэр должен поддерживать многопротокольный режим.

Брандмауэры управляют сетевым трафиком, проходящим внутри локальной сети, позволяют пропускать через сетевое соединение, только авторизованный трафик, контролируя тем самым сетевое взаимодействие между компьютерами глобальной и локальной сети. Брандмауэры позволяют маскировать IP-адреса хостов внутри локальной сети с помощью операции, называемой транзакцией сетевых адресов NAT (Network Address Translation). Маскирование IP-адреса становятся невидимыми для внешних пользователей, которые, например, для отправки почтовых сообщений внутреннему пользователю направляют его на почтовый шлюз, который переправляет его адресату.

Брандмауэры позволяют управлять доступом сетевых пользователей к различным сетевым службам. Эта задача решается конфигурированием брандмауэра, при котором можно разрешать или блокировать доступ к отдельной службе локальной сети с помощью списков контроля доступа ACL (Access Control List). Списки ACL предоставляют гибкие возможности управления доступом. С их помощью можно разрешать доступ к отдельным службам и запрещать доступ ко всем остальным службам или, наоборот, блокировать доступ к отдельным службам и разрешать доступ ко всем остальным службам. Хорошо настроенные брандмауэры не просто блокируют неавторизованные запросы со стороны внешних компьютеров, но и пытаются идентифицировать авторов запроса вместе с немедленным уведомлением пользователя-администратора системы о попытках таких запросов. Структура межсетевого экрана представлена на рис. 3.5.

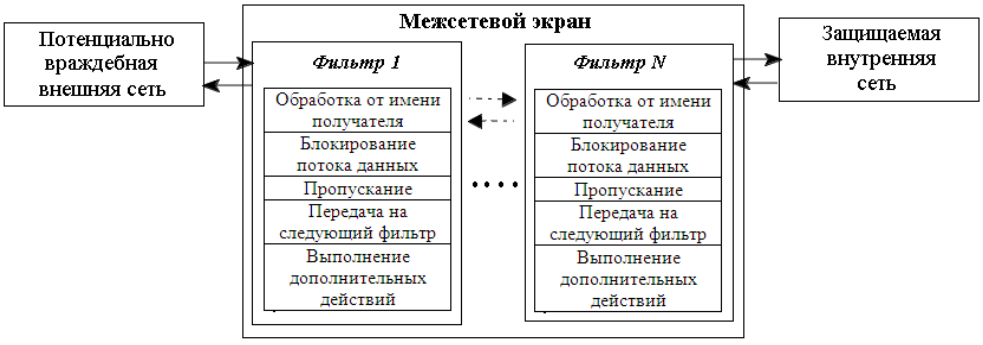

Рис. 3.5. Структура межсетевого экрана

Компоненты брандмауэра

Брандмауэры состоят из набора программных и аппаратных компонентов, в число которых входят следующие.

1. Бастионный хост. Представляет собой компьютер с защищенной версией ОС, подсоединенный к локальной и глобальной сети. На бастионном компьютере устанавливаются все прочие компоненты брандмауэра и необходимые службы, например Telnet, DNS, FTP, SNMP, а также средства пользовательской аутентификации.

2. Маршрутизатор с фильтрацией пакетов. Обычный маршрутизатор просто пересылает поступающие IP-пакеты по указанному адресу. Маршрутизатор с фильтрацией пакетов выполняет дополнительную функцию проверки поступающих IP-пакетов. Маршрутизаторы с фильтрацией пакетов иногда называют защищенными маршрутизаторами. Защищенные маршрутизаторы не проверяют содержимое пакетов, а имеют дело лишь с заголовочной информацией пакетов, контролируя IP-адреса источника и получателя, используемые протоколы, службы, порты и другую информацию, указанную в списке ACL.

3. Шлюзы приложений (прикладные шлюзы). Используются на бастионном хосте и ограничивают подсоединения к отдельным приложениям. Для этой цели используются службы-посредники, которые устанавливаются на шлюзе отдельно для каждого приложения, которому разрешено сетевое взаимодействие через брандмауэр. Только те сетевые службы, для которых установлены службы-посредники, могут получать и отправлять сетевой трафик через шлюзы приложений, причем службы-посредники можно настроить на разрешение доступа лишь к определенному, ограниченному набору средств приложения. Т.о., шлюзы приложений значительно усиливают возможности создания такой политики безопасности, которая обеспечит аутентификацию сетевых пользователей и ведение журнала регистрации. Примером шлюза прикладного уровня является

прокси-сервер, управляющий сетевым трафиком и выполняющий аутентификацию пользователей.

4. Канальные шлюзы. Связывают сетевой компьютер с портами TCP/IP бастионного хоста. Они не выполняют никакой проверки сетевого трафика и используются для передачи исходящих сообщений от доверенных внутренних пользователей. Позволяют защитить сеть от вторжений и в то же время ускорить работу системы.

Правила фильтрации пакетов брандмауэром

Брандмауэры выполняют фильтрацию пакетов путем проверки заголовков входящих пакетов на предмет их удовлетворения определенным критериям, устанавливаемым с помощью правил фильтрации пакетов. Фильтрации подвергаются пакеты, поступающие как изнутри, так и извне локальной сети, причем фильтр работает ассиметрично, различным образом обрабатывая входящие и исходящие пакеты. Т.о. для фильтрации входящих и исходящих пакетов следует использовать различные правила фильтрации.

При поступлении пакета в брандмауэр входящий в его состав маршрутизатор с фильтрацией пакетов извлекает из пакета заголовки и выполняет синтаксический анализ и проверку заголовков. При этом проверяются лишь заголовки, относящиеся к протоколам TCP, IP, UDP. Далее к пакету последовательно применяются правила фильтрации пакетов, причем в том порядке, в котором они сохранены в списке ACL брандмауэра. Применение правил выполняется с учетом следующих принципов:

- если при просмотре списка ACL будет найдено правило, разрешающее прохождение пакета, он немедленно направляется по назначению;
- если будет найдено правило, запрещающее прохождение пакета, он немедленно отбрасывается;
- если при просмотре ACL окажется, что для пакета отсутствуют правила, разрешающие его прохождение, пакет автоматически отбрасывается.

Чтобы создать правило фильтрации пакетов, следует указать: действие, выполняемое при совпадении критериев правила с параметрами пакета, протокол обработки пакета и номер порта для приема пакета. Некорректный порядок записи правил может привести к полному блокированию межсетевого соединения или к отбрасыванию корректных пакетов и разрешению некорректных.

Недостатки маршрутизаторов с фильтрацией пакетов

Фильтрация пакетов служит эффективным средством защиты различных служб от сетевых атак, но методы фильтрации пакетов неэффективны против атак, не зависящих от сетевых служб. Например, от атак с подменой IP-адреса пакета, которые могут быть применены к любой сетевой службе. Такой вид атак носит название IP-спуфинг. Для исполнения такого рода атаки, хакер в отсылаемом с внешнего хоста пакете заменяет исходный реальный IP-адрес на фальшивый, для которого разрешено прохождение пакетов. Этим фальшивым IP-адресом может быть IP-адрес внутреннего хоста сети. Если брандмауэр не настроен должным образом, пакет с фальсифицированным IP-адресом может быть пропущен в сеть.

Еще одним примером сетевой атаки, против которой бессильна фильтрация пакетов, является обход системы защиты сети указанием в переданном пакете маршрутной информации. Если брандмауэр не настроен на отбрасывание пакетов, содержащих маршрутную информацию, такая атака может завершиться успехом.

Брандмауэры с фильтрацией пакетов могут пропустить атаку, реализуемую фрагментацией пакетов, при которой хакер делит пересылаемые пакеты на маленькие части и посылает их на маршрутизатор с фильтрацией пакетов. Во фрагментированном пакете номер порта целевого хоста должен содержать только самый первый фрагмент, а остальные фрагменты содержат лишь само сообщение, поэтому, пропустив первый пакет, брандмауэр пропустит и остальные.

Другой недостаток маршрутизаторов с фильтрацией пакетов состоит в отсутствии проверки содержимого пакетов, что делает их непригодными для защиты от атак, управляемых данными. Они основаны на том, что проверка только заголовков пакетов не позволяет выявить, насколько безопасна информация, содержащаяся в пакете. Такая информация может включать в себя различные команды, параметры настройки и другую информацию, передача которых определенной службе сетевого хоста способна заставить службу выполнить действия, причиняющие вред компьютерной системе. Для отражения таких атак более эффективны другие методы, обеспечиваемые шлюзами приложений.

Шлюзы приложений

Шлюзы приложений позволяют создавать более жесткие правила политики безопасности, в отличие от маршрутизаторов с фильтрацией пакетов.

Для управления трафиком между хостами глобальной и локальной сети в шлюзах приложений используются специальные программы, называемые службами-посредниками. Для защиты каждого защищаемого шлюзом приложения требуется установить отдельную службу, без которой приложение не сможет предоставлять свои услуги сетевым пользователям. При использовании шлюзов приложений авторизованные пользователи имеют доступ к службам-посредникам для получения нужной им услуги, но им не разрешен доступ к шлюзу приложения, т.к. это несет угрозу безопасности брандмауэра.

В отличие от шлюзов с фильтрацией пакетов шлюзы приложений запрещают прямой обмен пакетами между внутренними и внешними хостами. Для решения вопроса о предоставлении доступа к службе-посреднику бастионный хост может выполнить дополнительную аутентификацию подсоединяющегося пользователя. Для этого может быть использована технология одноразовых паролей, генерируемых криптографическим устройством. Для усиления защиты такие средства

аутентификации могут быть реализованы отдельно для каждой из служб-посредников.

Основное преимущество шлюзов приложений в том, что они позволяют жестко ограничить доступ ко всем приложениям и службам, используемым в локальной сети, со стороны как внешних, так и внутренних хостов.

Недостаток заключается в ограничении свободы действий пользователей, а также в необходимости инсталляции на каждом хосте, запрашивающем службу-посредника, дополнительных программных средств.

Шлюзы с сохранением состояния и канальные шлюзы

Для определения указанных недостатков шлюзов приложений служат технологии создания канальных шлюзов с сохранением состояния. Канальные шлюзы напрямую соединяют TCP/IP-порты бастионного хоста с сетевым хостом и не проверяют проходящий сетевой трафик, что позволяет увеличить быстродействие брандмауэра.

Шлюзы с сохранением состояния позволяют достичь большего уровня безопасности путем сохранения информации обо всех подсоединениях. При решении вопроса, разрешить ли подсоединение поступившему запросу или нет, брандмауэр с сохранением состояния анализирует информацию, сохраненную при предыдущих запросах. Эти шлюзы не ограничиваются анализом заголовков пакетов, а могут выполнять более сложные логические и математические проверки содержимого пакетов. Тем самым они сочетают возможности шлюзов приложений и маршрутизаторов с фильтрацией пакетов, обеспечивая более высокий уровень безопасности компьютерной системы [4].

3.2.1. Способы развертывания межсетевых экранов в локальных сетях

При подключении локальной сетей к глобальной сети администратор сетевой безопасности должен учитывать следующие требования:

- защита локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;

- скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
- разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную.

Необходимость работы с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети. С помощью брандмауэра можно разделить локальную сеть на домены безопасности - группы компьютеров с одним уровнем защищенности. В зависимости от уровня безопасности на компьютерах разных доменов хранится информация разного уровня защищенности:

- свободно доступные сегменты информации;
- сегменты с ограниченным доступом;
- закрытые сегменты.

Существует большое количество схем подключения брандмауэров в сети.

При этом все схемы подразделяются на:

- стандартные схемы защиты отдельной локальной сети;
- схемы включения в составе средств коллективной защиты.

Стандартные схемы защиты отдельной локальной сети

Наиболее простым является решение, при котором брандмауэр просто экранирует локальную сеть от глобальной. При этом WWW-сервер, FTP-сервер, почтовый сервер и другие сервера оказываются также защищены межсетевым экраном. Однако требуется уделить много внимания на предотвращение проникновения на защищаемые станции локальной сети при помощи средств легкодоступных WWW-серверов.

Простое включение межсетевого экрана в сети показано на рис. 3.6.

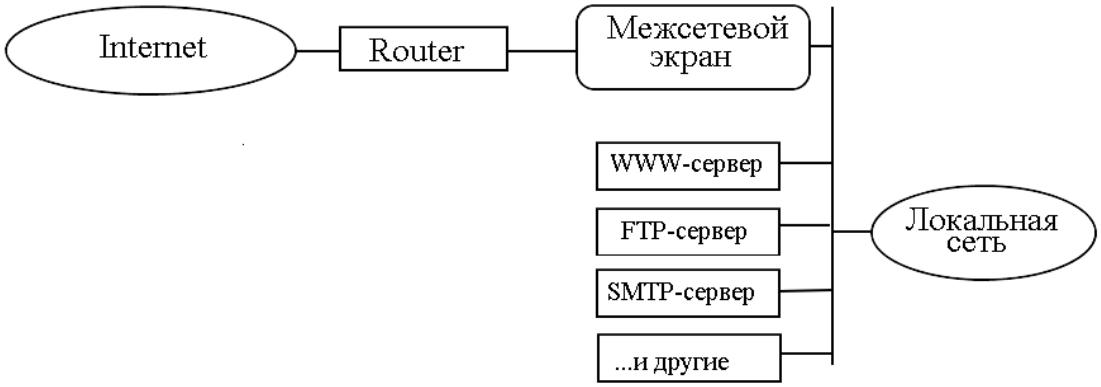

Рис. 3.6. Простое включение межсетевого экрана

Для предотвращения доступа в локальную сеть, используя ресурсы WWW-сервера, рекомендуется общедоступные серверы подключать перед межсетевым экраном. Данный способ обладает более высокой защищенностью локальной сети, но низким уровнем защищенности WWW- и FTP-серверов. Такой способ подключения межсетевого экрана показан на рис. 3.7.

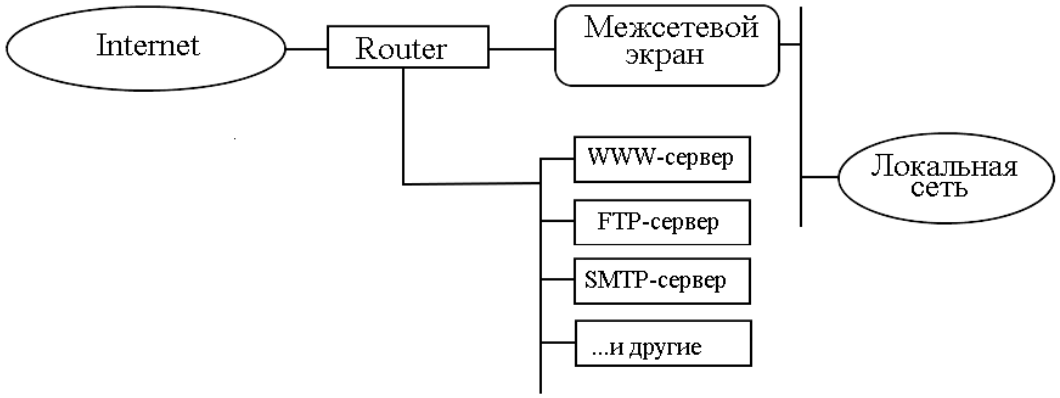

Рис. 3.7. Подключение межсетевого экрана с вынесением общедоступных серверов

Применение межсетевых экранов в составе средств коллективной защиты

Некоторые межсетевые экраны позволяют организовывать виртуальные корпоративные сети VPN (Virtual Private Network). При этом несколько локальных сетей, подключенных к глобальной сети, объединяются в одну виртуальную корпоративную сеть. Передача данных между этими локальными сетями производится прозрачно для пользователей локальных сетей. При этом обеспечивается конфиденциальность и целостность

передаваемой информации при помощи различных средств: шифрования, использования цифровых подписей и т.п. При передаче может шифроваться не только содержимое пакета, но и его заголовок, включая все, входящие в него поля. Возможная схема использования межсетевых экранов в составе виртуальных корпоративных сетей приведена на рис. 3.8.

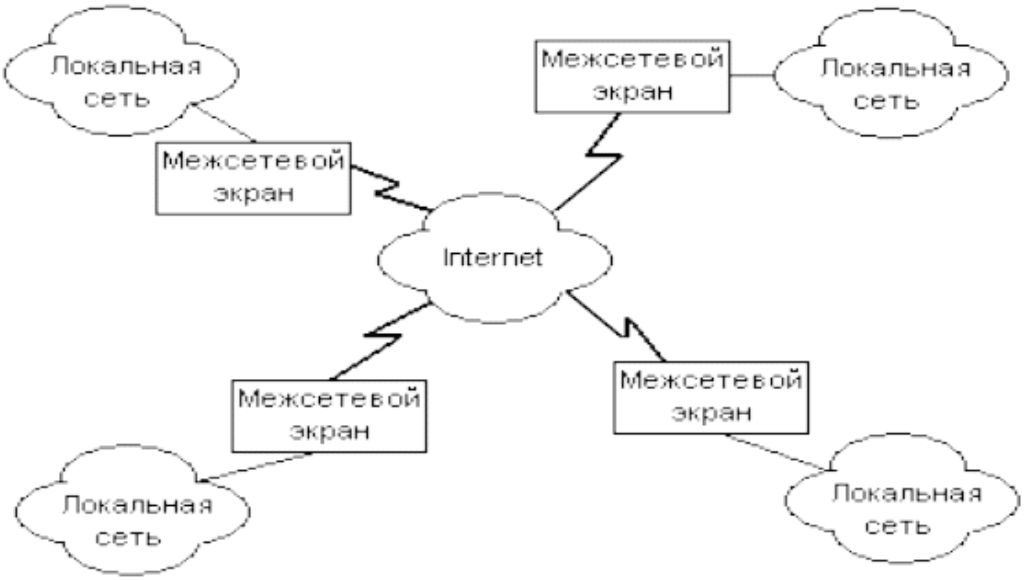

Рис. 3.8. Схема использования межсетевых экранов в составе виртуальных корпоративных сетей

3.2.2. Недостатки межсетевых экранов

Межсетевые экраны обеспечивают защиту только по периметру компьютерной системы. Они бесполезны против атак, выполняемых изнутри сети, в частности против атак, управляемых данными, при которых в локальную сеть передаются внешне безопасные данные, которые далее используются для атаки на сеть изнутри.

Некоторые межсетевые экраны снабжены средствами проверки поступающей электронной почты на наличие вирусов, но, как правило, они не в состоянии надежно защитить систему от проникновения вирусов.

Если на компьютере установлено несколько межсетевых экранов, не следует включать их одновременно, в результате одновременного их включения некоторые программы перестанут работать правильно.

Вывод: Межсетевые экраны не отменяют другие средства защиты - меры парольной защиты, антивирусную защиту, шифрование и организационные меры обеспечения безопасности.

Установка межсетевого экрана обеспечивает эффективную защиту только путем его точной настройки, выполняемой в течение длительного времени эксплуатации системы.

Для того чтобы межсетевой экран выполнял те функции, которые на него возлагаются для комплексной сетевой защиты, необходимо, чтобы все пакеты, приходящие по сети и уходящие в сеть, проходили через него. Если же это правило не соблюдается, или соблюдается частично, то все действия, направленные на создание безопасного сервера с использованием межсетевого экрана, будут бесполезны. Если существует хоть малейшая вероятность, что межсетевой экран можно обойти, эта возможность обязательно рано или поздно будет использована взломщиками.

Традиционные межсетевые экраны являются по существу средствами, только блокирующими атаки. В большинстве случаев они защищают от атак, которые уже находятся в процессе осуществления. Более эффективным было бы не только блокирование, но и упреждение атак, т.е. устранение предпосылок реализации вторжений.

Для организации упреждения атак необходимо использовать средства обнаружения атак и поиска уязвимостей, которые будут своевременно обнаруживать и рекомендовать меры по устранению «слабых мест» в системе защиты. Для защиты информационных ресурсов распределенных корпоративных систем необходимо применение комплексной системы информационной безопасности, которая позволит эффективно использовать достоинства межсетевых экранов и компенсировать их недостатки с помощью других средств безопасности.

3.3. Протоколы для защищенного обмена данными через Интернет

3.3.1. Протокол IPSec

Протокол IPSec (Internet Protocol Security) нацелен на защиту пакетов, передаваемых по сетям TCP/IP. Представляет собой набор открытых стандартов защиты соединений по IP-сетям средствами криптографии. Организует аутентификацию, обеспечение сохранности данных, шифрование и автоматическое снабжение конечных точек канала секретными ключами. Определен для IPv4 и IPv6.

При использовании протокола IPSec компьютер шифрует все отправленные данные, а получатель – дешифрует. Поэтому при условии построения многоуровневой системы защиты, включающей ограничение физического доступа к компьютерам, защиту периметра и корректную настройку пользовательского доступа, протокол IPSec обеспечит всестороннюю защиту сетевых данных.

Протокол IPSec защищает не сам канал передачи информации, а передаваемые по нему пакеты. Тем самым IPSec решает следующие задачи:

- Неотрицаемость сообщений. Данный протокол поддерживает создание цифровой подписи передаваемого сообщения закрытым ключом отправителя, что обеспечивает невозможность отрицания авторства сообщения;
- Аутентификация источника сообщения. Обеспечивается поддержкой инфраструктуры открытого ключа (PKI – Public Key Infrastructure), аутентифицирующей компьютер-отправитель на основе сертификата;
- Конфиденциальность передаваемых данных. Обеспечивается шифрованием информации криптостойкими алгоритмами DES (Data Encryption Standard — симметричный алгоритм шифрования) и 3DES;
- Защита целостности данных. Осуществляется путем подписания передаваемых пакетов хеш-кодами аутентификации сообщения HMAC (Hash Message Authentication Codes). Коды HMAC вначале подсчитываются компьютером-отправителем сообщения, использующим специальный

алгоритм и общий секретный ключ. Затем компьютер-получатель повторно подсчитывает код HMAC и сравнивает результат с полученным значением.

В IPSec используются два механизма защиты – защита заголовка IP-пакета и шифрование содержимого IP-пакета. В первом случае к заголовку пакета добавляется заголовок аутентификации (AH – Authentication Header), позволяющий проверить целостность и подлинность данных, а также обеспечить защиту от повторений. Во втором случае данные шифруются, обеспечивая их конфиденциальность, а с помощью дополнительного заголовка – защищаются от подмены и повторения.

На рис. 3.9 проиллюстрировано положение заголовка аутентификации AH в IP-пакете в транспортном и туннельном режимах.

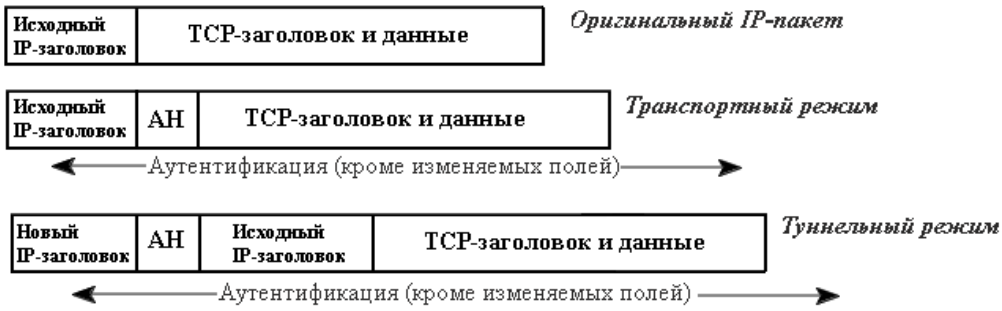

Рис. 3.9. Положение заголовка аутентификации AH в IP-пакете

В случае шифрования содержимого пакета к заголовку добавляются вложенные защищенные передаваемые данные (ESP – Encapsulated Security Payload) (рис.3.10). Заголовок ESP содержит два 32-битных слова – индекс параметра безопасности (Security parameters index) и последовательный номер. Хвост ESP состоит из заполнения (Padding), дополняющего блок шифруемых данных до требуемого размера и скрывающего истинный размер этих данных; 8-битного поля длины заполнителя (Pad length) и 8-битного поля следующего заголовка (Next header). Аутентификационные данные представляют собой «цифровую подпись» содержимого пакета.

Для защиты, как IP-заголовка, так и содержимого пакета следует использовать оба механизма.

Рис. 3.10. Положение ESP в IP-пакете

Режимы работы IPSec

Существует два режима работы IPSec: транспортный режим и туннельный режим. Первый характерен для локальных сетей, второй - для глобальных.

В транспортном режиме (защита данных в пакете) шифруется (или подписывается) только информативная часть IP-пакета. Так как заголовок IP пакета не изменяется (не шифруется), то маршрутизация не затрагивается.

Транспортный режим, как правило, используется для установления соединения между хостами. Он может также использоваться между шлюзами, для защиты туннелей, организованных каким-нибудь другим способом (IP tunnel, GRE и др.). Соединение и процесс инкапсуляции в транспортном режиме работы IPSec показан на рис. 3.11 и рис.3.12 соответственно.

Рис.3.11.Соединение IPSec. Транспортный режим

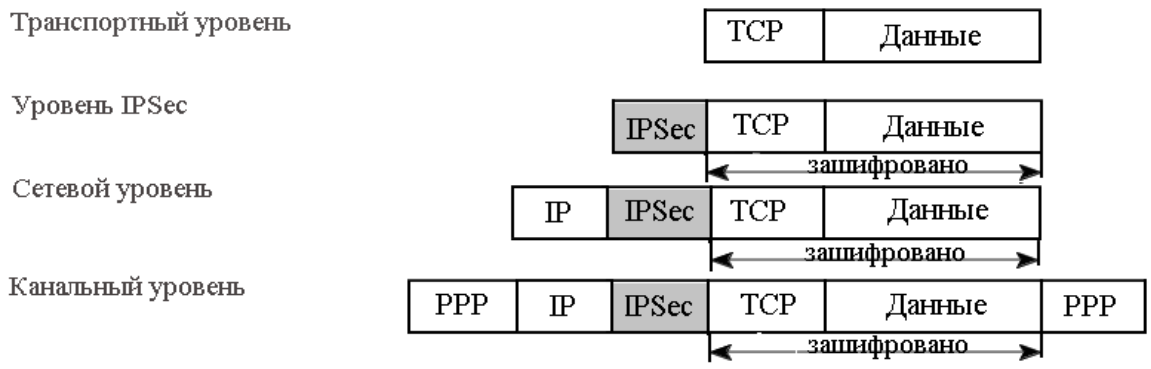

Рис. 3.12. Инкапсуляция IPSec для транспортного режима

В туннельном режиме (защита всего пакета, включая заголовок) IP-пакет шифруется целиком. Для того, чтобы его можно было передать по сети, он помещается в другой IP-пакет. По существу, это защищённый IP-туннель. Туннельный режим может использоваться для подключения удалённых компьютеров к виртуальной частной сети или для организации безопасной передачи данных через открытые каналы связи между шлюзами для объединения разных частей виртуальной частной сети. Соединение туннельном режиме показано на рис.3.13 (SG1 и SG2- шлюзы защиты).

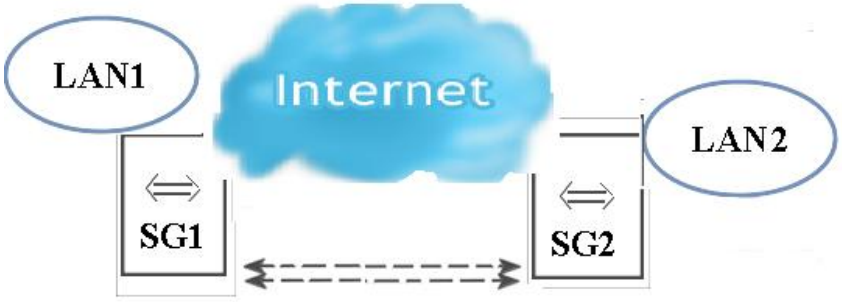

Рис.3.13. Соединение IPSec. Туннельный режим.

В туннельном режиме к пакету добавляется новый IP-заголовок, исходный IP-заголовок инкапсулируется (предварительно шифруется), адрес приемника и передатчика может изменяться на адрес граничного шлюза, инкапсуляция может производиться оконечной станцией или шлюзом VPN. Процесс инкапсуляции IPSec в туннельном режиме показан на рис.3.14.

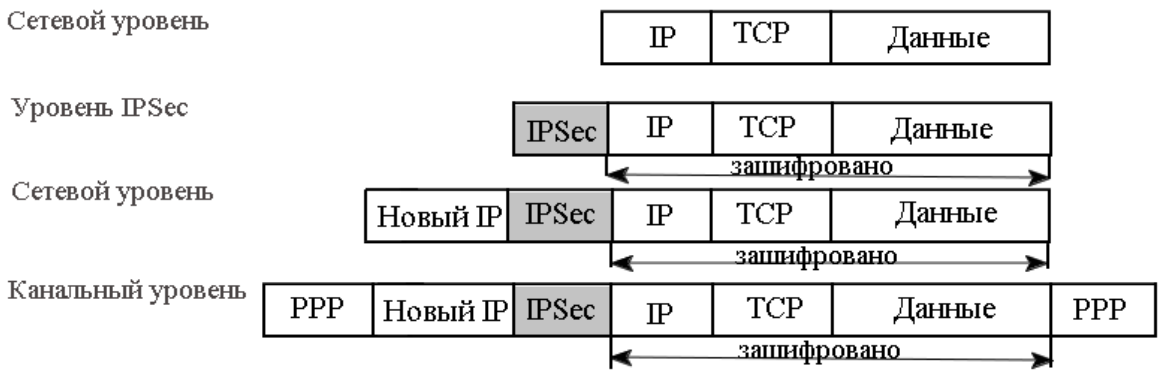

Рис. 3.14. Инкапсуляция IPSec для туннельного режима

Режимы IPSec не являются взаимоисключающими. На одном и том же узле некоторые SA (Security Associations) могут использовать транспортный режим, а другие — туннельный.

3.3.2. Протоколы SSL/TLS

Протокол SSL (Security Socket Layer) и близкий к нему протокол TLS (Transport Layer Security) представляет собой протоколы (над TCP), предназначенные для защиты прикладных протоколов.

Протокол SSL предложен Netscape Corporation в 1996 г. Актуальной в настоящее время является версия 3. Протокол TLS появился в январе 1999 г.

Протоколы обеспечивают:

- Конфиденциальность данных;
- Аутентификацию сервера и клиента;
- Целостность данных и опционально их компрессию.

Протоколы действуют при установке соединения (SSL/TLS handshake protocol протокол установления связи) и при шифровании данных (SSL/TLS record protocol – протокол записей).

Задачи SSL/TLS handshake protocol:

- Согласование версии протокола;
- Согласование алгоритма шифрования;
- Аутентификация обеих сторон или по выбору;
- Обмен ключами.

Процедура установления соединения на примере протокола SSL приведена на рис. 3.15.

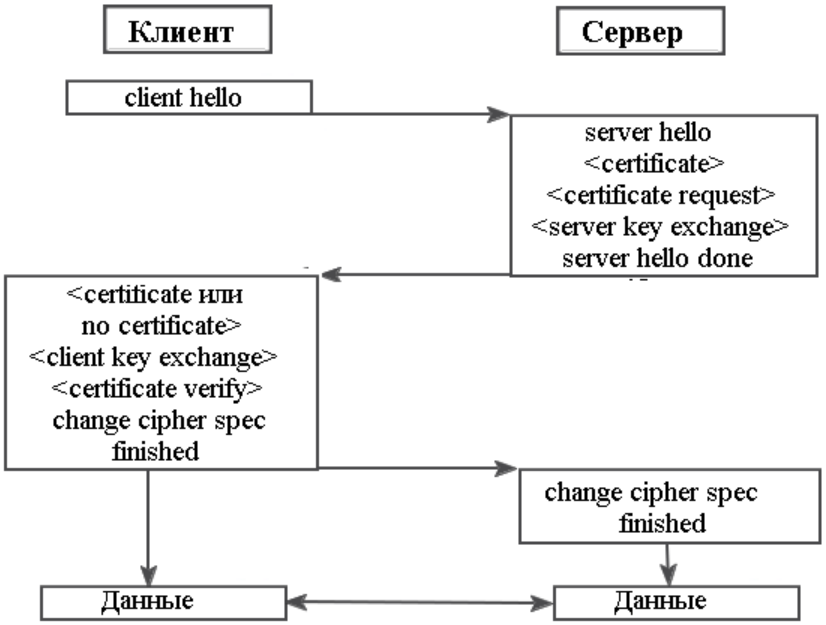

Рис.3.15. Установление соединения по протоколу SSL

В < > указаны опциональные параметры:

Client hello- сообщение клиента с информацией о:

Версии протокола,

Номере соединения (сессии),

Списке алгоритмов шифрования,

Списке методов компрессии,

Опорном случайном числе;

Server hello – поля Client hello, поддерживаемые сервером;

Certificate- сертификат сервера;

Certificate request- запрос сертификата клиента;

Server key exchange- способ передачи открытого ключа сервера;

Server hello done- конец сообщений сервера;

Client certificate или no certificate- наличие/ отсутствие сертификата клиента;

Client key exchange- данные для генерации секретных ключей;

Certificate verify- подтверждение своего сертификата;

Change cipher spec- параметры выбраны и занесены в список текущих;

Finished- конец согласований [12].

3.3.3. Программа PGP

Для шифрования электронной переписки во всем мире очень распространены программы PGP (Pretty Goode Privacy – достаточно хорошая секретность). Начиная с 1991 года является достаточно сильным средством криптографической защиты информации для пользователей сети Интернет. В основу работы PGP положена асимметричная криптография, использующая взаимосвязные пары ключей: закрытый, хранящийся только у владельца и служащий для расшифрования данных и их цифрового подписания, и открытый, который не нуждается в защите и может быть широко распространен и используется для зашифрования и сличения цифровых подписей (см. главу 3.4). На рис. 3.16 схематично показан обмен сообщениями, посредством шифрования алгоритмом с открытым ключом.

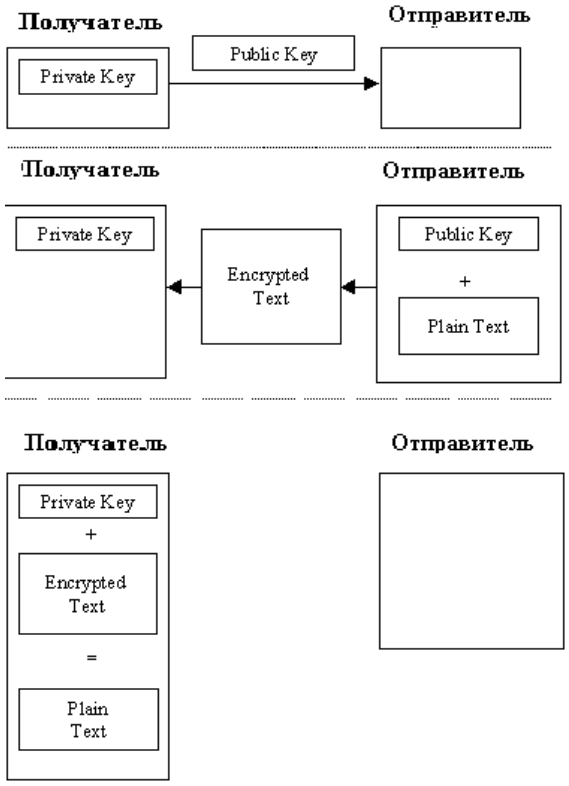

Рис. 3.16. Алгоритм шифрования открытым ключом

Алгоритм шифрования с закрытым ключом требует защищенного канала для передачи этого самого ключа. Система с открытым ключом позволяет распространять ключ для зашифровки сообщения совершенно свободно (это и есть открытый ключ), но расшифровать сообщение можно

только при помощи второго, закрытого ключа, который хранится уже у пользователя. Это справедливо и в обратную сторону. Недостатком этого алгоритма является его низкая скорость выполнения. При шифровании сообщения в PGP эти оба ограничения обойдены. Вначале генерируется случайным образом ключ для алгоритма с закрытым ключом. Ключ генерируется только на один сеанс, таким образом, что повторная генерация того же самого ключа практически невозможна. После того, как сообщение зашифровано, к нему прибавляется еще один блок, в котором содержится данный случайный (сеансовый) ключ, но уже зашифрованный при помощи открытого ключа алгоритма RSA (Rivest-Shamir-Adleman -это алгоритм ассиметричного шифрования, получивший свое название от имен его создателей) [13].

PGP имеет две основных возможности – шифровать данные и составлять электронную подпись (PGP-сигнатуру). Программа PGP достаточно распространена в Интернете и используется обычно с почтовыми программами.

3.4. Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) - это важный элемент электронного документооборота, который обеспечивает качественную защиту электронного документа от возможной подделки и умышленного изменения содержащейся в нем информации. ЭЦП подпись предназначена для аутентификации лица, подписавшего электронный документ. Кроме того, использование цифровой подписи позволяет осуществить:

- Контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему;

- Защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев;
- Невозможность отказа от авторства и др.

Передаваемые сообщения в сети Интернет, попав под перехват, могут быть не только прочтены, но и модифицированы. Цифровая подпись файлов или электронных почтовых сообщений выполняется с использованием криптографических алгоритмов, использующих асимметричные ключи, т.е. для подписи используется "секретный ключ", а для проверки чужой подписи - "открытый". Ключи представляют собой числа достаточно большой длины (от 512 до 4096 бит), математически связанные между собой. ЭЦП обладает такими свойствами, что если всего один бит информации будет (нарочно или случайно) изменен, то подпись будет недостоверна (недействительна). Основой электронной цифровой подписи является математическое преобразование подписываемых данных с использованием личного (секретного) ключа автора. Фактически, ЭЦП – это набор символов в виде строки, закодированный с помощью определенных технических средств.

В ее состав входят: открытый ключ, закрытый ключ и сертификат. Первые две части – это программные блоки в виде символов.

Ключи должен формировать центр сертификации. Центр сертификации - это некоторая структура (организация), которая занимается управлением сертификатами. Сертификат содержит основную информацию о владельце.

Для обеспечения конфиденциальности (секретности) передаваемого сообщения применяется шифрование. Для шифрования и дешифрования сообщения используется пара открытого и закрытого ключей электронной цифровой подписи, тех же, что и для формирования подписи. Для подписания сообщения используется закрытый ключ отправителя, а для шифрования — открытый ключ получателя. Получатель, используя свой

закрытый ключ - ЭЦП дешифрует, и открытый ключ отправителя - проверяет подлинность электронной цифровой подписи.

Сегодня, зачастую, для контроля целостности передаваемой информации используется построение так называемого дайджеста сообщения, или электронной подписи. При ее построении используется специальная функция, схожая по работе с функцией CRC (Control Cyclic Code- циклический код). Результаты работы этой функции шифруются.

Существует несколько схем построения цифровой подписи:

- На основе алгоритмов симметричного шифрования.

  Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.

- На основе алгоритмов асимметричного шифрования.

На данный момент такие схемы ЭЦП наиболее распространены и находят широкое применение.

Симметричные схемы имеют следующие преимущества:

- Стойкость симметричных схем ЭЦП вытекает из стойкости используемых блочных шифров, надежность которых также хорошо изучена;
- Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

У симметричных ЭЦП есть и ряд недостатков:

- Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи.

Подпись может превосходить сообщение по размеру на два порядка.

- Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписывания раскрывается половина секретного ключа.

Из-за рассмотренных недостатков симметричная схема ЭЦП Диффи-Хелмана не применяется, а используется её модификация, разработанная

Березиным и Дорошкевичем, в которой подписывается сразу группа из нескольких бит. Это приводит к уменьшению размеров подписи, но к увеличению объема вычислений.

Асимметричные схемы ЭЦП относятся к криптосистемам с открытым ключом. В отличие от асимметричных алгоритмов шифрования, в которых зашифрование производится с помощью открытого ключа, а расшифрование - с помощью закрытого, в схемах цифровой подписи подписывание производится с применением закрытого ключа, а проверка - с применением открытого.

Общепризнанная схема цифровой подписи охватывает три процесса:

- Генерация ключевой пары. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.
- Формирование подписи. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись.
- Проверка (верификация) подписи. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи.

Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:

- Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.
- Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.

На рис.3.17 приведена схема, поясняющая алгоритмы подписи и проверки.

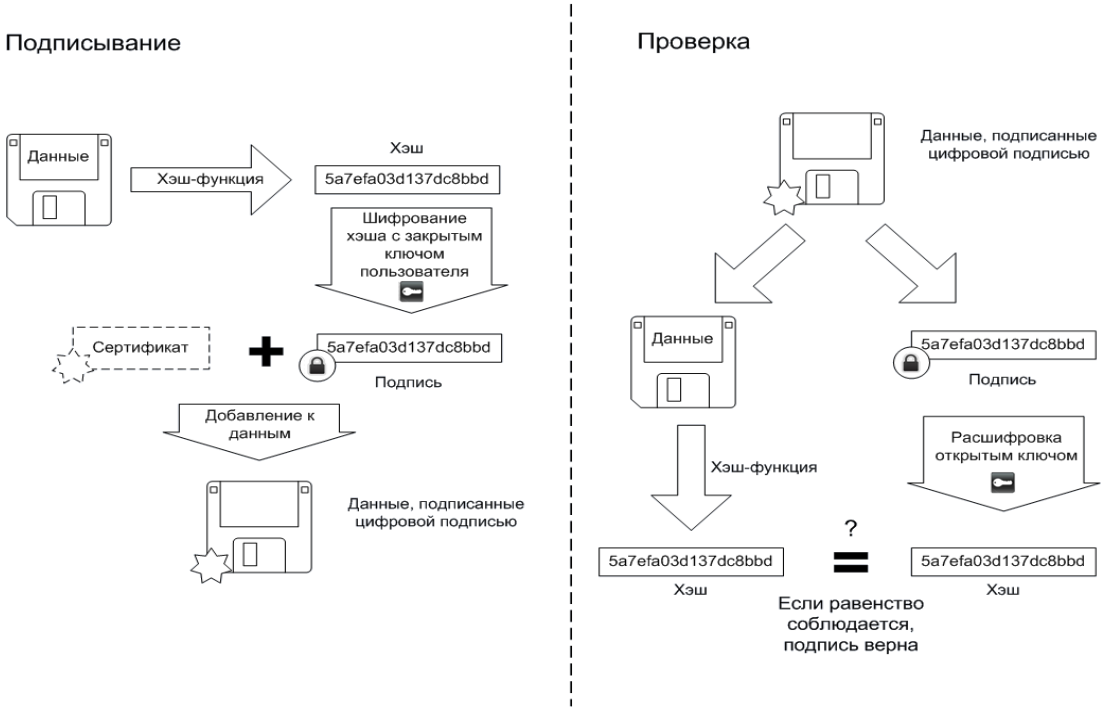

Рис.3.17. Схема, поясняющая алгоритмы подписи и проверки

Понятие электронной цифровой подписи появилось в середине 1970-х годов. Первый криптографический алгоритм был разработан в 1977 году.

В Россию ЭЦП пришла в 1994 году, когда был принят первый российский стандарт ЭЦП – ГОСТ Р 34.10-94, который в 2002 году был заменен на ГОСТ Р 34.10-2001. Новый закон РФ "Об электронной цифровой подписи" основывается на процедурах выработки и проверки подписи на основе математического аппарата эллиптических кривых. Алгоритм на эллиптических кривых - это усовершенствование схемы Эль Гамаля, часто используемой ранее для работы с ЭЦП. Новый вариант схемы Эль Гамаля использует аппарат эллиптических кривых над конечным полем из

p- элементов, которые определяются как множество пар чисел (x,y) (каждое из которых лежит в интервале от 0 до p-1), удовлетворяющих сравнению (числа a и b фиксированы и удовлетворяют некоторому дополнительному условию): y^2 = x^3 + ax + b mod p.

Первым законом, регулирующим правила пользования электронной цифровой подписью, в России был Закон РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

В марте 2011 года Госдума РФ одобрила проект Федерального закона «Об электронной подписи», который призван заменить существующий с 2002 года №1-ФЗ «Об электронной цифровой подписи». Закон призван «регулировать отношения по использованию электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также при совершении иных юридически значимых действий».

В соответствии со ст. 5 законопроекта определено три новых вида электронной подписи: простая, неквалифицированная и квалифицированная (наиболее защищенная).

- Простые подписи создаются с помощью кодов, паролей и других инструментов, которые позволяют идентифицировать автора документа, но не позволяют проверить его на предмет наличия изменений с момента подписания.
- Усиленная подпись создана с использованием криптографических средств и позволяет определить не только автора документа, но проверить его на наличие изменений. Для создания таких подписей может использоваться сертификат неаккредитованного центра, можно также вообще обойтись без сертификата, если технические средства позволяют выполнить требования закона.
- Усиленная квалицифированная подпись является разновидностью усиленных, она имеет сертификат от аккредитованного центра и создана с помощью подтвержденных ФСБ (Федеральная служба безопасности) средств [14].

Использующиеся на данный момент сертификаты ключей ЭЦП приравниваются к квалифицированным сертификатам электронной подписи.

3.5. Прокси-сервер

Прокси-сервер (от англ. proxy — представитель, уполномоченный) — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам.

Прокси-сервер - это обычная программа (а не системная), которая может работать с минимальными правами на любой ОС с поддержкой сети (стека TCP/IP). На рис. 3.18 приведен пример установления соединения с веб-сервером через прокси-сервер.

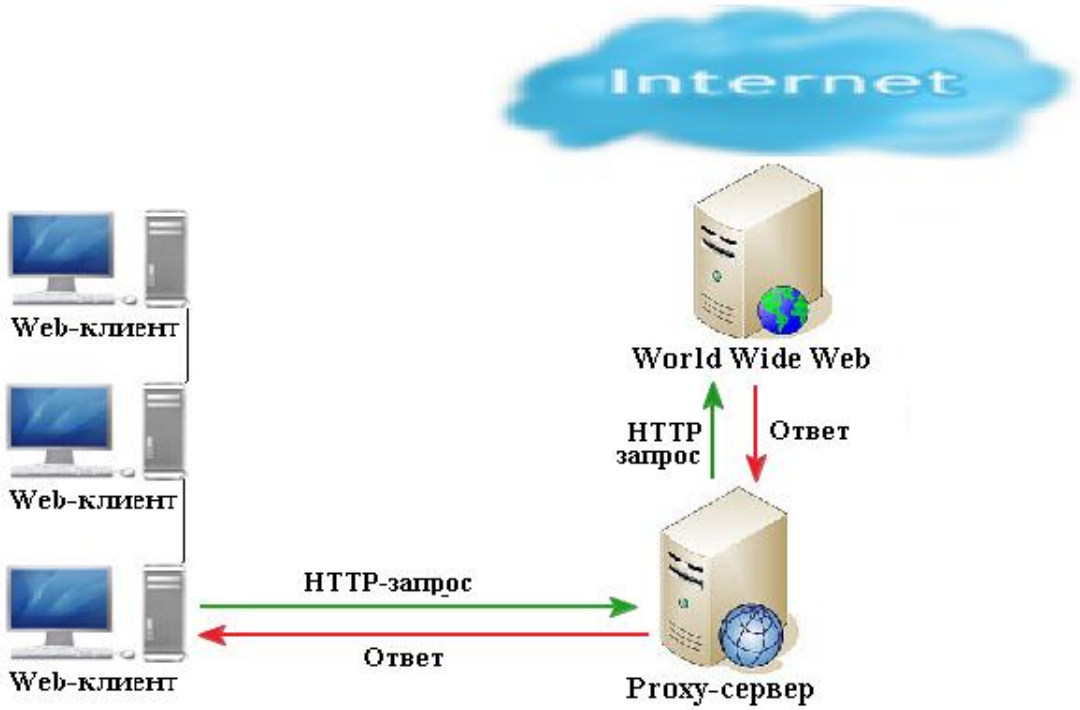

Рис.3.18. Пример установления соединения с веб-сервером через прокси-сервер.

Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс, например, e-mail, расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша, если прокси имеет свой кэш. В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Чаще всего прокси-серверы применяются для следующих целей:

- Обеспечение доступа с компьютеров локальной сети в Интернет;
- Кэширование данных. Если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации;
- Сжатие данных. Прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего трафика;
- Защита локальной сети от внешнего доступа. Например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер);
- Ограничение доступа из локальной сети к внешней. Например, можно запретить доступ к определённым веб-сайтам, ограничить использование Интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы;
- Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет возможности определить истинный источник запроса. Существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе;

- Обход ограничений доступа. Прокси-серверы популярны среди пользователей несвободных стран, где доступ к некоторым ресурсам ограничен законодательно и фильтруется.

Виды прокси-серверов

Прозрачный прокси — схема связи, при которой трафик, или его часть, перенаправляется на прокси-сервер неявно (средствами маршрутизатора). При этом клиент может использовать все преимущества прокси-сервера без дополнительных настроек, но с другой стороны, не имеет выбора.

Обратный прокси — прокси-сервер, который в отличие от прямого, ретранслирует запросы клиентов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети. Часто используется для балансировки сетевой нагрузки между несколькими веб-серверами и повышения их безопасности, играя при этом роль межсетевого экрана на прикладном уровне.

Прокси-сервер, к которому может получить доступ любой пользователь сети Интернет, называется открытым.

Технические подробности

Клиентский компьютер имеет возможность настройки (конкретной программы или операционной системы), в соответствии с которой все сетевые соединения по некоторому протоколу совершать не на IP-адрес сервера (ресурса), выделяемый из DNS-имени ресурса, или напрямую заданный, а на IP-адрес (и другой порт) прокси-сервера.

При необходимости обращения к любому ресурсу по этому протоколу, клиентский компьютер открывает сетевое соединение с прокси-сервером (на нужном порту) и совершает обычный запрос, как если бы он обращался непосредственно к ресурсу.

Распознав данные запроса, проверив его корректность и разрешения для клиентского компьютера, прокси-сервер, не разрывая соединения, сам открывает новое сетевое соединение непосредственно с ресурсом и делает

тот же самый запрос. Получив данные (или сообщение об ошибке), прокси-сервер передаёт их клиентскому компьютеру.

Из этого следуют два основных ограничения обычного прокси-сервера:

- прокси-сервер должен быть полнофункциональным сервером и клиентом для каждого поддерживаемого протокола;
- прокси-сервер может обслуживать только те сетевые протоколы, в запросе которых передаётся имя или ip-адрес ресурса (не относится к прозрачным прокси - они получают IP-адрес непосредственно из перехваченного соединения).

3.6. «Облачные» технологии

Примером формирования нового рынка на основе инновации в области информационных технологий является конкурентная борьба фирм-производителей программного обеспечения за возможность предоставления тех или иных ресурсов в качестве услуги. Появилась новая услуга, которая носит название «Облачные вычисления» - Cloud Computing. Cloud Computing служит альтернативой традиционной модели локально используемого аппаратного и программного обеспечения (on-premise).

Идея заключается в том, что документы, электронные письма и прочие данные пользователей хранятся на удаленном сервере (площадке провайдера услуг Интернет), и доступ к ним можно получать при помощи интернет-браузера с персонального компьютера, подключенного к сети Интернет. В масштабах локальной сети (например, организации, предприятия, фирмы, учебного заведения) Cloud Computing позволяет отказаться от собственной аппаратно-программной инфраструктуры, заменив ее подключением к соответствующей сетевой услуге — «облаку».

Технологии удаленного доступа к приложениям и аренда вычислительных сервисов через Интернет (интернет-хостинг) были известны и ранее. Cloud Computing — это новый виток развития модели аутсорсинга информационных технологий. Новизна «облачных вычислений» состоит в

расширении модели интернет-хостинга за пределы аренды интернет-сайтов и способности охватить широчайший круг задач, решаемых традиционными информационными технологиями, задач, чрезвычайно важных для бизнеса, например, системы взаимодействия с клиентами (CRM- Customer Relationship Management) или управления человеческими ресурсами (HR- Human Resources).

Экономическая эффективность Cloud Computing по сравнению с локально используемым аппаратным и программным обеспечением (on-premise) заключается в существенном сокращении затрат на аппаратно-программную инфраструктуру и тесно связана с технологическими преимуществами. Cloud Computing обладает следующими свойствами, составляющими экономическую эффективность этой модели:

- обеспечивает более быструю окупаемость по сравнению с традиционными информационными технологиями;
- не требует предварительных капитальных затрат;
- минимизирует операционные затраты;
- требует меньше технических ресурсов;
- предоставляет более простой уровень интеграции.

Один из наиболее важных плюсов Cloud Computing — независимость от географического расположения, как клиента, так и поставщика услуг.

«Облачные вычисления» в масштабе всей отрасли информационных технологий являются инструментом по сближению информационных технологий и бизнеса. Облачные вычисления несут явные преимущества, как для пользователей (сокращение издержек, снижение сложности обслуживания аппаратно-программной инфраструктуры), так и для поставщиков услуг (экономия за счет масштаба производства). Но при этом заказчики рискуют утратить контроль над своими данными, размещенными в «облаке». Также миграция от одного поставщика услуг к другому может оказаться более сложным процессом, чем смена пакетов традиционного программного обеспечения. Чтобы исключить такие проблемы, необходима

разработка согласованных стандартов, регламентирующих перемещение данных в «облаке». Так же возможно развитие понятий «внешнего» (public) и «внутреннего» (private) облака. Внешние облака имеют хорошие перспективы развития в сферах с открытой информацией, к примеру, в социальных сетях. Внутренние (корпоративные) облака будут развиваться на предприятиях и в организациях, для которых крайне важна безопасность информации [15].

Рассмотрим пример такого «Cloud Computing», разработанного компанией Symantec, которая является разработчиком, производителем и поставщиком систем и решений по сетевой защите, хранению данных и вычислительным комплексам.

Компания Symantec захватила 26% рынка безопасности. В сравнении с Google - в 2 раза больше позиций (рис. 3.19).

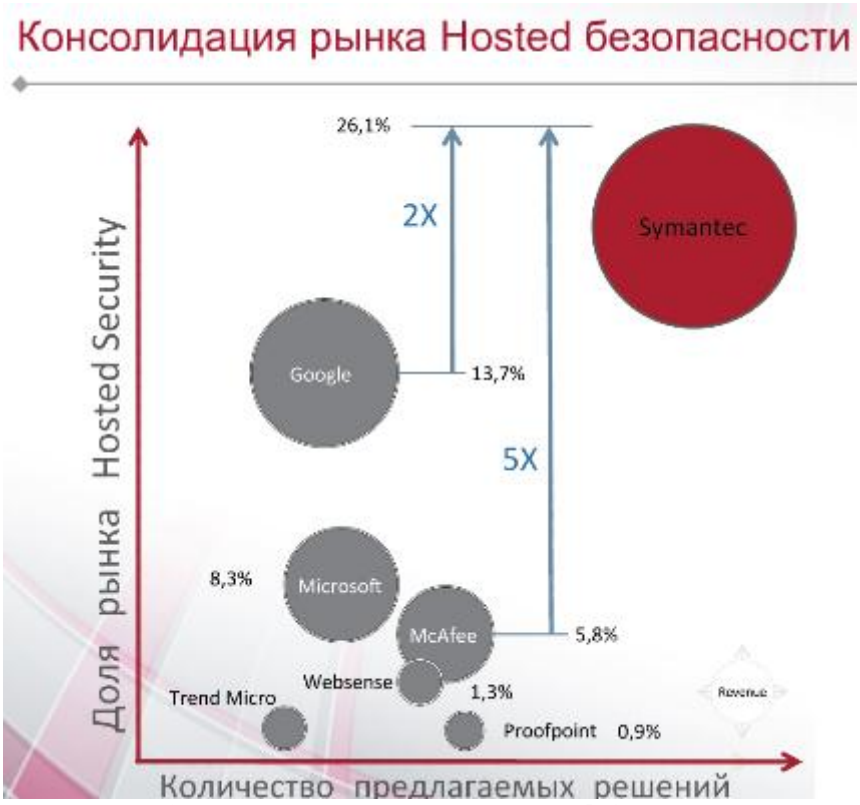

Рис. 3.19. Консолидация рынка Hosted безопасности

Выбор на изучение новой услуги Компании Symantec для обеспечения безопасности информации пал не случайно. 14 марта 2011 года я приняла участие в вебинаре, проводившимся под руководством компании Softline.

Вебинар – это мероприятие, проходящее в режиме on-line, похожее на обычный семинар – последовательные доклады, показ демонстраций, вопросы и ответы на них, но главное отличие в том, что все проходит в ресльном режиме времени через Интернет. Вебинар был посвящен знакомству с продуктом Symantec Hosted Services .

Работа Symantec Hosted Services состоит в том, что по своей структуре данный продукт состоит из гребенки фильтров. Каждый фильтр обладает своими свойствами. В основе стоит Skeptic-движок, который выполняет функцию 4-х. На почтовом сервере - не получается установить 4 движка, т.к. это будет тормозить его работу. Скептик-модуль имеет несколько фильтров, что позволяет, экономя ресурсы, определить спам или вирус, пришедшее на сервер письмо. Фильтр Content image распознает картинку и запрещает прохождение ее дальше, если, например, эта картинка содержит порно. Такие файлы зачастую содержат вирус.

Фильтр saas обновляет антивирус или антиспам на компьютере.

Другой фильтр ограничивает количество доменов или IP-адресов, распространяющих спам, и блокирует их в дальнейшем. На рис.3.20 приведена схема фильтрации почтового трафика пользователей.

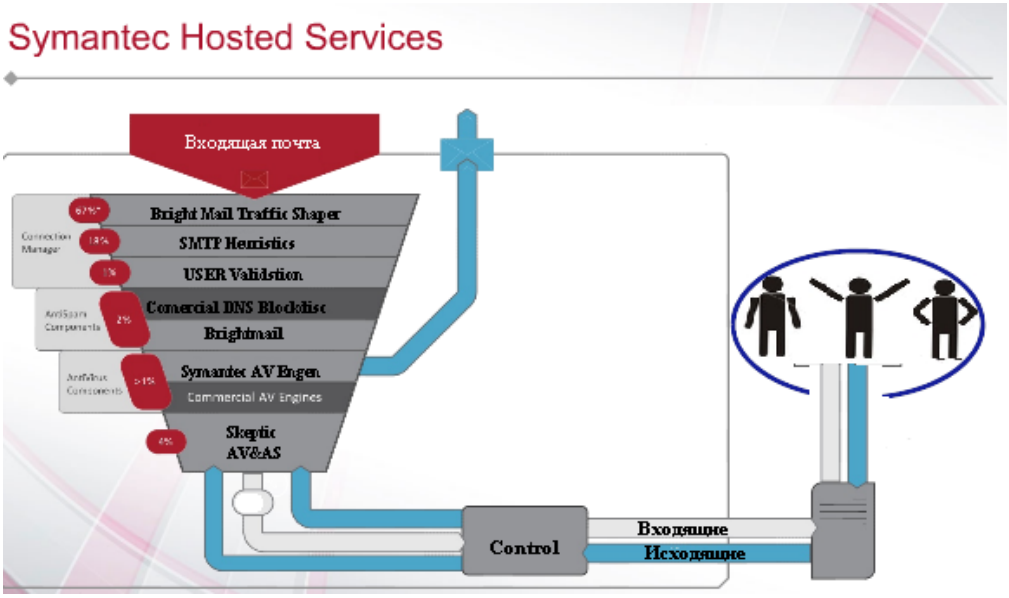

Рис. 3.20.Фильтрация почтового трафика

Ваша почта не потеряется, так как Symantec имеет 4 дата-центра в мире. И если 1-2 дата-центра «падают», то всю работу по изучению трафика берут на себя другие. Вы получите свое письмо в целостности и сохранности. Почта приходит не на сервер напрямую, поэтому не забивает канал. Symantec Hosted Services проверяет почту в «облаке» и отфильтровывает ее там. Вредоносный контент не попадет на сервера. И в сервер или на компьютер приходит чистая почта. Облачный сервис позволяет экономить ресурсы.

4. СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СОСТАВЕ ОС

На сегодняшний день любой пользователь имеет возможность не только получать посредствам Интернета интересующую его информацию, а также выбирать с помощью каких аппаратных и технических средств это осуществлять. К нашим услугам предоставлена возможность выбора операционной системы персонального компьютера, провайдера и типа соединения с Интернет, а также способов обеспечения нашей информационной безопасности. Под безопасностью операционной системы понимается помимо обеспечения безопасности самого ядра ОС еще и безопасность программного обеспечения, установленного на ней. Другими словами, безопасность операционной системы – это комплекс мер, направленных на предотвращение действий со стороны пользователя или других программ, которые могут привести к нарушению нормального функционирования операционной системы.

Говоря о безопасности ОС, следует рассмотреть локальную и сетевую безопасность по отдельности. Компьютер, на котором установлена ОС, может выступать как в качестве пользовательского компьютера, так и в качестве сервера. Локальная безопасность – это правила, меры и усилия, направленные на защиту системы изнутри, от локальных пользователей. Локальная безопасность является обязательной в любом случае, даже тогда, когда к компьютеру имеет доступ один пользователь, имеется вероятность

угрозы со стороны используемых им носителей информации. Сетевая же безопасность имеет место в том случае, когда компьютер имеет выход в сеть.

Вне зависимости от выбора ОС в основе защиты компьютера лежат «три А» - аутентификация, авторизация и аудит.

Аутентификация. Это установление подлинности пользователя, то есть установление факта того, что пользователь с таким именем является именно тем, за кого себя выдает. Для предотвращения доступа в компьютер незарегистрированных пользователей в системах защиты ОС для каждого пользователя устанавливается учетная запись и вводится в действие следующий принцип парольной защиты - пока пользователь не введет достоверного имени и пароля, указанного в учетной записи, он не сможет войти в систему. Важно удостовериться при создании аутентификации, что учетные записи пользователя защищены, и никто не может замаскироваться под зарегистрированного пользователя. С этой целью можно:

- скрывать имена пользователей;
- защищать пароли.

Пароль – это набор символов (секретное слово), известный только его владельцу и используемый для удостоверения его подлинности. Каждый пользователь в системе имеет свой собственный пароль. В каждой ОС есть возможность установить длину пароля. Microsoft рекомендует использовать минимальную длину пароля в своих ОС не менее 11 символов.

Авторизация. В любой достаточно защищенной ОС доступ к файлам пользователя определяется по группе, в которую он входит. С помощью организации групп пользователей администратору приходится настраивать систему защиты для всей группы, обладающей одинаковыми правами и разрешениями доступа к функциональным средствам системы и конкретным сегментом информации, а не делать это для каждой учетной записи в отдельности.

Аудит. Это отслеживание действий пользователя путем регистрации событий заданного типа в журнале безопасности. Аудит применяется для

контроля несанкционированного доступа к файлам и другим компонентам системы, для регистрации попыток входа в систему, выключения и перезагрузки компьютеров и т.п.[4].

Операционные системы имеют штатные средства для обеспечения информационной безопасности, к сожалению, не многие пользователи используют их. Рассмотрим такие средства защиты информации в каждой из популярных сегодня операционных систем.

4.1. Обеспечение безопасности в ОС Windows

Для входа в компьютер с ОС Windows каждому пользователю назначают персональную учетную запись с внутренним идентификатором защиты (SID - Security Identifier), по которому ОС однозначно идентифицирует пользователя. Эти учетные записи системы Windows хранятся в базе данных SAM (Security Account Manager - диспетчер учетных данных системы защиты). Для защиты базы SAM от взлома все хранящиеся в ней пароли шифруются специальным алгоритмом. Для защиты хранимых в SAM паролей применяется шифрование по методу Syskey. В последних версиях Windows, начиная от Windows 2000, для упрощения работы администраторов по управлению системными службами была разработана консоль MMC (Microsoft Management Console - консоль управления Microsoft).

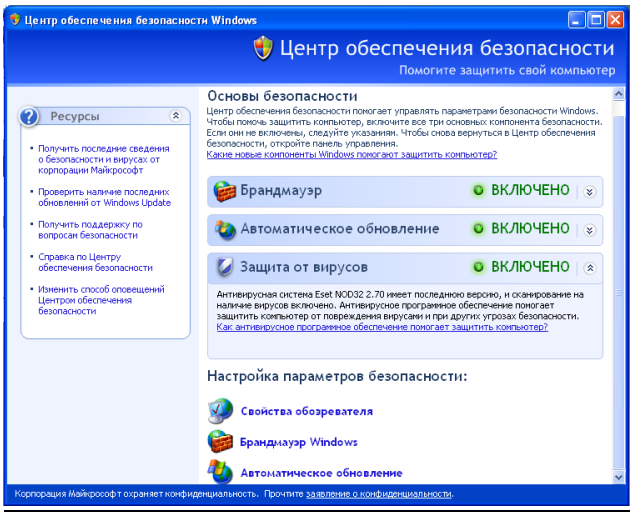

Рис.4.1. Интерфейс центра обеспечения безопасности. ОС Windows XP

4.2. Обеспечение безопасности в ОС Linux

Linux является сетевой многопользовательской системой с достаточно простой и распределенной архитектурой. Каждый пользователь имеет свой уникальный числовой идентификатор, по которому он идентифицируется в системе. Этому идентификатору соответствует имя пользователя. Например, для привилегированного пользователя root зарезервирован нулевой идентификатор.

Все имена пользователей Linux и соответствующие им идентификаторы хранятся в специальном файле passwd. Этот файл располагается в каталоге etc, который, в свою очередь, находится в корневом каталоге системы /. Файл имеет обычную текстовую форму. При входе в систему программа, предоставляющая доступ, производит чтение информации о пользователях из файла passwd. Право на запись в этот файл имеет только привилегированный пользователь root, читать же его могут все пользователи системы.

Этот файл никогда не редактируется вручную, хотя, в принципе, это вполне допустимо. Обычно для редактирования файла пользователей используют специальные программы: useradd, usermod и userdel.

Имя пользователя не является секретной информацией, и его могут без проблем узнать другие пользователи системы. Чтобы исключить возможность входа одного пользователя под именем другого, используется аутентификация пользователя с помощью пароля.

Каждый пользователь в системе имеет свой собственный пароль. Наличие пароля – необходимая составляющая политики безопасности пользователей Linux. Без пароля, зная только имя пользователя, проникнуть в систему невозможно.

Пароли хранятся в отдельном файле /etc/shadow. В ранних версиях Linux имена и пароли пользователей хранились в одном файле /etc/passwd. Но практика показала, что для обеспечения более надежной защиты паролей

необходимо создание отдельного файла для их хранения. Технология выделения отдельного файла shadow для хранения паролей получила название технологии «теневых паролей».

Для устранения сетевой угрозы, как и для локальной, существуют такие средства защиты, как межсетевые экраны.

В Linux брандмауэр является частью ядра, а поскольку все операции при работе с сетью контролирует ядро, гарантию того, что все сетевые пакеты пройдут через него, можно считать практически стопроцентной [16].

Для настройки и управления брандмауэром в составе ОС Linux поставляется программный пакет iptables. На рис.4.2 показан интерфейс настройки брандмауэра в ОС Linux.

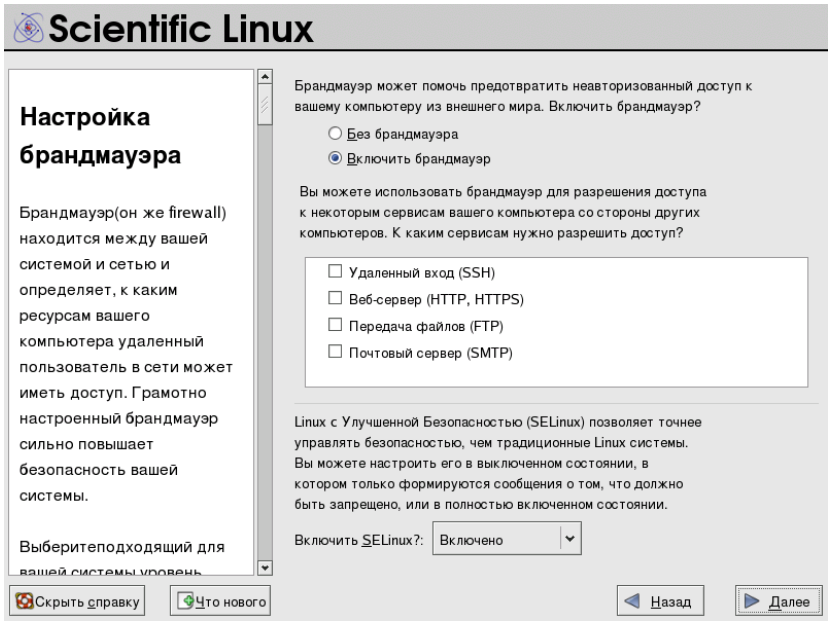

Рис. 4.2. Настройка брандмауэра в ОС Linux

Помимо стандартных средств организации безопасной работы Linux существует большое количество дополнительного системного программного обеспечения, позволяющего расширить возможности стандартных средств и добавить новые, более гибкие и приспособленные к специфическим условиям. Когда к системе предъявляются повышенные требования, и стандартных средств обеспечения безопасности может оказаться недостаточно, тогда используют дополнительные программные пакеты.

4.3. Обеспечение безопасности в Mac OS X

При разработке системы Mac OS X учитывались самые последние требования к безопасности. Встроенная защита от вирусов и вредоносного ПО не мешает работе пользователя сообщениями и отчётами системы безопасности. Файлы, загружаемые через Safari, Mail и iChat, проверяются на наличие в них опасных программ. При обнаружении угрозы Mac OS X уведомляет пользователя, а затем предупреждает об угрозе при первом открытии приложения. Пользователь сам решает, открыть приложение или лучше отказаться от этого. Mac OS X может также использовать цифровые подписи, чтобы отслеживать изменения в приложениях с момента их создания.

Mac OS X обеспечивает многослойную систему защиты от вирусов и других вредоносных программ. Например, система защищает программы от хакеров с помощью метода под названием «песочница», который ограничивает возможные действия вредоносных программ на Mac, их доступ к файлам и запуск ими других программ. Среди других автоматических функций безопасности — случайное перемещение системных библиотек, не позволяющее вредоносным командам достичь своей цели, а также функция отключения выполнения, защищающая от атак память компьютера Mac.

При возникновении угрозы безопасности Apple даёт быстрый ответ, позволяя автоматически загрузить и установить программные обновления для обеспечения безопасности. Для упреждающей идентификации и быстрого устранения уязвимостей операционной системы компания Apple сотрудничает с сообществом аварийного реагирования, в том числе через форум FIRST, объединяющий группы реагирования на нарушения информационной безопасности, и через группу защиты FreeBSD. Кроме того, Apple тесно взаимодействует с такими организациями как CERT/CC (Координационный центр группы компьютерной «скорой помощи»).

В Mac OS X можно легко настраивать и использовать функции защиты. Например, для настройки безопасного обмена файлами нужно выполнить

всего лишь несколько действий в системных настройках. FileVault позволяет шифровать все файлы в домашней папке — для этого достаточно сделать пару нажатий мышью и выбрать пароль. Межсетевой экран предварительно настроен на блокировку сетевых вторжений, но можно легко внести любые изменения в настройки.

В Mac OS X присутствует такое понятие как «родительский контроль».

Родительский контроль - это возможность настраивать запрет к доступу определенных сайтов или программ для детей. Настроив функцию «родительский контроль», можно контролировать, сколько времени дети проводят за компьютером, на какие сайты они заходят и с кем общаются.

Предусмотрена защита от фишинга. Технология защиты от фишинга в Safari позволяет выявить подменённые веб-сайты. При посещении подозрительного сайта Safari блокирует эту страницу и выдаёт предупреждение [17].

Mac OS X позволяет легко поддерживать безопасность компьютера в сети. Функция «Ассистент пароля» позволяет заблокировать доступ похитителям личных данных, а встроенные технологии шифрования защищают личную информацию и обеспечивают безопасное общение. На рис.4.3 показан интерфейс центра обеспечения безопасности в Mac OS X.

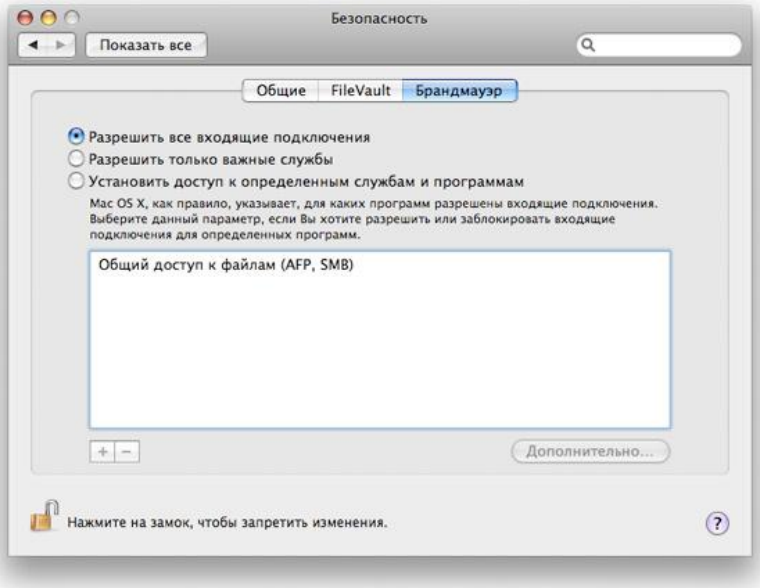

Рис.4.3. Интерфейс центра обеспечения безопасности в Mac OS X

Несколько способов обеспечить максимальную безопасность информации.

- Использовать FileVault для шифрования самых ценных документов.
- Контролировать доступ к Mac, блокируя экран при отсутствии работы.
- Безопасно удалять устаревшие ценные файлы с помощью команды «Очистить Корзину необратимо».

4.4. Рекомендации для пользователей услуг Интернет

В дипломной работе были рассмотрены некоторые угрозы, подстерегающие обычных пользователей Интернета. Противостояние такого рода угрозам включает два основных момента:

- Пользователь должен быть бдительным и не поддаваться психологическим ухищрениям злоумышленников, которые стараются всеми силами заставить его выполнить действия, реализующие атаку на локальный компьютер;
- Требуется установить рубеж защиты компьютера, который будет включать в себя необходимые средства обеспечения информационной безопасности.

Рекомендации, которым следует придерживаться:

- Использовать современные ОС с регулярными обновлениями;
- Использовать лицензионное ПО;
- Работать на ПК под правами пользователя, а не администратора;
- Использовать антивирусные и антиспам-продукты известных производителей с автоматическими обновлениями сигнатурных баз.

Рекомендацией к использованию такого продукта для ПК, учитывая проведенные исследования, является антивирусная программа Kaspersky Internet Security 2011 (11.0.2.556);

- Использовать персональный межсетевой экран и настроить его на прием трафика из достоверных источников;
- Ограничить физический доступ к компьютеру посторонних лиц;
- Не открывать файлы, полученные от ненадёжных источников;
- Использовать внешние носители информации только от проверенных источников;
- Для хранения наиболее важной информации использовать резервное копирование данных и др.
- Чтобы защититься от угроз, связанных с сервисами электронной почты и доставки файлов, стоит придерживаться следующим рекомендациям:
- Настройте антивирусную программу на непрерывную проверку поступающего трафика на наличие вирусов;
- Чтобы исключить перехват паролей доступа, используйте почтовые службы, предоставленными на Web-сайтах, поддерживающих SSL-доступ при регистрации на сайте и имеющих сертификат от доверенных бюро CA;
- Отсылаемые электронные письма шифруйте и подписывайте своей ЭЦП. Если у Вас нет правомочной (легитимной) подписи, используйте средства PGP для создания доверенных отношений с получателями своих писем и др.

Только применение комплексных мер и соблюдение вышеизложенных рекомендаций, в не зависимости от используемой ОС на ПК, может привести к информационной безопасности пользователей услуг сети Интернет. Применение рассмотренных способов и средств защиты информации по отдельности не приведет к требуемому результату.

5. НАСТРОЙКА БРАНДМАУЭРА В ОС WINDOWS

В ОС Windows XP фирма Microsoft включила брандмауэр ICF (Internet Connection Firewall – брандмауэр соединений с Интернет), который позволяет защитить соединения с Интернет от хакерских атак.

Брандмауэр ICF представляет собой шлюз с сохранением состояния, который отслеживает все аспекты состояния соединения с Интернет, включая начальный и конечный адрес каждого сообщения. Весь входящий из Интернет трафик проходит сравнение с данными, хранящимися в таблице соединений брандмауэра ICF. В компьютер могут проникнуть только те сообщения, которые либо приходят из внутрисетевых компьютеров, либо удовлетворяют правилам настройки брандмауэра. Имеется возможность указать, к каким службам FTP, HTTP и др., запущенным на компьютере, разрешается обращаться внешним приложениям и пользователям, а также на какие запросы ICMP из Интернет компьютеру разрешается отвечать. По умолчанию они отключены.

Недостатком ICF брандмауэра является ограниченность его функций только защитой соединения с Интернет. Возможности и недостатки брандмауэра в Windows приведены в табл. 5.1.

Таблица 5.1

Возможности	Недостатки
Блокировка доступа на компьютер вирусов и червей.	Невозможно обнаружить или обезвредить вирусы и черви, если они уже попали на компьютер.
Запрос пользователя на блокировку или разрешение на подключение потенциально опасных запросов из сети.	Невозможно запретить пользователю открывать сообщения электронной почты с опасными вложениями.
Ведение журнала безопасности.	Невозможно блокировать спам или несанкционированные почтовые рассылки.

Работа брандмауэра определяется параметрами: «Включить», «Включить, но не разрешать исключения» и «Выключить» (рис. 5.1).

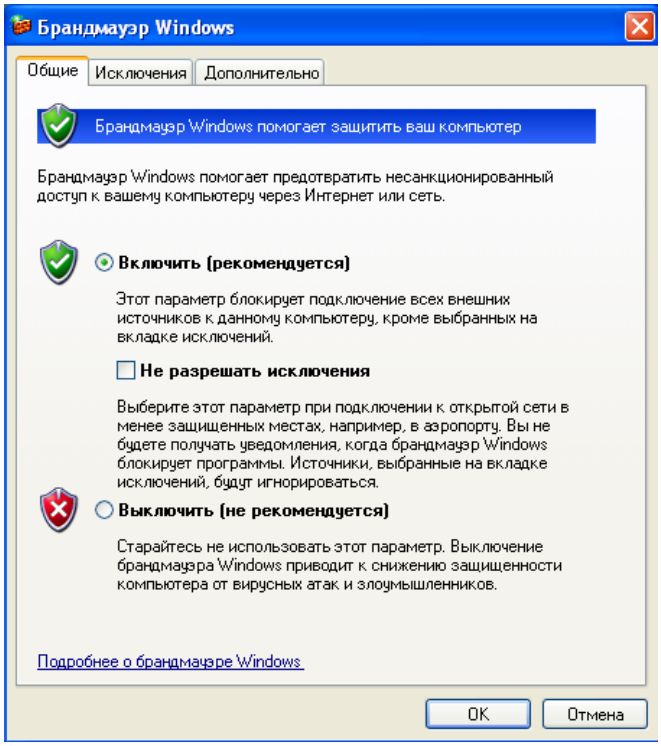

Рис. 5.1. Графический интерфейс брандмауэра Windows

Включить. По умолчанию брандмауэр включен. В этом состоянии он блокирует все непредусмотренные запросы на подключение к вашему компьютеру за исключение тех, которые предназначены для программ или служб, выбранных на вкладке «Исключения» (рис. 5.2).

Чтобы разрешить непредусмотренные исключения необходимо на вкладке «Исключения» нажать кнопку «Добавить программу», и в появившемся окошке выбрать необходимую программу и подтвердить выбор кнопкой «ОК» (рис. 5.3).

Для временного удаления из списка программы снимается соответствующий флажок. Для длительного удаления программы - выделяем требуемую программу и нажимаем кнопку «Удалить». После чего подтверждаем выбор кнопкой «ОК» (рис. 5.4).

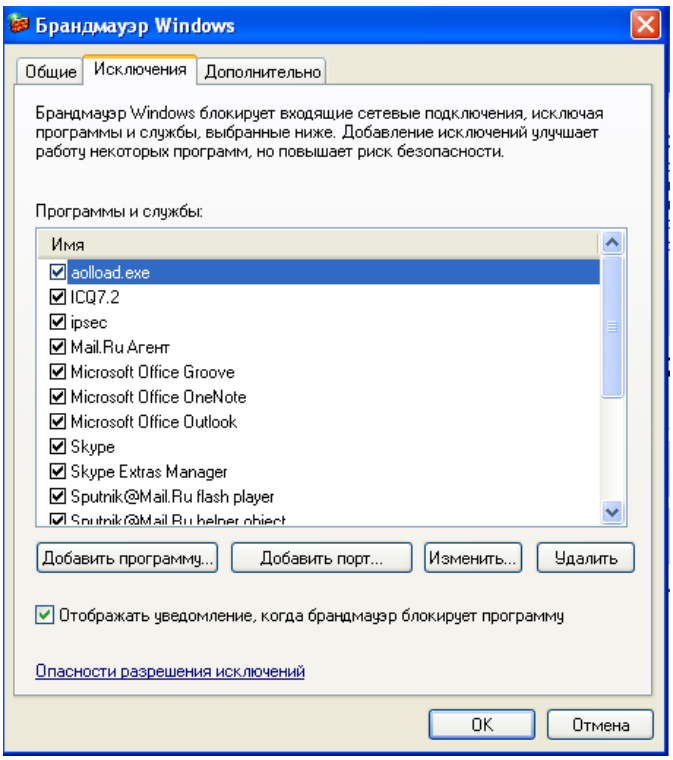

Рис. 5.2. Вкладка «Исключения» интерфейса Брандмауэра

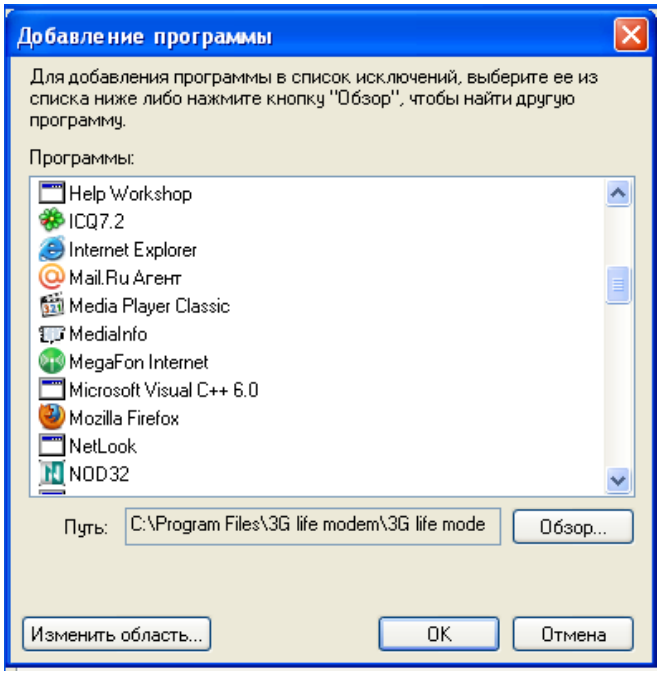

Рис. 5.3. «Добавление программы» во вкладке «Исключения»

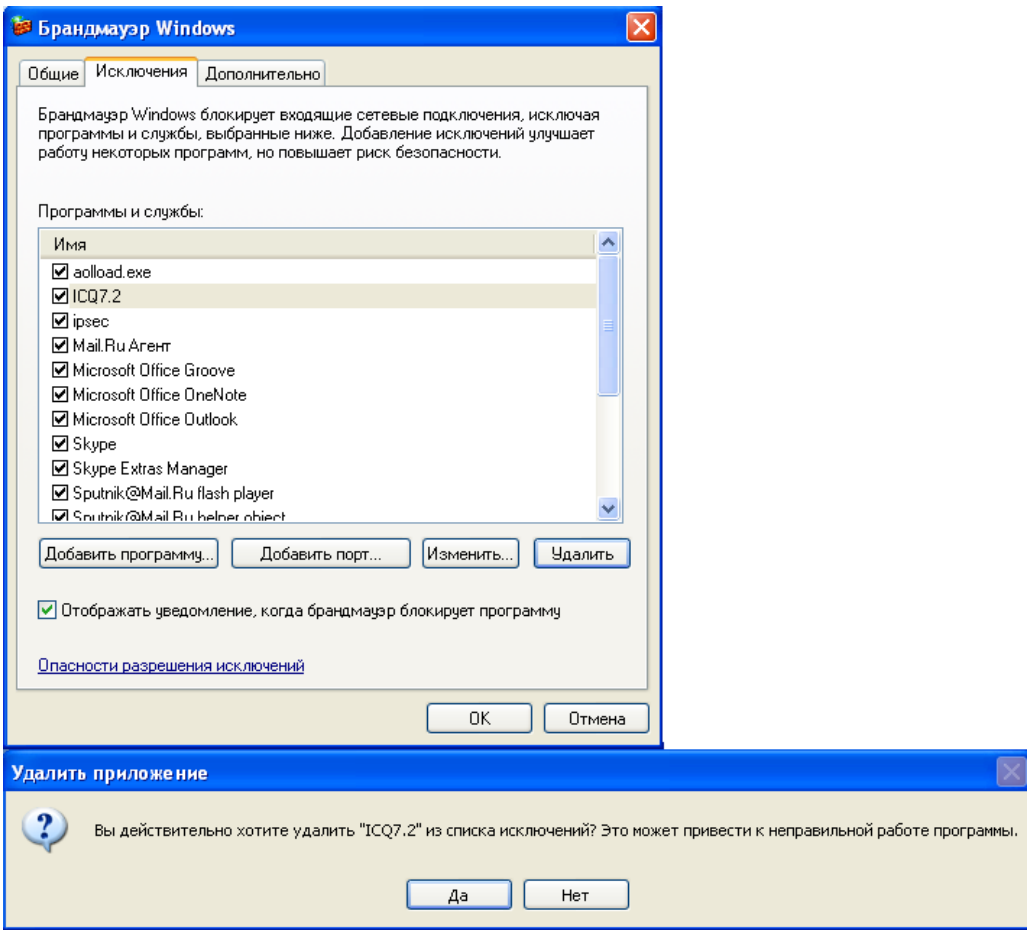

Рис. 5.4. Удаление приложения

Чтобы обеспечить безопасность компьютера, следует брандмауэр держать включенным, чтобы он блокировал любые непредусмотренные запросы на подключение к компьютеру. Для возможности подключения такого типа необходимо разрешить исключение или открыть порт для конкретной программы или службы.

Порт – это «проход» в компьютер, через который может передаваться информация. Каждый открытый порт, дающий программе или службе связываться через брандмауэр, делает компьютер уязвимым.

Разрешение работы программ через порт показано на рис. 5.5.

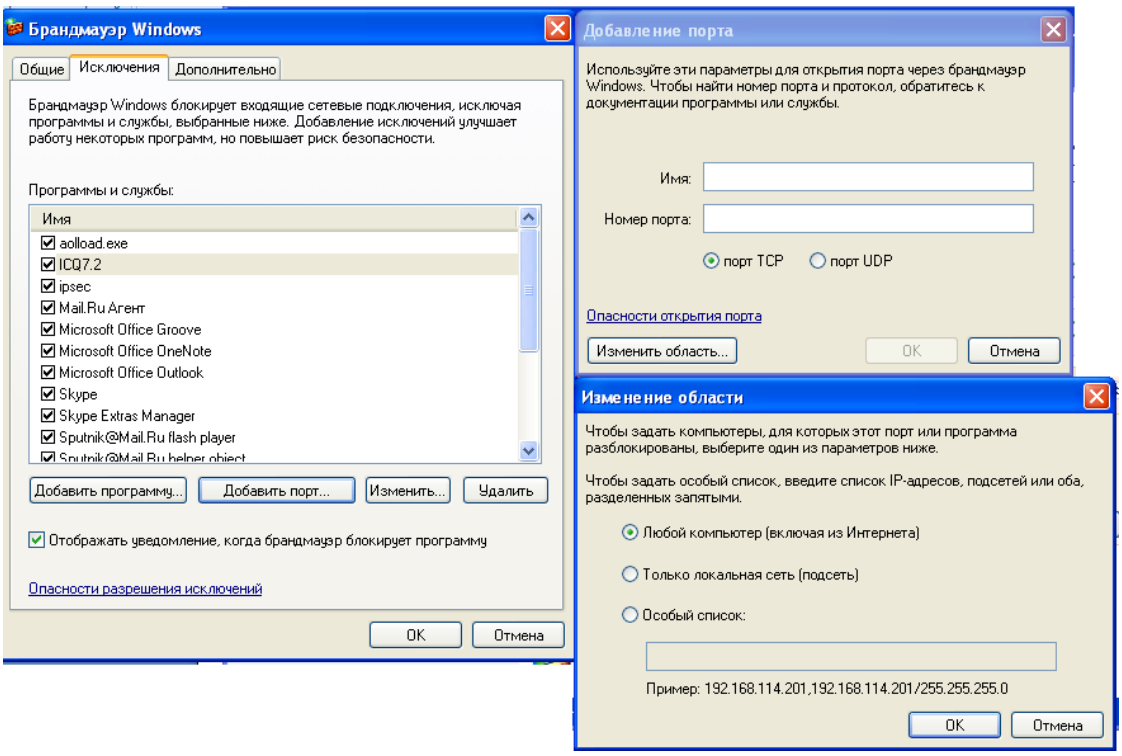

Рис. 5.5. Добавление порта

У каждого порта есть свой номер. Многие программы и службы имеют «постоянные адреса». Если во вкладке изменение области выбран вариант «Любой компьютер», то к компьютеру смогут подключиться любые компьютеры из локальной сети или сети Интернет. Если выбран вариант «Только локальная сеть» – смогут подключиться компьютеры локальной сети. Если «Особый список», то – доступ будет разрешен тем компьютерам, чьи IP-адреса и подсети укажут в поле. Рекомендуется вручную закрыть доступ к следующим входящим портам (с указанием протокола доступа) (табл. 5.2):

Таблица 5.2

Протокол	Порты
TCP	20; 25; 69; 135; 139; 445; 555; 4444; 12345; 54321; 54320; 65000
UDP	69; 135; 137; 139; 445

Включить, но не разрешать исключения. Брандмауэр блокирует все непредусмотренные запросы на подключение к компьютеру, в том числе и те, которые предназначены для программ и служб, выбранных на вкладке «Исключения».

Не разрешать исключения. Можно отправлять и получать электронную почту, использовать программу передачи мгновенных сообщений или просматривать большинство Web-страниц. Но при установке флажка в поле «Не разрешать исключения» некоторые программы могут перестать работать корректно, к тому же, будут блокироваться непредусмотренные запросы к следующим службам:

- Служба доступа к файлам и принтерам;
- Средства «Удаленный помощник» и «Дистанционное управление рабочим столом»;
- Обнаружение сетевых устройств;
- Заранее настроенные программы и службы в списке «Исключения»;
- Дополнительные объекты, добавленные в список «Исключения».

Есть возможность открывать порты и настраивать их для отдельных подключений. Для этого стоит воспользоваться вкладкой «Дополнительно» и использовать параметры в группе «Параметры сетевого подключения» (рис.5.6).

Сочетание параметров на вкладке «Исключения» и любых параметров на вкладке «Дополнительно» в разделе «Параметры сетевого подключения» называются результирующим набором параметра брандмауэра Windows.

Выключить. Отключает брандмауэр, в результате чего компьютер становится уязвимым к атакам злоумышленников и вирусов.

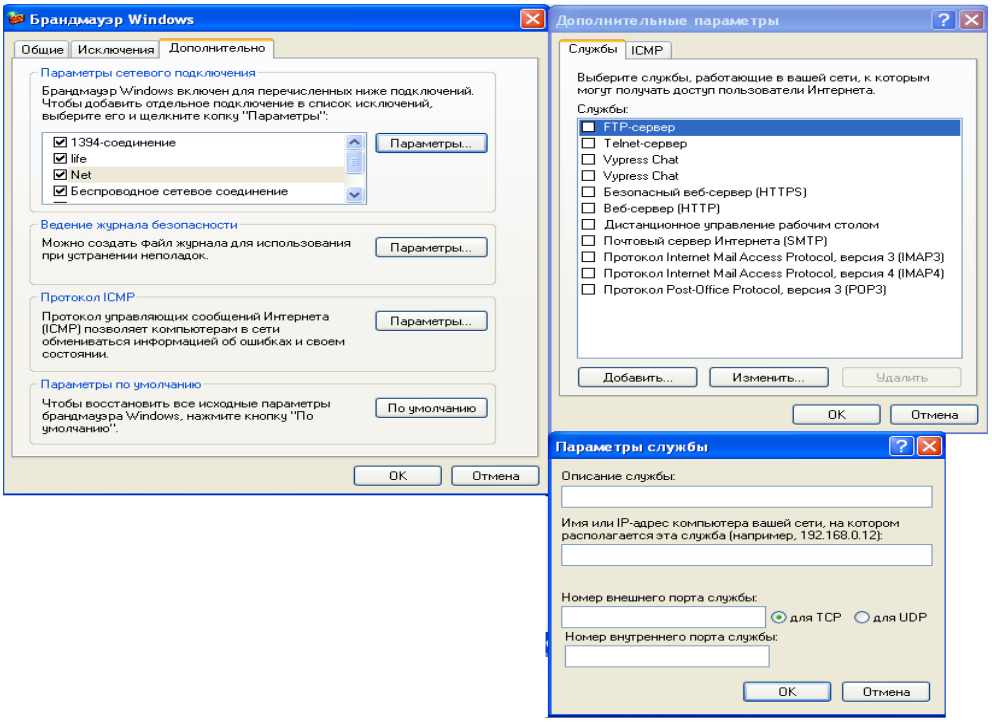

Рис. 5.6. Параметры сетевого подключения

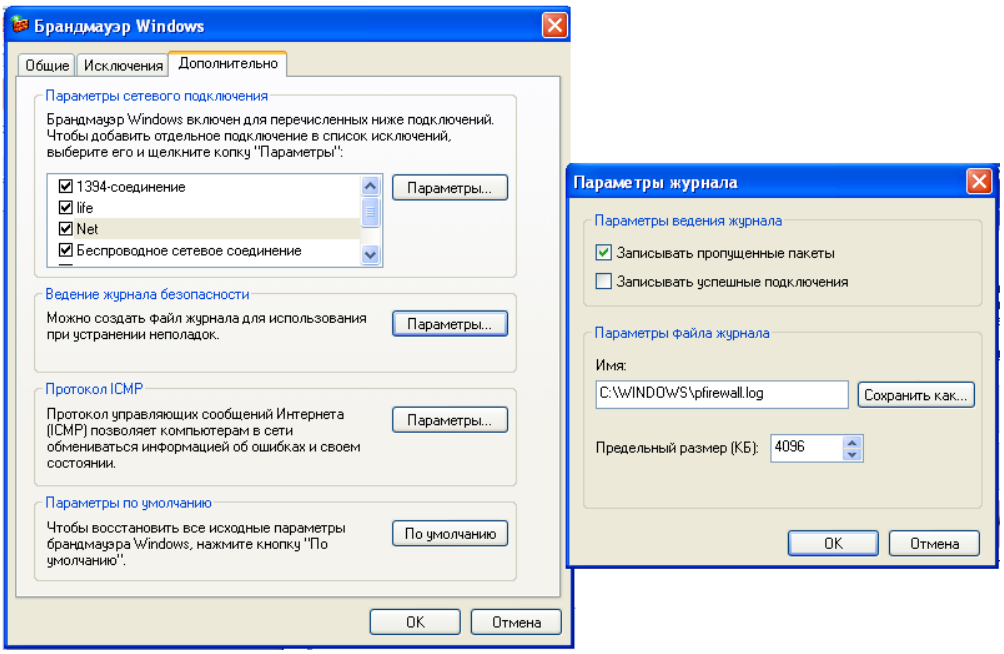

Рис. 5.7. Настройка параметров ведения журнала безопасности

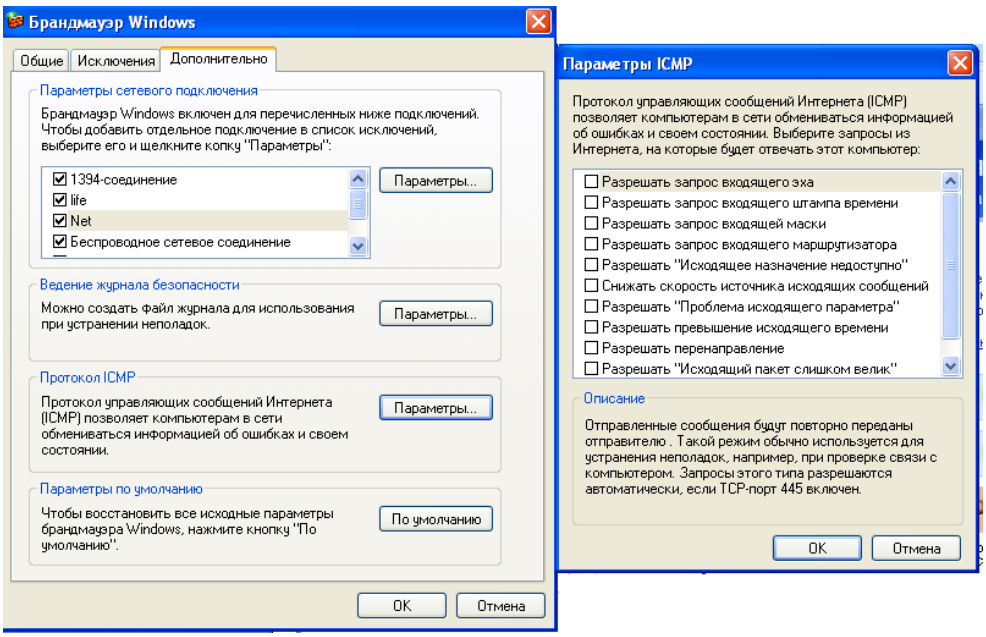

Рис. 5.8. Настройка параметров протокола ICMP

Опыт эксплуатации брандмауэров показывают, что только правильно сконфигурированный брандмауэр обеспечивает надежную систему защиты; хорошо настроенный брандмауэр практически неуязвим для злоумышленников, но плохо защищенный и некорректно сконфигурированный брандмауэр может стать причиной многих неприятностей.

5.1. Реализация учебного видео-пособия по настройке брандмауэра 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 File.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.).

ЗАКЛЮЧЕНИЕ

В ходе дипломной работы проведен анализ возможных угроз информационной безопасности пользователей услуг Интернет. Рассмотрены основные услуги сети Интернет, а также деструктивные факторы, существующие в Сети, и последствия их разрушительного воздействия. Рассмотрены классификации, даны описания и характеристики распространенных вирусов.

Приведены результаты сравнительного анализа последних версий современных антивирусных программ по различным критериям. Даны описания и схемы подключения межсетевых экранов, описаны принципы работы основных протоколов, использующихся для защиты информации и ПК.

Даны рекомендации для пользователей услуг сети Интернет по выбору средств, обеспечивающих защиту информации. Разработан обучающий видео-курс по настройке брандмауэра в ОС Microsoft Windows XP.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Гольдштейн Б. С., Соколов Н.А., Яновский Г. Г. Сети связи. СПб.: БХВ-Петербург, 2010.
2. www.pingdom.com
3. www.opds.sut.ru
4. Прохода А.Н. Обеспечение Интернет-безопасности. Практикум. Москва.: Горячая линия - Телеком, 2007.
5. Закон РФ N 85-ФЗ от 04.07.96" Об участии в международном информационном обмене".
6. Приходько А.Я. Словарь-справочник по информационной безопасности. 2001 г.
7. Национальный стандарт Российской Федерации «Защиты информации. Основные термины и определения» ГОСТ Р 50922-2006.
8. Рекомендации по стандартизациям «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005) и словарь терминов по безопасности и криптографии Европейского института стандартов электросвязи
9. Домарев В. В. Безопасность информационных технологий. Системный подход. Киев.: ДиаСофт, 2004.
10. www.antivirus-analiz.ru/antivirus.html
11. www.securelist.com/ru/analysis/208050692/rss/analysis
12. Жеребцова А.В., Захаров А.А., Созиев Д.М. Локальные и глобальные компьютерные сети: учебное пособие. СПб: СПбГУТ, 2005.
13. Блэк У. Интернет: протоколы безопасности. Учебный курс. СПб: Питер, 2001.
14. Федеральный закон РФ № 63-ФЗ от 06 апреля 2011 г. «Об электронной цифровой подписи»
15. всеос.рф/blogs/облачные-вычисления/

16.всеос.рф/blogs/безопасность-linux/

17. www.apple.com/ru/macosx/sequrity/

18.Зима Владимир, Молдовян Александр, Молдовян Николай. Безопасность глобальных сетевых технологий. СПб.:БХВ-Петербург, 2003.

19.Гордейчик С. В., Дубровин В. В. Безопасность беспроводных сетей. Москва.: Горячая линия - Телеком, 2008.

20.Леонтьев В. Безопасность в сети Интернет. Москва: ОЛМА Медиа Групп. 2008.