ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

НУКУССКИЙ ФИЛИАЛ ТАШКЕНТСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра информационных технологии

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Бухарбаева Нурсултана студента 4–го курса факультета компьютерной инжиниринга по направлению сервис предприятия

ТЕМА: Криптографический метод и их алгоритмы защиты информаций в Интернете

Научной руководитель: _____ **Начальник отдела RC Каракалпакского филиала АК «Ўзбектелеком» Хожамуратова С.**

_____ **асс. Сапарова Г.А.**

Зав. кафедрой: _____ **к.т.н. Арзымбетов Т.З.**

Хожамуратова С. «Ўзбектелеком» АК Қорақалпоғистон филиали RC бўлими бошлиғи

НУКУС - 2014 г.

Содержание

ВВЕДЕНИЕ

Internet - глобальная компьютерная сеть, охватывающая весь мир. Сегодня Internet имеет около 15 миллионов абонентов в более чем 150 странах мира. Ежемесячно размер сети увеличивается на 7-10%. Internet образует как бы ядро, обеспечивающее связь различных информационных сетей, принадлежащих различным учреждениям во всем мире, одна с другой.

Если ранее сеть использовалась исключительно в качестве среды передачи файлов и сообщений электронной почты, то сегодня решаются более сложные задачи распределеного доступа к ресурсам. Около двух лет назад были созданы оболочки, поддерживающие функции сетевого поиска и доступа к распределенным информационным ресурсам, электронным архивам.

Internet, служившая когда-то исключительно исследовательским и учебным группам, чьи интересы простирались вплоть до доступа к суперкомпьютерам, становится все более популярной в деловом мире.

Компании соблазняют быстрота, дешевая глобальная связь, удобство для проведения совместных работ, доступные программы, уникальная база данных сети Internet. Они рассматривают глобальную сеть как дополнение к своим собственным локальной сетям.

Фактически Internet состоит из множества локальных и глобальных сетей, принадлежащих различным компаниям и предприятиям, связанных между собой различными линиями связи. Internet можно представить себе в виде мозаики сложенной из небольших сетей разной величины, которые активно взаимодействуют одна с другой, пересылая файлы, сообщения и т.п.

При низкой стоимости услуг (часто это только фиксированная ежемесячная плата за используемые линии или телефон) пользователи могут получить доступ к коммерческим и некоммерческим информационным службам США, Канады, Австралии и многих европейских стран. В архивах свободного доступа сети Internet можно найти информацию практически по всем сферам человеческой деятельности, начиная с новых научных открытий до прогноза погоды на завтра.

Кроме того Internet предоставляет уникальные возможности дешевой, надежной и конфиденциальной глобальной связи по всему миру. Это оказывается очень удобным для фирм имеющих свои филиалы по всему миру, транснациональных корпораций и структур управления. Обычно, использование инфраструктуры Internet для международной связи обходится значительно дешевле прямой компьютерной связи через спутниковый канал или через телефон.

Электронная почта - самая распространенная услуга сети Internet. В настоящее время свой адрес по электронной почте имеют приблизительно 20 миллионов человек. Посылка письма по электронной почте обходится значительно дешевле посылки обычного письма. Кроме того сообщение, посланное по электронной почте дойдет до адресата за несколько часов, в то время как обычное письмо может добираться до адресата несколько дней, а то и недель.

В настоящее время Internet испытывает период подъема, во многом благодаря активной поддержке со стороны правительств европейских стран и США. Ежегодно в США выделяется около 1-2 миллионов долларов на создание новой сетевой инфраструктуры. Исследования в области сетевых коммуникаций финансируются также правительствами Великобритании, Швеции, Финляндии, Германии.

Однако, государственное финансирование - лишь небольшая часть поступающих средств, т.к. все более заметной становится "коммерцизация" сети (80-90% средств поступает из частного сектора).

1. ОБЩАЯ ХАРАКТЕРИСТИКА СЕТИ INTERNET

1.1. История сети Internet

В 1961 году Defence Advanced Research Agensy (DARPA) по заданию министерства обороны США приступило к проекту по созданию экспериментальной сети передачи пакетов. Эта сеть, названная ARPANET, предназначалась первоначально для изучения методов обеспечения надежной связи между компьютерами различных типов. Многие методы передачи данных через модемы были разработаны в ARPANET. Тогда же были разработаны и протоколы передачи данных в сети - TCP/IP. TCP/IP - это множество коммуникационных протоколов, которые определяют, как компьютеры различных типов могут общаться между собой.

Эксперимент с ARPANET был настолько успешен, что многие организации захотели войти в нее, с целью использования для ежедневной передачи данных. И в 1975 году ARPANET превратилась из экспериментальной сети в рабочую сеть. Ответственность за администрирование сети взяло на себя Defence Communication Agency (DCA), в настоящее время называемое Defence Information Systems Agency (DISA). Но развитие ARPANET на этом не остановилось; Протоколы TCP/IP продолжали развиваться и совершенствоваться.

В 1983 году вышел первый стандарт для протоколов TCP/IP, вошедший в Military Standarts (MIL STD), т.е. в военные стандарты, и все, кто работал в сети, обязаны были перейти к этим новым протоколам. Для облегчения этого перехода DARPA обратилась с предложением к руководителям фирмы Berkley Software Design - внедрить протоколы TCP/IP в Berkeley(BSD) UNIX. С этого и начался союз UNIX и TCP/IP.
Спустя некоторое время TCP/IP был адаптирован в обычный, то есть в общедоступный стандарт, и термин Internet вошел во всеобщее употребление. В 1983 году из ARPANET выделилась MILNET, которая стала относиться к Defence Data Network (DDN) министерства обороны США. Термин Internet стал использоваться для обозначения единой сети: MILNET плюс ARPANET. И хотя в 1991 году ARPANET прекратила свое существование, сеть Internet существует, ее размеры намного превышают первоначальные, так как она объединила множество сетей во всем мире. Диаграмма 1.1 иллюстрирует рост числа хостов, подключенных к сети Internet с 4 компьютеров в 1969 году до 8,3 миллионов в 1994. Хостом в сети Internet называются компьютеры, работающие в многозадачной операционной системе (Unix, VMS), поддерживающие протоколы TCP\IP и предоставляющие пользователям какие-либо сетевые услуги.

Диаграмма 1.1

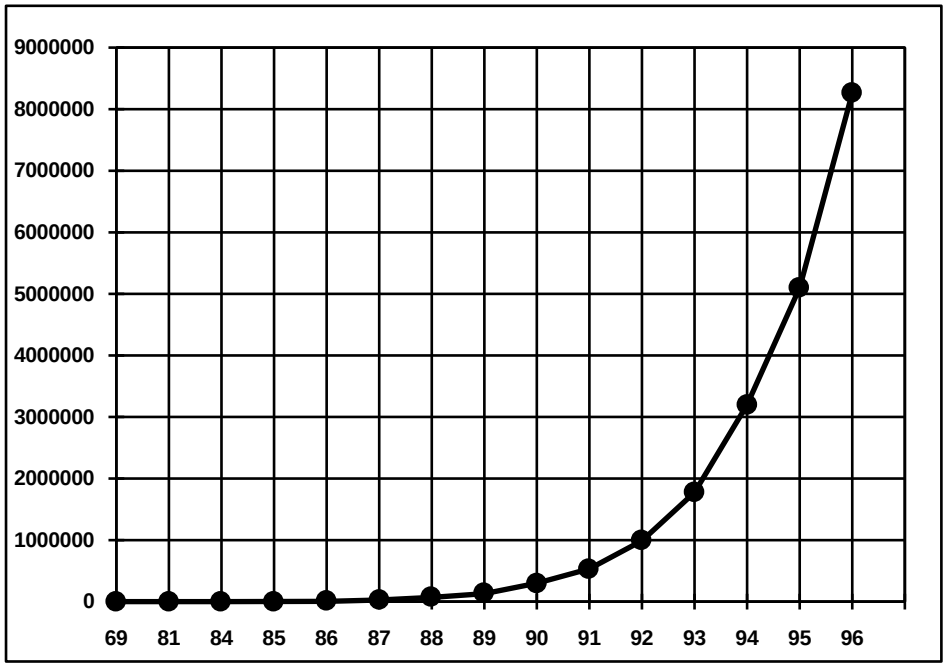

Диаграмма 1.1. Количество хостов, подключенных к Internet .

Протоколы сети Internet

Основное, что отличает Internet от других сетей - это ее протоколы - TCP/IP. Вообще, термин TCP/IP обычно означает все, что связано с протоколами взаимодействия между компьютерами в Internet. Он охватывает целое семейство протоколов, прикладные программы, и даже саму сеть. TCP/IP - это технология межсетевого взаимодействия, технология internet. Сеть, которая использует технологию internet, называется "internet". Если речь идет о глобальной сети, объединяющей множество сетей с технологией internet, то ее называют Internet.

Свое название протокол TCP/IP получил от двух коммуникационных протоколов (или протоколов связи). Это Transmission Control Protocol (TCP) и Internet Protocol (IP). Несмотря на то, что в сети Internet используется большое число других протоколов, сеть Internet часто называют TCP/IP-сетью, так как эти два протокола, безусловно, являются важнейшими.

Как и во всякой другой сети в Internet существует 7 уровней взаимодействия между компьютерами: физический, логический, сетевой, транспортный, уровень сеансов связи, представительский и прикладной уровень. Соответственно каждому уровню взаимодействия соответствует набор протоколов (т.е. правил взаимодействия).

Протоколы физического уровня определяют вид и характеристики линий связи между компьютерами. В Internet используются практически

все известные в настоящее время способы связи от простого провода (витая пара) до волоконно-оптических линий связи (ВОЛС).

Для каждого типа линий связи разработан соответствующий протокол логического уровня, занимающийся управлением передачей информации по каналу. К протоколам логического уровня для телефонных линий относятся протоколы SLIP (Serial Line Interface Protocol) и PPP (Point to Point Protocol). Для связи по кабелю локальной сети - это пакетные драйверы плат ЛВС.

Протоколы сетевого уровня отвечают за передачу данных между устройствами в разных сетях, то есть занимаются маршрутизацией пакетов в сети. К протоколам сетевого уровня принадлежат IP (Internet Protocol) и ARP (Address Resolution Protocol).

Протоколы транспортного уровня управляют передачей данных из одной программы в другую. К протоколам транспортного уровня принадлежат TCP (Transmission Control Protocol) и UDP (User Datagram Protocol).

Протоколы уровня сеансов связи отвечают за установку, поддержание и уничтожение соответствующих каналов. В Internet этим занимаются уже упомянутые TCP и UDP протоколы, а также протокол UUCP (Unix to Unix Copy Protocol).

Протоколы представительского уровня занимаются обслуживанием прикладных программ. К программам представительского уровня принадлежат программы, запускаемые, к примеру, на Unix-сервере, для предоставления различных услуг абонентам. К таким программам относятся: telnet-сервер, FTP-сервер, Gopher-сервер, NFS-сервер, NNTP (Net News Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP2 и POP3 (Post Office Protocol) и т.д.

К протоколам прикладного уровня относятся сетевые услуги и программы их предоставления.

1.2. Услуги, предоставляемые сетью

Все услуги предоставляемые сетью Internet можно условно поделить на две категории: обмен информацией между абонентами сети и использование баз данных сети.

К числу услуг связи между абонентами принадлежат.

Telnet - удаленный доступ. Дает возможность абоненту работать на любой ПК сети Internet как на своей собственной. То есть запускать программы, менять режим работы и т.д.

FTP (File Transfer Protocol) - протокол передачи файлов. Дает возможность абоненту обмениваться двоичными и текстовыми файлами с любым компьютером сети. Установив связь с удаленным компьютером,

пользователь может скопировать файл с удаленного компьютера на свой или скопировать файл со своего компьютера на удаленный.

NFS (Network File System) - распределенная файловая система. Дает возможность абоненту пользоваться файловой системой удаленного компьютера, как своей собственной.

Электронная почта - обмен почтовыми сообщениями с любым абонентом сети Internet. Существует возможность отправки как текстовых, так и двоичных файлов. На размер почтового сообщения в сети Internet накладывается следующее ограничение - размер почтового сообщения не должен превышать 64 килобайт.

Новости - получение сетевых новостей и электронных досок объявлений сети и возможность помещения информации на доски объявлений сети. Электронные доски объявлений сети Internet формируются по тематике. Пользователь может по своему выбору подписаться на любые группы новостей.

Rsh (Remote Shell) - удаленный доступ. Аналог Telnet, но работает только в том случае, если на удаленном компьютере стоит ОС UNIX.

Rexec (Remote Execution) - выполнение одной команды на удаленной UNIX-машине.

Lpr - сетевая печать. Отправка файла на печать на удаленном (сетевом) принтере.

Lpq - сетевая печать. Показывает файлы стоящие в очереди на печать на сетевом принтере.

Ping - проверка доступности удаленной ПК по сети.

Talk - дает возможность открытия "разговора" с пользователем удаленной ПК. При этом на экране одновременно виден вводимый текст и ответ удаленного пользователя.

Iptunnel - дает возможность доступа к серверу ЛВС NetWare с которым нет непосредственной связи по ЛВС, а имеется лишь связь по сети Internet.

Whois - адресная книга сети Internet. По запросу абонент может получить информацию о принадлежности удаленного компьютера, о пользователях.

Finger - получение информации о пользователях удаленного компьютера.

Кроме вышеперечисленных услуг, сеть Internet предоставляет также следующие специфические услуги.

Webster - сетевая версия толкового словаря английского языка.

Факс-сервис - дает возможность пользователю отправлять сообщения по факсимильной связи, пользуясь, факс - сервером сети.

Электронный переводчик - производит перевод присланного на него текста с одного языка на другой. Обращение к электронным переводчикам происходит посредством электронной почты.

Шлюзы - дают возможность абоненту отправлять сообщения в сети, не работающие с протоколами TCP\IP (FidoNet, Goldnet, AT50).

К системам автоматизированного поиска информации в сети Internet принадлежат следующие системы.

Gopher - наиболее широко распространенное средство поиска информации в сети Internet, позволяющее находить информацию по ключевым словам и фразам. Работа с системой Gopher напоминает просмотр оглавления, при этом пользователю предлагается пройти сквозь ряд вложенных меню и выбрать нужную тему. В Internet в настоящее время свыше 2000 Gopher-систем, часть из которых является узкоспециализированной, а часть содержит более разностороннюю информацию.

Gopher позволяет получить информацию без указания имен и адресов авторов, благодаря чему пользователь не тратит много времени и нервов. Он просто сообщит системе Gopher, что именно ему нужно, и система находит соответствующие данные. Gopher-серверов свыше двух тысяч, поэтому с их помощью не всегда просто найти требуемую информацию. В случае возникших затруднений можно воспользоваться службой VERONICA. VERONICA осуществляет поиск более чем в 500 системах Gopher, освобождая пользователя от необходимости просматривать их вручную.

WAIS - еще более мощное средство получения информации, чем Gopher, поскольку оно осуществляет поиск ключевых слов во всех текстах документов. Запросы посылаются в WAIS на упрощенном английском языке. Это значительно легче, чем формулировать их на языке алгебры логики, и это делает WAIS более привлекательной для пользователей-непрофессионалов.

При работе с WAIS пользователям не нужно тратить много времени, чтобы найти необходимые им материалы.

В сети Internet существует более 200 WAIS - библиотек. Но поскольку информация представляется преимущественно сотрудниками академических организаций на добровольных началах, большая часть материалов относится к области исследований и компьютерных наук.

WWW - система для работы с гипертекстом. Потенциально она является наиболее мощным средством поиска. Гипертекст соединяет различные документы на основе заранее заданного набора слов. Например, когда в тексте встречается новое слово или понятие, система, работающая с гипертекстом, дает возможность перейти к другому

документу, в котором это слово или понятие рассматривается более подробно.

WWW часто используется в качестве интерфейса к базам данных WAIS, но отсутствие гипертекстовых связей ограничивает возможности WWW до простого просмотра.

Пользователь со своей стороны может задействовать возможность WWW работать с гипертекстом для связи между своими данными и данными WAIS и WWW таким образом, чтобы собственные записи пользователя как бы интегрировались в информацию для общего доступа. На самом деле этого, конечно, не происходит, но воспринимается именно так.

WWW - это относительно новая система. Установлены несколько демонстрационных серверов, в том числе Vatican Exibit в библиотеке Конгресса США и мультфильм о погоде "Витки спутника" в Мичиганском государственном университете. В качестве демонстрации также работают серверы into.funet.fi (Финляндия); into.cern.ch. (Швейцария) и eies2.njit.edu (США).

Практически все услуги сети построены на принципе клиент-сервер. Сервером в сети Internet называется компьютер способный предоставлять клиентам (по мере прихода от них запросов) некоторые сетевые услуги. Взаимодействие клиент-сервер строится обычно следующим образом. По приходу запросов от клиентов сервер запускает различные программы предоставления сетевых услуг. По мере выполнения запущенных программ сервер отвечает на запросы клиентов.

Все программное обеспечение сети также можно поделить на клиентское и серверное. При этом программное обеспечение сервера занимается предоставлением сетевых услуг, а клиентское программное обеспечение обеспечивает передачу запросов серверу и получение ответов от него.

1.3. Гипертекстовая технология WWW, URL, HTML

World Wide Web переводится на русский язык как “Всемирная Паутина”. И, в сущности, это действительно так. WWW является одним из самых совершенных инструментов для работы в глобальной мировой сети Internet. Эта служба появилась сравнительно недавно и все еще продолжает бурно развиваться.

Наибольшее количество разработок имеют отношение к родине WWW - CERN, European Particle Physics Laboratory; но было бы ошибкой считать, что Web является инструментом, разработанным физиками и для физиков. Плодотворность и привлекательность идей, положенных в основу проекта, превратили WWW в систему мирового масштаба,

предоставляющую информацию едва ли не во всех областях человеческой деятельности и охватывающую примерно 30 млн. пользователей в 83 странах мира.

Главное отличие WWW от остальных инструментов для работы с Internet заключается в том, что WWW позволяет работать практически со всеми доступными сейчас на компьютере видами документов: это могут быть текстовые файлы, иллюстрации, звуковые и видео ролики, и т.д.

Что такое WWW? Это попытка организовать всю информацию в Internet, плюс любую локальную информацию по вашему выбору, как набор гипертекстовых документов. Вы перемещаетесь по сети, переходя от одного документа к другому по ссылкам. Все эти документы написаны на специально разработанном для этого языке, который называется HyperText Markup Language (HTML). Он чем-то напоминает язык, использующийся для написания текстовых документов, только HTML проще. Причем, можно использовать не только информацию, предоставляемую Internet, но и создавать собственные документы. В последнем случае существует ряд практических рекомендаций к их написанию.

Вся польза гипертекста состоит в создании гипертекстовых документов, если вас заинтересовал какой либо пункт в таком документе, то вам достаточно ткнуть туда курсором для получения нужной информации. Также в одном документе, возможно, делать ссылки на другие, написанные другими авторами или даже расположенные на другом сервере. В то время как вам это представляется как одно целое.

Гипермедиа это надмножество гипертекста. В гипермедиа производятся операции не только над текстом, но и над звуком, изображениями, анимацией.

Существуют WWW-серверы для Unix, Macintosh, MS Windows и VMS, большинство из них распространяются свободно. Установив WWW-сервер, вы можете решить две задачи:

1. Предоставить информацию внешним потребителям - сведения о вашей фирме, каталоги продуктов и услуг, техническую или научную информацию.

2. Предоставить своим сотрудникам удобный доступ к внутренним информационным ресурсам организации. Это могут быть последние распоряжения руководства, внутренний телефонный справочник, ответы на часто задаваемые вопросы для пользователей прикладных систем, техническая документация и все, что подскажет фантазия администратора и пользователей. Информация, которую вы хотите предоставить пользователям WWW, оформляется в виде файлов на языке HTML.

HTML - простой язык разметки, который позволяет помечать фрагменты текста и задавать ссылки на другие документы, выделять

заголовки нескольких уровней, разбивать текст на абзацы, центрировать их и т. п., превращая простой текст в отформатированный гипермедийный документ. Достаточно легко создать html-файл вручную, однако, имеются специализированные редакторы и преобразователи файлов из других форматов.

Для просмотра документов используются специальные просмоторщики, такие как Mosaic, Netscape, Internet Explorer, lynx, www и другие. Mosaic и Netscape удобно использовать на графических терминалах. Для работы на символьных терминалах можно порекомендовать lynx.

Архитектура WWW-технологии

От описания основных компонентов перейдем к архитектуре взаимодействия программного обеспечения в системе World Wide Web. WWW построена по хорошо известной схеме “клиент-сервер”. На схеме 1.2 показано, как разделены функции в этой схеме. Программа-клиент выполняет функции интерфейса пользователя и обеспечивает доступ практически ко всем информационным ресурсам Internet. В этом смысле она выходит за обычные рамки работы клиента только с сервером определенного протокола, как это происходит в telnet, например. Отчасти, довольно широко распространенное мнение, что Mosaic или Netscape, которые являются WWW-клиентами, это просто графический интерфейс в Internet, является отчасти верным. Однако, как уже было отмечено, базовые компоненты WWW-технологии (HTML и URL) играют при доступе к другим ресурсам Mosaic не последнюю роль, и поэтому мультипротокольные клиенты должны быть отнесены именно к World Wide Web, а не к другим информационным технологиям Internet. Фактически, клиент—это интерпретатор HTML. И как типичный интерпретатор, клиент в зависимости от команд (разметки) выполняет различные функции.

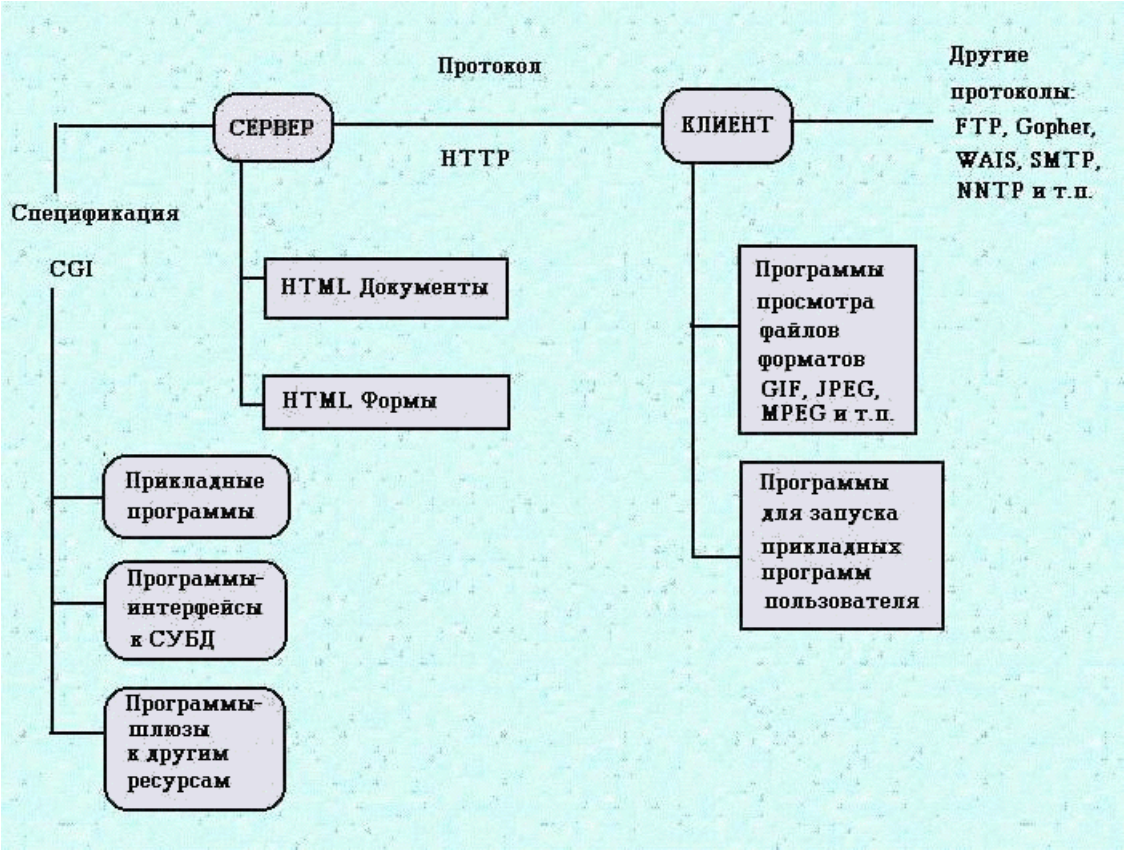

Схема 1.2. Структура ”клиент - сервер”.

В круг этих функций входит не только размещение текста на экране, но обмен информацией с сервером по мере анализа полученного HTML-текста, что наиболее наглядно происходит при отображении встроенных в текст, графических образов. При анализе URL-спецификации или по командам сервера клиент запускает дополнительные внешние программы для работы с документами в форматах, отличных от HTML, например GIF, JPEG, MPEG, Postscript. Для запуска клиентом программ независимо от типа документа была разработана программа Luncher, но в последнее время гораздо большее распространение получил механизм согласования запускаемых программ через MIME-типы. Другую часть программного комплекса WWW составляет сервер протокола HTTP, базы данных документов в формате HTML, управляемые сервером, и программное обеспечение, разработанное в стандарте спецификации CGI. До самого последнего времени (до образования Netscape) реально использовалось два HTTP-сервера: сервер CERN и сервер NCSA. Но в настоящее время число базовых серверов расширилось. Появился очень неплохой сервер для MS-Windows и Apachie-сервер для Unix-платформ. Существуют и другие, но два последних можно выделить из соображений доступности использования. Сервер для Windows - это shareware, но без встроенного самоликвидатора, как в Netscape. Учитывая распространенность

персоналок в нашей стране, такое программное обеспечение дает возможность попробовать, что такое WWW. Второй сервер - это ответ на угрозу коммерциализации. Netscape уже не распространяет свой сервер Netsite свободно и прошел слух, что NCSA-сервер также будет распространяться на коммерческой основе. В результате был разработан Apachie, который по словам его авторов будет freeware, и реализует новые дополнения к протоколу HTTP, связанные с защитой от несанкционированного доступа, которые предложены группой по разработке этого протокола и реализуются практически во всех коммерческих серверах.

База данных HTML-документов – это часть файловой системы, которая содержит текстовые файлы в формате HTML и связанные с ними графику и другие ресурсы. Особое внимание хотелось бы обратить на документы, содержащие элементы экранных форм. Эти документы реально обеспечивают доступ к внешнему программному обеспечению.

Прикладное программное обеспечение, работающее с сервером, можно разделить на программы-шлюзы и прочие. Шлюзы—это программы, обеспечивающие взаимодействие сервера с серверами других протоколов, например ftp, или с распределенными на сети серверами Oracle. Прочие программы – это программы, принимающие данные от сервера и выполняющие какие - либо действия: получение текущей даты, реализацию графических ссылок, доступ к локальным базам данных или просто расчеты.

Завершая обсуждение архитектуры World Wide Web хотелось бы еще раз подчеркнуть, что ее компоненты существуют практически для всех типов компьютерных платформ и свободно доступны в сети. Любой, кто имеет доступ в Internet, может создать свой WWW-сервер, или, по крайней мере, посмотреть информацию с других серверов.

Основные компоненты технологии World Wide Web

К 1989 году гипертекст, представлял новую, многообещающую технологию, которая имела относительно большое число реализаций с одной стороны, а с другой стороны делались попытки построить формальные модели гипертекстовых систем, которые носили скорее описательный характер и были навеяны успехом реляционного подхода описания данных. Идея Т. Бернерс-Ли заключалась в том, чтобы применить гипертекстовую модель к информационным ресурсам, распределенным в сети, и сделать это максимально простым способом. Он заложил три краеугольных камня системы из четырех существующих ныне, разработав:

язык гипертекстовой разметки документов HTML (HyperText Markup Language);
- универсальный способ адресации ресурсов в сети URL (Universal Resource Locator);
- протокол обмена гипертекстовой информацией HTTP (HyperText Transfer Protocol).
Позже команда NCSA добавила к этим трем компонентам четвертый:
- универсальный интерфейс шлюзов CGI (Common Gateway Interface).

Идея HTML—пример чрезвычайно удачного решения проблемы построения гипертекстовой системы при помощи специального средства управления отображением. На разработку языка гипертекстовой разметки существенное влияние оказали два фактора: исследования в области интерфейсов гипертекстовых систем и желание обеспечить простой и быстрый способ создания гипертекстовой базы данных, распределенной на сети.

В 1989 году активно обсуждалась проблема интерфейса гипертекстовых систем, т.е. способов отображения гипертекстовой информации и навигации в гипертекстовой сети. Значение гипертекстовой технологии сравнивали со значением книгопечатания. Утверждалось, что лист бумаги и компьютерные средства отображения/воспроизведения серьезно отличаются друг от друга, и поэтому форма представления информации тоже должна отличаться. Наиболее эффективной формой организации гипертекста были признаны контекстные гипертекстовые ссылки, а кроме того было признано деление на ссылки, ассоциированные со всем документом в целом и отдельными его частями.

Самым простым способом создания любого документа является его набивка в текстовом редакторе. Опыт создания хорошо размеченных для последующего отображения документов в CERN_е был - трудно найти физика, который не пользовался бы системой TeX или LaTeX. Кроме того к тому времени существовал стандарт языка разметки—Standard Generalised Markup Language (SGML).

Следует также принять во внимание, что согласно своим предложениям Бернерс-Ли предполагал объединить в единую систему имеющиеся информационные ресурсы CERN, и первыми демонстрационными системами должны были стать системы для NeXT и VAX/VMS.

Обычно гипертекстовые системы имеют специальные программные средства построения гипертекстовых связей. Сами гипертекстовые ссылки хранятся в специальных форматах или даже составляют специальные файлы. Такой подход хорош для локальной системы, но не для распределенной на множестве различных компьютерных платформ. В HTML гипертекстовые ссылки встроены в тело документа и хранятся как

его часть. Часто в системах применяют специальные форматы хранения данных для повышения эффективности доступа. В WWW документы - это обычные ASCII- файлы, которые можно подготовить в любом текстовом редакторе. Таким образом, проблема создания гипертекстовой базы данных была решена чрезвычайно просто.

В качестве базы для разработки языка гипертекстовой разметки был выбран SGML (Standard Generalised Markup Language). Следуя академическим традициям, Бернерс-Ли описал HTML в терминах SGML (как описывают язык программирования в терминах формы Бекуса-Наура). Естественно, что в HTML были реализованы все разметки, связанные с выделением параграфов, шрифтов, стилей и т. п., т.к. реализация для NeXT подразумевала графический интерфейс. Важным компонентом языка стало описание встроенных и ассоциированных гипертекстовых ссылок, встроенной графики и обеспечение возможности поиска по ключевым словам.

С момента разработки первой версии языка (HTML 1.0) прошло уже пять лет. За это время произошло довольно серьезное развитие языка. Почти вдвое увеличилось число элементов разметки, оформление документов все больше приближается к оформлению качественных печатных изданий, развиваются средства описания не текстовых информационных ресурсов и способы взаимодействия с прикладным программным обеспечением. Совершенствуется механизм разработки типовых стилей. Фактически, в настоящее время HTML развивается в сторону создания стандартного языка разработки интерфейсов как локальных, так и распределенных систем.

Вторым краеугольным камнем WWW стала универсальная форма адресации информационных ресурсов. Universal Resource Identification (URI) представляет собой довольно стройную систему, учитывающую опыт адресации и идентификации e-mail, Gopher, WAIS, telnet, ftp и т. п. Но реально из всего, что описано в URI, для организации баз данных в WWW требуется только Universal Resource Locator (URL). Без наличия этой спецификации вся мощь HTML оказалась бы бесполезной. URL используется в гипертекстовых ссылках и обеспечивает доступ к распределенным ресурсам сети. В URL можно адресовать как другие гипертекстовые документы формата HTML, так и ресурсы e-mail, telnet, ftp, Gopher, WAIS, например. Различные интерфейсные программы по разному осуществляют доступ к этим ресурсам. Одни, как например Netscape, сами способны поддерживать взаимодействие по протоколам, отличным от протокола HTTP, базового для WWW, другие, как например Chimera, вызывают для этой цели внешние программы. Однако, даже в первом случае, базовой формой представления отображаемой информации является HTML, а ссылки на другие ресурсы имеют форму

URL. Следует отметить, что программы обработки электронной почты в формате MIME также имеют возможность отображать документы, представленные в формате HTML. Для этой цели в MIME зарезервирован тип “text/html”.

Третьим в нашем списке стоит протокол обмена данными в World Wide Web -HyperText Transfer Protocol. Данный протокол предназначен для обмена гипертекстовыми документами и учитывает специфику такого обмена. Так в процессе взаимодействия, клиент может получить новый адрес ресурса на сети (relocation), запросить встроенную графику, принять и передать параметры и т. п. Управление в HTTP реализовано в виде ASCII-команд. Реально разработчик гипертекстовой базы данных сталкивается с элементами протокола только при использовании внешних расчетных программ или при доступе к внешним относительно WWW информационным ресурсам, например базам данных.

Последняя составляющая технологии WWW - это уже плод работы группы NCSA - спецификация Common Gateway Interface. CGI была специально разработана для расширения возможностей WWW за счет подключения всевозможного внешнего программного обеспечения. Такой подход логично продолжал принцип публичности и простоты разработки и наращивания возможностей WWW. Если команда CERN предложила простой и быстрый способ разработки баз данных, то NCSA развила этот принцип на разработку программных средств. Надо заметить, что в общедоступной библиотеке CERN были модули, позволяющие программистам подключать свои программы к серверу HTTP, но это требовало использования этой библиотеки. Предложенный и описанный в CGI способ подключения не требовал дополнительных библиотек и буквально ошеломлял своей простотой. Сервер взаимодействовал с программами через стандартные потоки ввода/вывода, что упрощает программирование до предела. При реализации CGI чрезвычайно важное место заняли методы доступа, описанные в HTTP. И хотя реально используются только два из них (GET и POST), опыт развития HTML показывает, что сообщество WWW ждет развития и CGI по мере усложнения задач, в которых будет использоваться WWW-технология.

2. ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ INTERNET

2.1. Проблемы защиты информации

Internet и информационная безопасность несовместимы по самой природе Internet. Она появилась, как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность получить прямой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

Как известно, чем проще доступ в сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в Internet - хуже воровства, так как пользователь может даже и не узнать, что у него были скопированы - файлы и программы, не говоря уже о возможности их порчи и корректировки.

Что же определяет бурный рост Internet, характеризующийся ежегодным удвоением числа пользователей? Ответ прост - дешевизна программного обеспечения (TCP/IP), которое в настоящее время включено в Windows 95, легкость и дешевизна доступа в Internet (либо с помощью IP-адреса, либо с помощью провайдера) и ко всем мировым информационным ресурсам.

Платой за пользование Internet является всеобщее снижение информационной безопасности, поэтому для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию intranet, ставят фильтры (fire-wall) между внутренней сетью и Internet, что фактически означает выход из единого адресного пространства. Еще большую безопасность даст отход от протокола TCP/IP и доступ в Internet через шлюзы.

Этот переход можно осуществлять одновременно с процессом построения всемирной информационной сети общего пользования, на базе использования сетевых компьютеров, которые с помощью сетевой карты 10Base-T и кабельного модема обеспечивают высокоскоростной доступ (10 Мбит/с) к локальному Web-серверу через сеть кабельного телевидения.

Для решения этих и других вопросов при переходе к новой архитектуре Internet нужно предусмотреть следующее:

Во-первых, ликвидировать физическую связь между будущей Internet (которая превратится во Всемирную информационную сеть общего пользования) и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web.

Во-вторых, заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Ethernet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов.

В-третьих, перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети, и позволяющее в рамках 48-бит создать адреса для более чем 64 триллионов независимых узлов.

Безопасность данных является одной из главных проблем в Internet. Появляются все новые и новые страшные истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Internet в деловых кругах. Одна только мысль о том, что какие-нибудь хулиганы или, что еще хуже, конкуренты, смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и частным сетям, практически равные шансы стать жертвами компьютерного террора.

Каждая организация, имеющая дело с какими бы то ни было ценностями, рано или поздно сталкивается с посягательством на них. Предусмотрительные начинают планировать защиту заранее, непредусмотрительные - после первого крупного “прокола”. Так или иначе, встает вопрос о том, что, как и от кого защищать.

Обычно первая реакция на угрозу – стремление спрятать ценности в недоступное место и приставить к ним охрану. Это относительно несложно, если речь идет о таких ценностях, которые вам долго не понадобятся: убрали и забыли. Куда сложнее, если вам необходимо постоянно работать с ними. Каждое обращение в хранилище за вашими ценностями потребует выполнения особой процедуры, отнимет время и создаст дополнительные неудобства. Такова дилемма безопасности: приходится делать выбор между защищенностью вашего имущества и его доступностью для вас, а значит, и возможностью полезного использования.

Все это справедливо и в отношении информации. Например, база данных, содержащая конфиденциальные сведения, лишь тогда полностью защищена от посягательств, когда она находится на дисках, снятых с компьютера и убранных в охраняемое место. Как только вы установили эти диски в компьютер и начали использовать, появляется сразу несколько каналов, по которым злоумышленник, в принципе, имеет возможность получить к вашим тайнам доступ без вашего ведома. Иными словами, ваша информация либо недоступна для всех, включая и вас, либо не защищена.

Может показаться, что из этой ситуации нет выхода, но информационная безопасность сродни безопасности мореплавания: и то, и другое возможно лишь с учетом некоторой допустимой степени риска.

В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

В банковской сфере проблема безопасности информации осложняется двумя факторами: во-первых, почти все ценности, с которыми имеет дело банк (кроме наличных денег и еще кое-чего), существуют лишь в виде той или иной информации. Во-вторых, банк не может существовать без связей с внешним миром: без клиентов, корреспондентов и т. п. При этом по внешним связям обязательно передается та самая информация, выражающая собой ценности, с которыми работает банк (либо сведения об этих ценностях и их движении, которые иногда стоят дороже самих ценностей). Извне приходят документы, по которым банк переводит деньги с одного счета на другой. Вовне банк передает распоряжения о движении средств по корреспондентским счетам, так что открытость банка задана a priori.

Стоит отметить, что эти соображения справедливы по отношению не только к автоматизированным системам, но и к системам, построенным на традиционном бумажном документообороте и не использующим иных связей, кроме курьерской почты. Автоматизация добавила головной боли службам безопасности, а новые тенденции развития сферы банковских услуг, целиком основанные на информационных технологиях, усугубляют проблему.

2.1.1. Информационная безопасность и информационные технологии

На раннем этапе автоматизации внедрение банковских систем (и вообще средств автоматизации банковской деятельности) не повышало открытость банка. Общение с внешним миром, как и прежде, шло через операционистов и курьеров, поэтому дополнительная угроза безопасности информации проистекала лишь от возможных злоупотреблений со стороны работавших в самом банке специалистов по информационным технологиям.

Положение изменилось после того, как на рынке финансовых услуг стали появляться продукты, само возникновение которых было немыслимо без информационных технологий. В первую очередь это - пластиковые карточки. Пока обслуживание по карточкам шло в режиме голосовой авторизации, открытость информационной системы банка повышалась незначительно, но затем появились банкоматы, POS-терминалы, другие устройства самообслуживания—то есть средства, принадлежащие к информационной системе банка, но расположенные вне ее и доступные посторонним для банка лицам.

Повысившаяся открытость системы потребовала специальных мер для контроля и регулирования обмена информацией: дополнительных средств идентификации и аутентификации лиц, которые запрашивают доступ к системе (PIN-код, информация о клиенте на магнитной полосе или в памяти микросхемы карточки, шифрование данных, контрольные числа и другие средства защиты карточек), средств криптозащиты информации в каналах связи и т. д.

Еще больший сдвиг баланса “защищенность-открытость” в сторону последней связан с телекоммуникациями. Системы электронных расчетов между банками защитить относительно несложно, так как субъектами электронного обмена информацией выступают сами банки. Тем не менее, там, где защите не уделялось необходимое внимание, результаты были вполне предсказуемы. Наиболее кричащий пример – к сожалению, наша страна. Использование крайне примитивных средств защиты телекоммуникаций в 1992 г. привело к огромным потерям на фальшивых авизо.

Общая тенденция развития телекоммуникаций и массового распространения вычислительной техники привела в конце концов к тому, что на рынке банковских услуг во всем мире появились новые, чисто телекоммуникационные продукты, и в первую очередь системы Home Banking (отечественный аналог - “клиент-банк”). Это потребовало обеспечить клиентам круглосуточный доступ к автоматизированной банковской системе для проведения операций, причем полномочия на совершение банковских транзакций получил непосредственно клиент.

Степень открытости информационной системы банка возросла почти до предела. Соответственно, требуются особые, специальные меры для того, чтобы столь же значительно не упала ее защищенность.

Наконец, грянула эпоха “информационной супермагистрали”: взрывообразное развитие сети Internet и связанных с нею услуг. Вместе с новыми возможностями эта сеть принесла и новые опасности. Казалось бы, какая разница, каким образом клиент связывается с банком: по коммутируемой линии, приходящей на модемный пул банковского узла связи, или по IP-протоколу через Internet? Однако в первом случае максимально возможное количество подключений ограничивается техническими характеристиками модемного пула, во втором же - возможностями Internet, которые могут быть существенно выше. Кроме того, сетевой адрес банка, в принципе, общедоступен, тогда как телефонные номера модемного пула могут сообщаться лишь заинтересованным лицам. Соответственно, открытость банка, чья информационная система связана с Internet, значительно выше, чем в первом случае. Так только за пять месяцев 1995 г. компьютерную сеть Citicorp взламывали 40 раз! (Это свидетельствует, впрочем, не столько о какой-то “опасности” Internet вообще, сколько о недостаточно квалифицированной работе администраторов безопасности Citicorp.)

Все это вызывает необходимость пересмотра подходов к обеспечению информационной безопасности банка. Подключаясь к Internet, следует заново провести анализ риска и составить план защиты информационной системы, а также конкретный план ликвидации последствий, возникающих в случае тех или иных нарушений конфиденциальности, сохранности и доступности информации.

На первый взгляд, для нашей страны проблема информационной безопасности банка не столь остра: до Internet ли нам, если в большинстве банков стоят системы второго поколения, работающие в технологии “файл-сервер”. К сожалению, и у нас уже зарегистрированы “компьютерные кражи”. Положение осложняется двумя проблемами. Прежде всего, как показывает опыт общения с представителями банковских служб безопасности, и в руководстве, и среди персонала этих служб преобладают бывшие оперативные сотрудники органов внутренних дел или госбезопасности. Они обладают высокой квалификацией в своей области, но в большинстве своем слабо знакомы с информационными технологиями. Специалистов по информационной безопасности в нашей стране вообще крайне мало, потому что массовой эта профессия становится только сейчас.

Вторая проблема связана с тем, что в очень многих банках безопасность автоматизированной банковской системы не анализируется и не обеспечивается всерьез. Очень мало где имеется тот необходимый

набор организационных документов (анализ риска, план защиты и план ликвидации последствий), о котором говорилось выше. Более того, безопасность информации сплошь и рядом просто не может быть обеспечена в рамках имеющейся в банке автоматизированной системы и принятых правил работы с ней.

Не так давно мне довелось читать лекцию об основах информационной безопасности на одном из семинаров для руководителей управлений автоматизации коммерческих банков. На вопрос: “Знаете ли вы, сколько человек имеют право входить в помещение, где находится сервер базы данных Вашего банка?”, утвердительно ответило не более 40% присутствующих. Пофамильно назвать тех, кто имеет такое право, смогли лишь 20%. В остальных банках доступ в это помещение не ограничен и никак не контролируется. Что говорить о доступе к рабочим станциям!

Что касается автоматизированных банковских систем, то наиболее распространенные системы второго-третьего поколений состоят из набора автономных программных модулей, запускаемых из командной строки DOS на рабочих станциях. Оператор имеет возможность в любой момент выйти в DOS из такого программного модуля. Предполагается, что это необходимо для перехода в другой программный модуль, но фактически в такой системе не существует никаких способов не только исключить запуск оператором любых других программ (от безобидной игры до программы, модифицирующей данные банковских счетов), но и проконтролировать действия оператора. Стоит заметить, что в ряде систем этих поколений, в том числе разработанных весьма уважаемыми отечественными фирмами и продаваемых сотнями, файлы счетов не шифруются, т. е. с данными в них можно ознакомиться простейшими общедоступными средствами. Многие разработчики ограничивают средства администрирования безопасности штатными средствами сетевой операционной системы: вошел в сеть -- делай, что хочешь.

Положение меняется, но слишком медленно. Даже во многих новых разработках вопросам безопасности уделяется явно недостаточное внимание. На выставке “Банк и Офис – 95” была представлена автоматизированная банковская система с архитектурой клиент—сервер, причем рабочие станции функционируют под Windows. В этой системе очень своеобразно решен вход оператора в программу: в диалоговом окне запрашивается пароль, а затем предъявляется на выбор список фамилий всех операторов, имеющих право работать с данным модулем! Таких примеров можно привести еще много.

Тем не менее, наши банки уделяют информационным технологиям много внимания, и достаточно быстро усваивают новое. Сеть Internet и финансовые продукты, связанные с ней, войдут в жизнь банков России

быстрее, чем это предполагают скептики, поэтому уже сейчас необходимо озаботиться вопросами информационной безопасности на другом, более профессиональном уровне, чем это делалось до сих пор.

Некоторые рекомендации:

1. Необходим комплексный подход к информационной безопасности.

Информационная безопасность должна рассматриваться как составная часть общей безопасности банка - причем как важная и неотъемлемая ее часть. Разработка концепции информационной безопасности должна обязательно проходить при участии управления безопасности банка. В этой концепции следует предусматривать не только меры, связанные с информационными технологиями (криптозащиту, программные средства администрирования прав пользователей, их идентификации и аутентификации, “брандмауэры” для защиты входов—выходов сети и т. п.), но и меры административного и технического характера, включая жесткие процедуры контроля физического доступа к автоматизированной банковской системе, а также средства синхронизации и обмена данными между модулем администрирования безопасности банковской системы и системой охраны.

2. Необходимо участие сотрудников управления безопасности на этапе выбора – приобретения – разработки автоматизированной банковской системы. Это участие не должно сводиться к проверке фирмы-поставщика. Управление безопасности должно контролировать наличие надлежащих средств разграничения доступа к информации в приобретаемой системе.

К сожалению, ныне действующие системы сертификации в области банковских систем скорее вводят в заблуждение, чем помогают выбрать средства защиты информации. Сертифицировать использование таких средств имеет право ФАПСИ, однако правом своим этот орган пользуется весьма своеобразно. Так, один высокопоставленный сотрудник ЦБ РФ (попросивший не называть его имени) рассказал, что ЦБ потратил довольно много времени и денег на получение сертификата на одно из средств криптозащиты информации (кстати, разработанное одной из организаций, входящих в ФАПСИ). Почти сразу же после получения сертификата он был отозван: ЦБ было предложено вновь пройти сертификацию уже с новым средством криптозащиты—разработанным той же организацией из ФАПСИ.

Возникает вопрос, а что же на самом деле подтверждает сертификат? Если, как предполагает наивный пользователь, он подтверждает пригодность средства криптозащиты выполнению этой функции, то отзыв

сертификата говорит о том, что при первоначальном сертифицировании ФАПСИ что-то упустило, а затем обнаружило дефект. Следовательно, данный продукт не обеспечивает криптозащиты и не обеспечивал ее с самого начала.

Если же, как предполагают пользователи более искушенные, ФАПСИ отозвало сертификат не из-за огрехов в первом продукте, то значение сертификации этим агентством чего бы то ни было сводится к нулю. Действительно, раз “некие” коммерческие соображения преобладают над объективной оценкой продукта, то кто может гарантировать, что в первый раз сертификат был выдан благодаря высокому качеству продукта, а не по тем же “неким” соображениям?

Отсюда следует третья практическая рекомендация: относиться сугубо осторожно к любым сертификатам и отдавать предпочтение тем продуктам, надежность которых подтверждена успешным использованием в мировой финансовой практике. Безопасность в сети Internet

2.2. Средства защиты информации

Сейчас вряд ли кому-то надо доказывать, что при подключении к Internet Вы подвергаете риску безопасность Вашей локальной сети и конфиденциальность содержащейся в ней информации. По данным CERT Coordination Center в 1995 году было зарегистрировано 2421 инцидентов - взломов локальных сетей и серверов. По результатам опроса, проведенного Computer Security Institute (CSI) среди 500 наиболее крупных организаций, компаний и университетов с 1991 число незаконных вторжений возросло на 48.9 %, а потери, вызванные этими атаками, оцениваются в 66 млн. долларов США.

Одним из наиболее распространенных механизмов защиты от интернетовских бандитов - “хакеров” является применение межсетевых экранов - **брэндмауэров (firewalls).**

Стоит отметить, что в следствии непрофессионализма администраторов и недостатков некоторых типов брэндмауэров порядка 30% взломов совершается после установки защитных систем.

Не следует думать, что все изложенное выше - “заморские диковины”. Всем, кто еще не уверен, что Россия уверенно догоняет другие страны по числу взломов серверов и локальных сетей и принесенному ими ущербу, следует познакомиться с тематической подборкой материалов российской прессы и материалами Hack Zone (Zhurnal.Ru).

Не смотря на кажущийся правовой хаос в расматриваемой области, любая деятельность по разработке, продаже и использованию средств защиты информации регулируется множеством законодательных и

нормативных документов, а все используемые системы подлежат обязательной сертификации Государственой Технической Комисией при президенте России.

2.2.1. Технология работы в глобальных сетях Solstice FireWall-1

В настоящее время вопросам безопасности данных в распределенных компьютерных системах уделяется очень большое внимание. Разработано множество средств для обеспечения информационной безопасности, предназначенных для использования на различных компьютерах с разными ОС. В качестве одного из направлений можно выделить межсетевые экраны (firewalls), призванные контролировать доступ к информации со стороны пользователей внешних сетей.

В настоящем документе рассматриваются основные понятия экранирующих систем, а также требования, предъявляемые к ним. На примере пакета Solstice FireWall-1 рассматривается несколько типичных случаев использования таких систем, особенно применительно к вопросам обеспечения безопасности Internet-подключений. Рассмотрено также несколько уникальных особенностей Solstice FireWall-1, позволяющих говорить о его лидерстве в данном классе приложений.

Назначение экранирующих систем и требования к ним

Проблема межсетевого экранирования формулируется следующим образом. Пусть имеется две информационные системы или два множества информационных систем. Экран (firewall) - это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

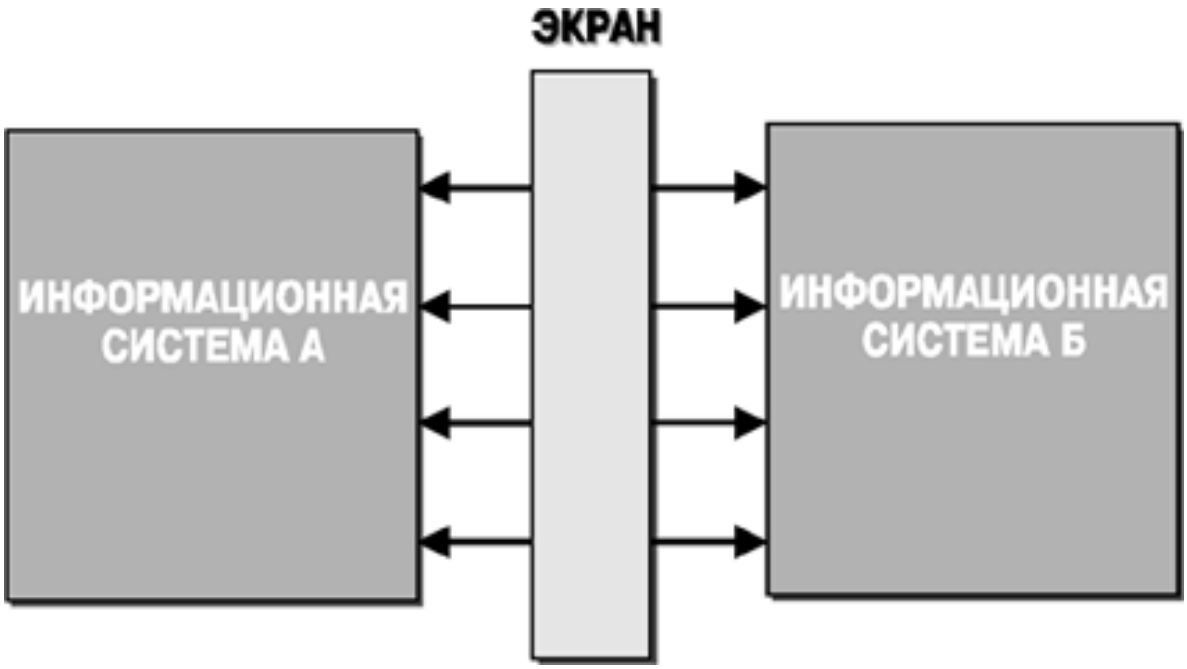

Рисунок 2.2.1. Экран FireWall.

Экран выполняет свои функции, контролируя все информационные потоки между этими двумя множествами информационных систем, работая как некоторая “информационная мембрана”. В этом смысле экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа. в частности, фиксировать все “незаконные” попытки доступа к информации и, дополнительно, сигнализировать о ситуациях, требующих немедленной реакции, то есть поднимать тревогу.

Обычно экранирующие системы делают несимметричными. Для экранов определяются понятия “внутри” и “снаружи”, и задача экрана состоит в защите внутренней сети от “потенциально враждебного” окружения. Важнейшим примером потенциально враждебной внешней сети является Internet.

Рассмотрим более подробно, какие проблемы возникают при построении экранирующих систем. При этом мы будем рассматривать не только проблему безопасного подключения к Internet, но и разграничение доступа внутри корпоративной сети организации.

Первое, очевидное требование к таким системам, это обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

Во-вторых, экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного воплощения в жизнь политики безопасности организации и, кроме того, для обеспечения простой реконфигурации системы при изменении структуры сети.

В-третьих, экранирующая система должна работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий.

В-четвертых, экранирующая система должна работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в "пиковых" режимах. Это необходимо для того, чтобы firewall нельзя было, образно говоря, "забросать" большим количеством вызовов, которые привели бы к нарушению ее работы.

Пятое. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий, поскольку она является ключом к конфиденциальной информации в организации.

Шестое. В идеале, если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности.

Седьмое. Система Firewall должна иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им, тем немение, требуется доступ, по крайней мере, к некоторым ресурсам внутренней компьютерной сети организации. Система должна уметь надежно распознавать таких пользователей и предоставлять им необходимый доступ к информации.

Структура системы Solstice Firewall-1

Классическим примером, на котором хотелось бы проиллюстрировать все вышеизложенные принципы, является программный комплекс Solstice FireWall-1 компании Sun Microsystems. Данный пакет неоднократно отмечался наградами на выставках и конкурсах. Он обладает многими полезными особенностями, выделяющими его среди продуктов аналогичного назначения.

Рассмотрим основные компоненты Solstice FireWall-1 и функции, которые они реализуют (рис. 2.2.2).

Центральным для системы FireWall-1 является модуль управления всем комплексом. С этим модулем работает администратор безопасности сети. Следует отметить, что продуманность и удобство графического

интерфейса модуля управления отмечалось во многих независимых обзорах, посвященных продуктам данного класса.

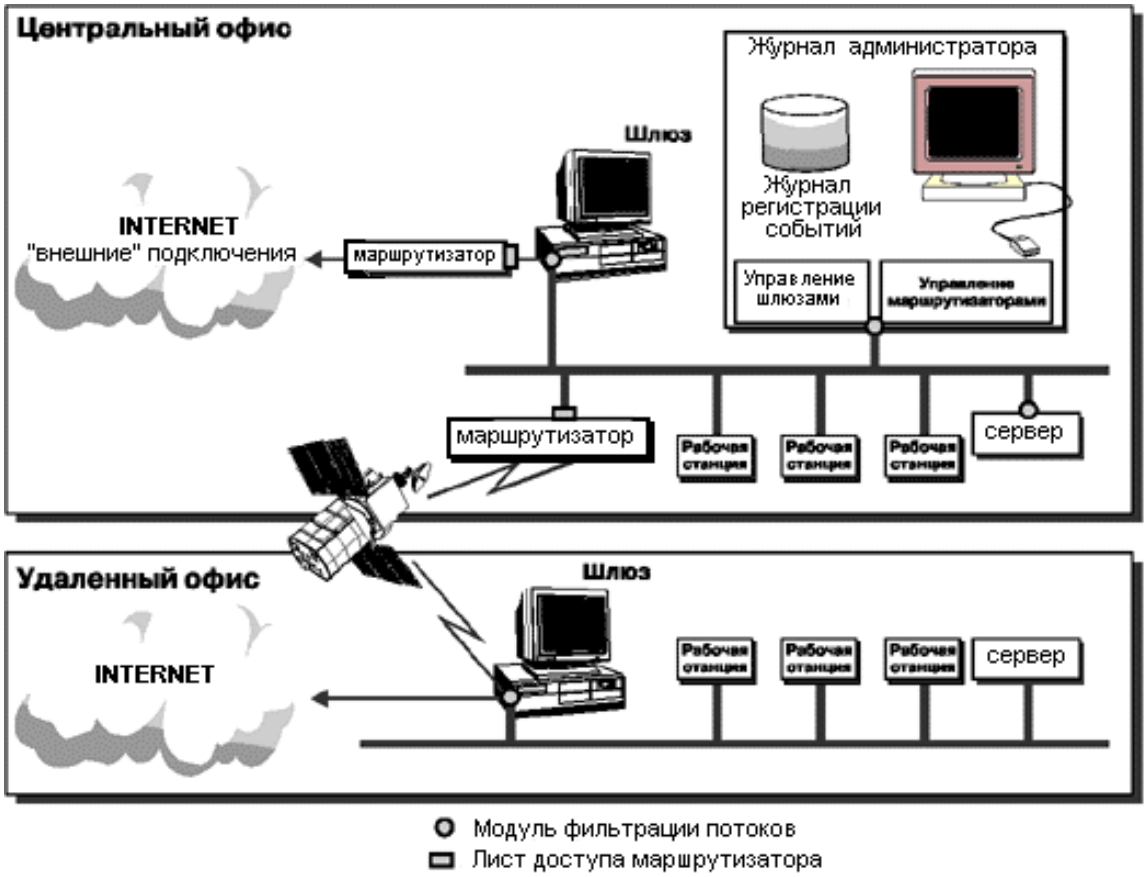

Рисунок 2.2.2. Основные компоненты Solstice FireWall-1 .

Администратору безопасности сети для конфигурирования комплекса FireWall-1 необходимо выполнить следующий ряд действий:

- Определить объекты, участвующие в процессе обработки информации. Здесь имеются в виду пользователи и группы пользователей, компьютеры и их группы, маршрутизаторы и различные подсети локальной сети организации.
- Описать сетевые протоколы и сервисы, с которыми будут работать приложения. Впрочем, обычно достаточным оказывается набор из более чем 40 описаний, поставляемых с системой FireWall-1.
- Далее, с помощью введенных понятий описывается политика разграничения доступа в следующих терминах: “Группе пользователей А разрешен доступ к ресурсу Б с помощью сервиса или протокола С, но об этом необходимо сделать пометку в регистрационном журнале”. Совокупность таких записей компилируется в исполнимую форму блоком управления и далее передается на исполнение в модули фильтрации.

Модули фильтрации могут располагаться на компьютерах - шлюзах или выделенных серверах - или в маршрутизаторах как часть конфигурационной информации. В настоящее время поддерживаются следующие два типа маршрутизаторов: Cisco IOS 9.x, 10.x, а также BayNetworks (Wellfleet) OS v.8.

Модули фильтрации просматривают все пакеты, поступающие на сетевые интерфейсы, и, в зависимости от заданных правил, пропускают или отбрасывают эти пакеты, с соответствующей записью в регистрационном журнале. Следует отметить, что эти модули, работая непосредственно с драйверами сетевых интерфейсов, обрабатывают весь поток данных, располагая полной информацией о передаваемых пакетах.

Пример реализации политики безопасности

Рассмотрим процесс практической реализации политики безопасности организации с помощью программного пакета FireWall-1. (рис. 2.2.3) .

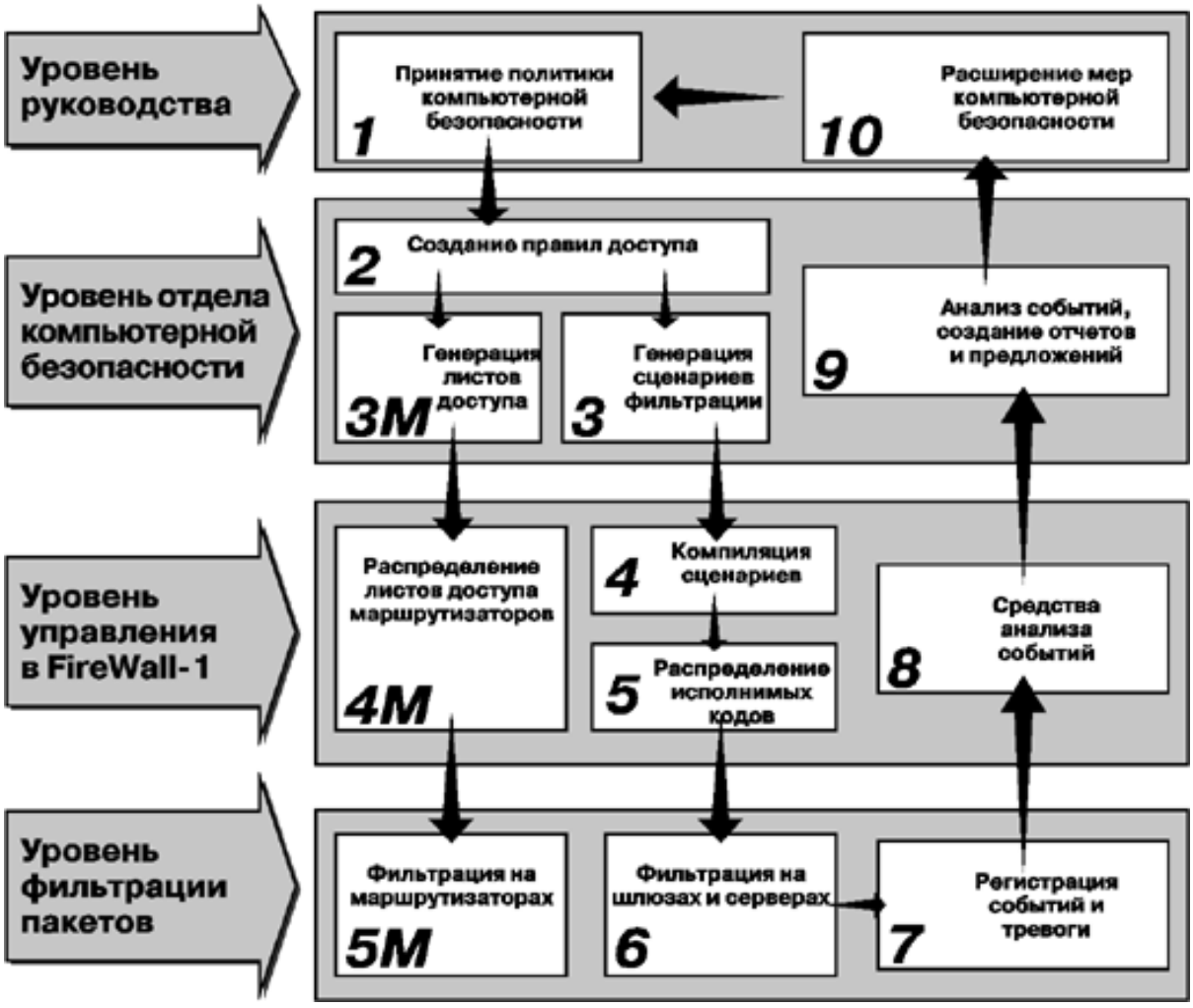

Рисунок 2.2.3. Реализация политики безопасности FireWall.

1. Прежде всего, как уже отмечалось, разрабатываются и утверждаются на уровне руководства организации правила политики безопасности.

2. После утверждения эти правила надо воплотить в жизнь. Для этого их нужно перевести в структуру типа “откуда, куда и каким способом доступ разрешен или, наоборот, запрещен. Такие структуры, как мы уже знаем, легко переносятся в базы правил системы FireWall-1.

3. Далее, на основе этой базы правил формируются списки доступа для маршрутизаторов и сценарии работы фильтров на сетевых шлюзах. Списки и сценарии далее переносятся на физические компоненты сети, после чего правила политики безопасности “вступают в силу”.

4. В процессе работы фильтры пакетов на шлюзах и серверах генерируют записи обо всех событиях, которые им приказали отслеживать, а, также, запускают механизмы “тревоги”, требующие от администратора немедленной реакции.

5. На основе анализа записей, сделанных системой, отдел компьютерной безопасности организации может разрабатывать предложения по изменению и дальнейшему развитию политики безопасности.

Рассмотрим простой пример реализации следующих правил:

1. Из локальных сетей подразделений, возможно удаленных, разрешается связь с любой локальной сетью организации после аутентификации, например, по UNIX-паролю.

2. Всем запрещается доступ к сети финансового департамента, за исключением генерального директора и директора этого департамента.

3. Из Internet разрешается только отправлять и получать почту. Обо всех других попытках связи необходимо делать подробную запись.

Все эти правила естественным образом представляются средствами графического интерфейса Редактора Правил FireWall-1 (рис. 2.2.4).

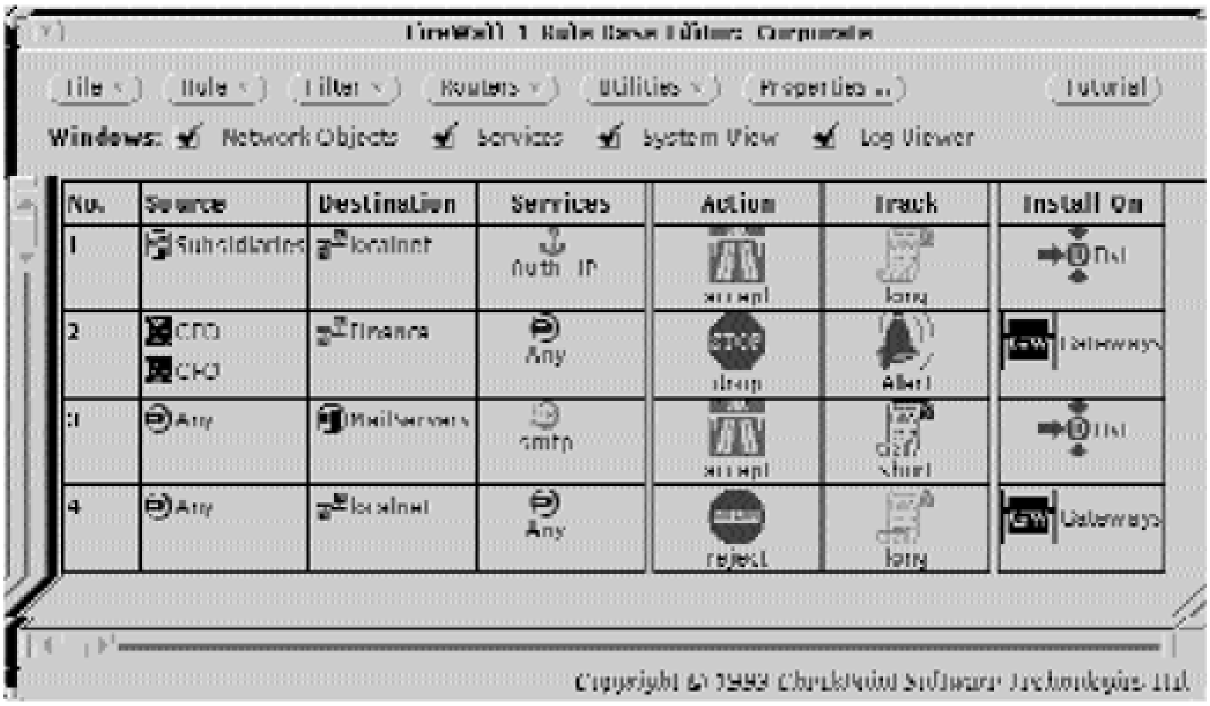

Рисунок 2.2.4. Графический интерфейс Редактора Правил FireWall-1 .

После загрузки правил, FireWall-1 для каждого пакета, передаваемого по сети, последовательно просматривает список правил до нахождения элемента, соответствующего текущему случаю.

Важным моментом является защита системы, на которой размещен административно-конфигурационный модуль FireWall-1. Рекомендуется запретить средствами FireWall-1 все виды доступа к данной машине, или по крайней мере строго ограничить список пользователей, которым это разрешено, а также принять меры по физическому ограничению доступа и по защите обычными средствами ОС UNIX.

Управление системой FireWall-1

На рис. 2.2.5 показаны основные элементы управления системой FireWall-1.

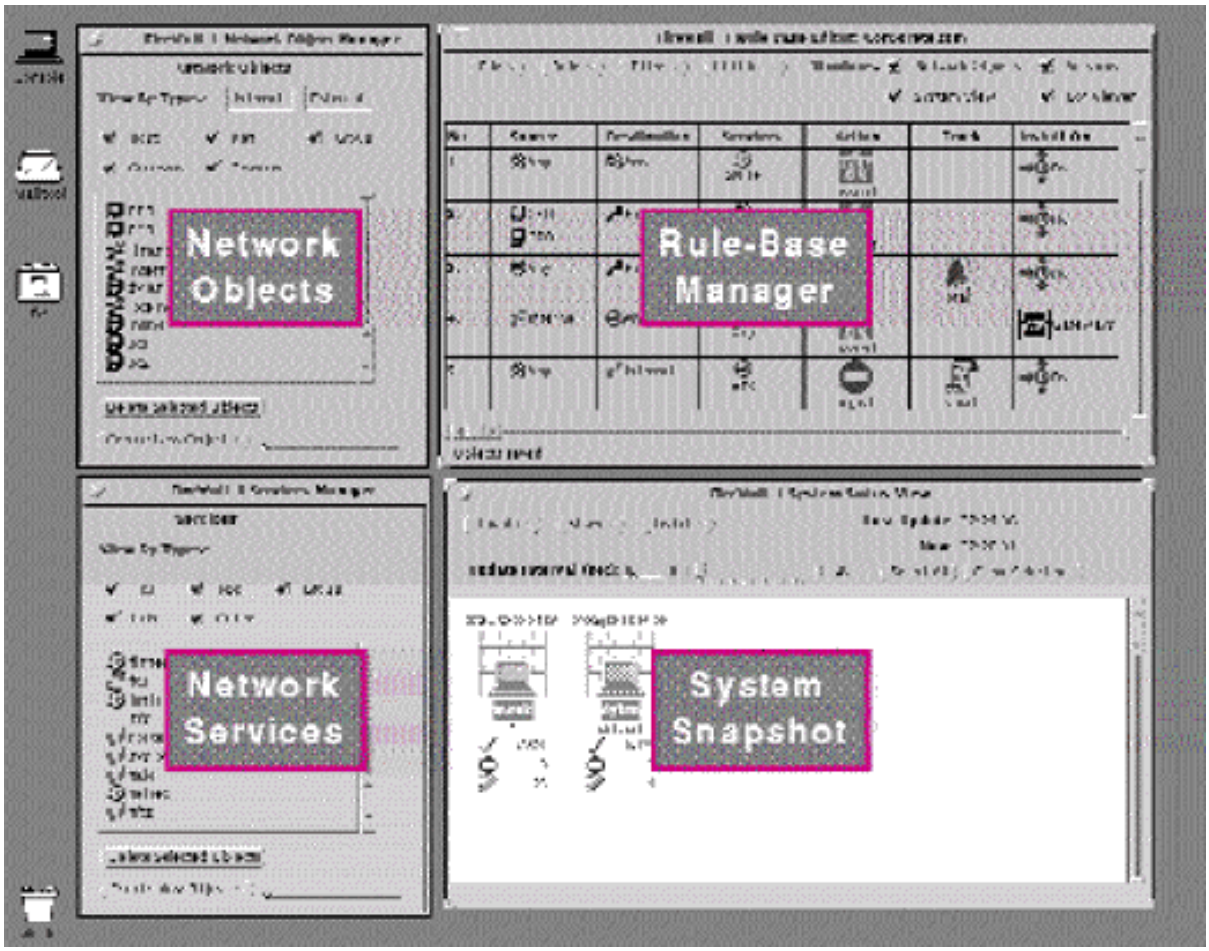

Рисунок 2.2.5. Основные элементы управления системой FireWall-1.

Слева расположены редакторы баз данных об объектах, существующих в сети и о протоколах или сервисах, с помощью которых происходит обмен информацией. Справа вверху показан редактор правил доступа.

Справа внизу располагается интерфейс контроля текущего состояния системы, в котором для всех объектов, которые занес туда администратор, отображаются данные о количестве разрешенных коммуникаций (галочки), о количестве отвергнутых связей (знак “кирпич”) и о количестве коммуникаций с регистрацией (иконка карандаш). Кирпичная стена за символом объекта (компьютера) означает, что на нем установлен модуль фильтрации системы FireWall-1.

Еще один пример реализации политики безопасности

Рассмотрим теперь случай, когда первоначальная конфигурация сети меняется, а вместе с ней меняется и политика безопасности.

Пусть мы решили установить у себя в организации несколько общедоступных серверов для предоставления информационных услуг. Это

могут быть, например, серверы World Wide Web, FTP или другие информационные серверы. Поскольку такие системы обособлены от работы всей остальной сети организации, для них часто выделяют свою собственную подсеть, имеющую выход в Internet через шлюз (рис. 2.2.6).
Рисунок 2.2.6

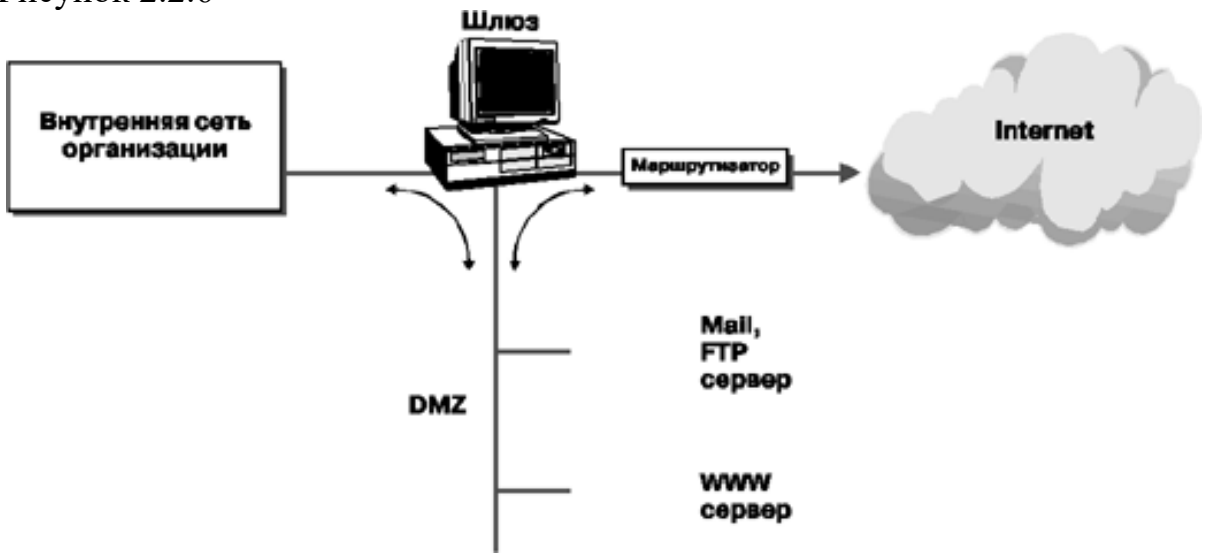

Рисунок 2.2.6. Схема шлюза Internet.

Поскольку в предыдущем примере локальная сеть была уже защищена, то все, что нам надо сделать, это просто разрешить соответствующий доступ в выделенную подсеть. Это делается с помощью одной дополнительной строки в редакторе правил, которая здесь показана. Такая ситуация является типичной при изменении конфигурации FireWall-1. Обычно для этого требуется изменение одной или небольшого числа строк в наборе правил доступа, что, несомненно, иллюстрирует мощь средств конфигурирования и общую продуманность архитектуры FireWall-1.

Аутенфикация пользователей при работе с FTP

Solstice FireWall-1 позволяет администратору установить различные режимы работы с интерактивными сервисами FTP и telnet для различных пользователей и групп пользователей. При установленном режиме аутентификации, FireWall-1 заменяет стандартные FTP и telnet демоны UNIX на свои собственные, располагая их на шлюзе, закрытом с помощью модулей фильтрации пакетов. Пользователь, желающий начать интерактивную сессию по FTP или telnet (это должен быть разрешенный пользователь и в разрешенное для него время), может сделать это только через вход на такой шлюз, где и выполняется вся процедура

аутентификации. Она задается при описании пользователей или групп пользователей и может проводиться следующими способами:
- Unix-пароль;
- программа S/Key генерации одноразовых паролей;
- карточки SecurID с аппаратной генерацией одноразовых паролей.

Гибкие алгоритмы фильтрации UDP – пакетов, динамическое экранирование

UDP-протоколы, входящие в состав набора TCP/IP, представляют собой особую проблему для обеспечения безопасности. С одной стороны на их основе создано множество приложений. С другой стороны, все они являются протоколами “без состояния”, что приводит к отсутствию различий между запросом и ответом, приходящим извне защищаемой сети.

Пакет FireWall-1 решает эту проблему созданием контекста соединений поверх UDP сессий, запоминая параметры запросов. Пропускаются назад только ответы внешних серверов на высланные запросы, которые однозначно отличаются от любых других UDP-пакетов (читай: незаконных запросов), поскольку их параметры хранятся в памяти FireWall-1.

Следует отметить, что данная возможность присутствует в весьма немногих программах экранирования, распространяемых в настоящий момент.

Заметим также, что подобные механизмы задействуются для приложений, использующих RPC, и для FTP сеансов. Здесь возникают аналогичные проблемы, связанные с динамическим выделением портов для сеансов связи, которые FireWall-1 отслеживает аналогичным образом, запоминая необходимую информацию при запросах на такие сеансы и обеспечивая только “законный” обмен данными.

Данные возможности пакета Solstice FireWall-1 резко выделяют его среди всех остальных межсетевых экранов. Впервые проблема обеспечения безопасности решена для всех без исключения сервисов и протоколов, существующих в Internet.

Язык программирования

Система Solstice FireWall-1 имеет собственный встроенный обьектно-ориентированный язык программирования, применяемый для описания поведения модулей - Фильтров системы. Собственно говоря, результатом работы графического интерфейса администратора системы является сгенерированный сценарий работы именно на этом внутреннем

языке. Он не сложен для понимания, что допускает непосредственное программирование на нем. Однако на практике данная возможность почти не используется, поскольку графический интерфейс системы и так позволяет сделать практически все, что нужно.

Прозрачность и эффективность

FireWall-1 полностью прозрачен для конечных пользователей. Еще одним замечательным свойством системы Solstice FireWall-1 является очень высокая скорость работы. Фактически модули системы работают на сетевых скоростях передачи информации, что обусловлено компиляцией сгенерированных сценариев работы перед подключением их непосредственно в процесс фильтрации.

Компания Sun Microsystems приводит такие данные об эффективности работы Solstice FireWall-1. Модули фильтрации на Internet-шлюзе, сконфигурированные типичным для многих организаций образом, работая на скоростях обычного Ethernet в 10 Мб/сек, забирают на себя не более 10% вычислительной мощности процессора SPARCstation 5,85 МГц или компьютера 486DX2-50 с операционной системой Solaris/x86.

Solstice FireWall-1 - эффективное средство защиты корпоративных сетей и их сегментов от внешних угроз, а также от несанкционированных взаимодействий локальных пользователей с внешними системами.

Solstice FireWall-1 обеспечивает высокоуровневую поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP.

Solstice FireWall-1 характеризуется прозрачностью для легальных пользователей и высокой эффективностью.

По совокупности технических и стоимостных характеристик Solstice FireWall-1 занимает лидирующую позицию среди межсетевых экранов.

2.2.2. Ограничения доступа в WWW серверах

Рассмотрим два из них:

- Ограничить доступ по IP адресам клиентских машин;
- ввести идентификатор получателя с паролем для данного вида документов.

Такого рода ввод ограничений стал использоваться достаточно часто, т.к. многие стремятся в Internet, чтобы использовать его коммуникации для доставки своей информации потребителю. С помощью такого рода механизмов по разграничению прав доступа удобно производить саморассылку информации на получение которой существует договор.

Ограничения по IP адресам

Доступ к приватным документам можно разрешить, либо наоборот запретить используя IP адреса конкретных машин или сеток, например:

123.456.78.9

123.456.79.

В этом случае доступ будет разрешен (или запрещен в зависимости от контекста) для машины с IP адресом 123.456.78.9 и для всех машин подсетки 123.456.79.

Ограничения по идентификатору получателя

Доступ к приватным документам можно разрешить, либо наоборот запретить используя присвоенное имя и пароль конкретному пользователю, причем пароль в явном виде нигде не хранится.

Рассмотрим такой пример: Агенство печати предоставляет свою продукцию, только своим подписчикам, которые заключили договор и оплатили подписку. WWW Сервер находится в сети Internet и общедоступен.

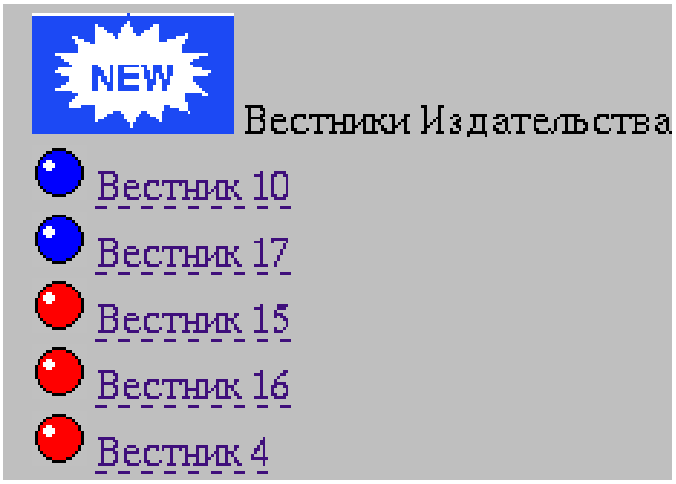

Рисунок 2.2.7. Пример списка вестников издательства.

Выберем Вестник предоставляемый конкретному подписчику. На клиентском месте подписчик получает сообщение:

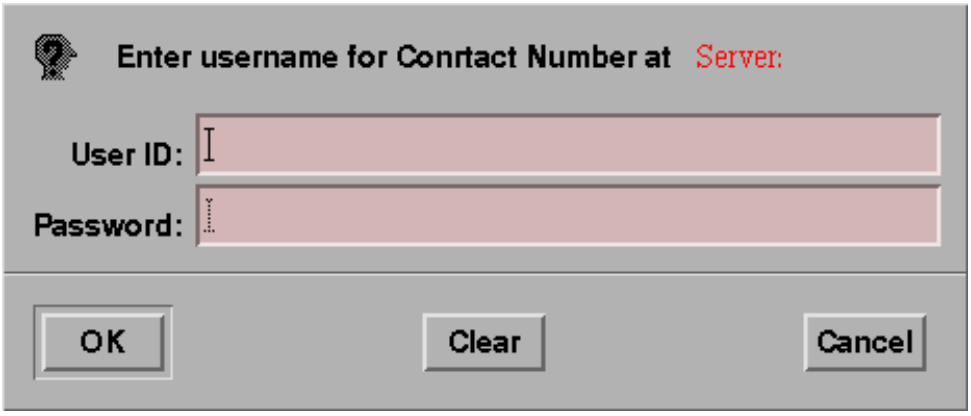

Рисунок 2.2.8. Окно ввода пароля.

Если он правильно написал свое имя и пароль, то он допускается до документа, в противном случае - получает сообщение:

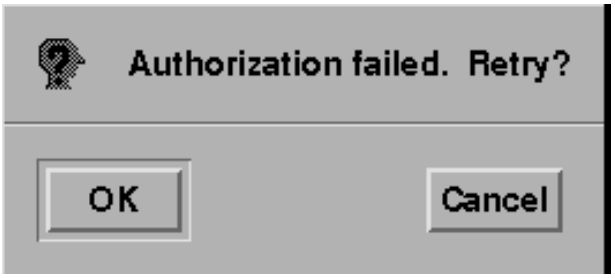

Рисунок 2.2.9. Окно неправильного ввода пароля.

2.3. Информационная безопасность в Intranet

Архитектура Intranet подразумевает подключение к внешним открытым сетям, использование внешних сервисов и предоставление собственных сервисов вовне, что предъявляет повышенные требования к защите информации.

В Intranet-системах используется подход клиент-сервер, а главная роль на сегодняшний день отводится Web-сервису. Web-серверы должны поддерживать традиционные защитные средства, такие как аутентификация и разграничение доступа; кроме того, необходимо обеспечение новых свойств, в особенности безопасности программной среды и на серверной, и на клиентской сторонах.

Таковы, если говорить совсем кратко, задачи в области информационной безопасности, возникающие в связи с переходом на технологию Intranet. Далее мы рассмотрим возможные подходы к их решению.

Формирование режима информационной безопасности - проблема комплексная.

Меры по ее решению можно разделить на четыре уровня:
- законодательный (законы, нормативные акты, стандарты и т.п.);
- административный (действия общего характера, предпринимаемые руководством организации);
- процедурный (конкретные меры безопасности, имеющие дело с людьми);
- программно-технический (конкретные технические меры).

В таком порядке и будет построено последующее изложение.

Разработка сетевых аспектов политики безопасности

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:
- невозможность миновать защитные средства;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть “тайных” модемных входов или тестовых линий, идущих в обход экрана.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо

полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

Последний принцип - всеобщая поддержка мер безопасности - носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать

заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Анализ рисков - важнейший этап выработки политики безопасности. При оценке рисков, которым подвержены Intranet-системы, нужно учитывать следующие обстоятельства:

- новые угрозы по отношению к старым сервисам, вытекающие из возможности пассивного или активного прослушивания сети. Пассивное прослушивание означает чтение сетевого трафика, а активное - его изменение (кражу, дублирование или модификацию передаваемых данных). Например, аутентификация удаленного клиента с помощью пароля многократного использования не может считаться надежной в сетевой среде, независимо от длины пароля;
- новые (сетевые) сервисы и ассоциированные с ними угрозы.

Как правило, в Intranet-системах следует придерживаться принципа “все, что не разрешено, запрещено”, поскольку “лишний” сетевой сервис может предоставить канал проникновения в корпоративную систему. В принципе, ту же мысль выражает положение “все непонятное опасно”.

Процедурные меры

В общем и целом Intranet-технология не предъявляет каких-либо специфических требований к мерам процедурного уровня. На наш взгляд, отдельного рассмотрения заслуживают лишь два обстоятельства:

- описание должностей, связанных с определением, наполнением и поддержанием корпоративной гипертекстовой структуры официальных документов;
- поддержка жизненного цикла информации, наполняющей Intranet.

При описании должностей целесообразно исходить из аналогии между Intranet и издательством. В издательстве существует директор, определяющий общую направленность деятельности. В Intranet ему соответствует Web-администратор, решающий, какая корпоративная информация должна присутствовать на Web-сервере и как следует структурировать дерево (точнее, граф) HTML-документов.

В многопрофильных издательствах существуют редакции, занимающиеся конкретными направлениями (математические книги, книги для детей и т.п.). Аналогично, в Intranet целесообразно выделить должность публикатора, ведающего появлением документов отдельных подразделений и определяющего перечень и характер публикаций.

У каждой книги есть титульный редактор, отвечающий перед издательством за свою работу. В Intranet редакторы занимаются вставкой документов в корпоративное дерево, их коррекцией и удалением. В

больших организациях “слой” публикатор/редактор может состоять из нескольких уровней.

Наконец, и в издательстве, и в Intranet должны быть авторы, создающие документы. Подчеркнем, что они не должны иметь прав на модификацию корпоративного дерева и отдельных документов. Их дело - передать свой труд редактору.

Кроме официальных, корпоративных, в Intranet могут присутствовать групповые и личные документы, порядок работы с которыми (роли, права доступа) определяется, соответственно, групповыми и личными интересами.

Переходя к вопросам поддержки жизненного цикла Intranet-информации, напомним о необходимости использования средств конфигурационного управления. Важное достоинство Intranet-технологии состоит в том, что основные операции конфигурационного управления - внесение изменений (создание новой версии) и извлечение старой версии документа - естественным образом вписываются в рамки Web-интерфейса. Те, для кого это необходимо, могут работать с деревом всех версий всех документов, подмножеством которого является дерево самых свежих версий.

Управление доступом путем фильтрации информации

Мы переходим к рассмотрению мер программно-технического уровня, направленных на обеспечение информационной безопасности систем, построенных в технологии Intranet. На первое место среди таких мер мы поставим межсетевые экраны - средство разграничения доступа, служащее для защиты от внешних угроз и от угроз со стороны пользователей других сегментов корпоративных сетей.

Отметим, что бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС - это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для получения нелегальных привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений (как и врач, не ведающий всех побочных воздействий рекомендуемых лекарств). Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.).

Как указывалось выше, единственный перспективный путь связан с разработкой специализированных защитных средств, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран - это полупроницаемая мембрана, которая располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и контролирует все информационные потоки во внутреннюю сеть и из нее (Рис. 2.3.1). Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

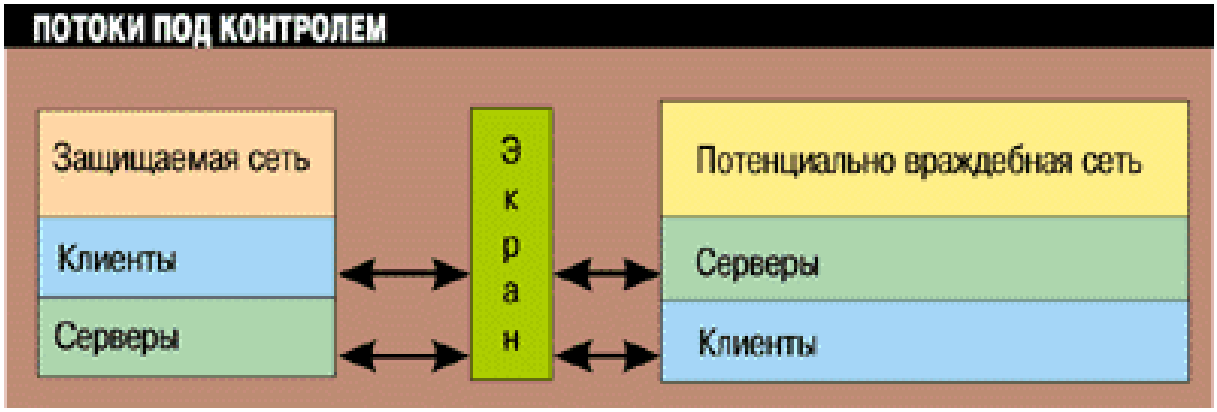

Рисунок 2. 3.1. Межсетевой экран как средство контроля информационных потоков.

Целесообразно разделить случаи, когда экран устанавливается на границе с внешней (обычно общедоступной) сетью или на границе между сегментами одной корпоративной сети. Соответственно, мы будет говорить о внешнем и внутреннем межсетевых экранах.

Как правило, при общении с внешними сетями используется исключительно семейство протоколов TCP/IP. Поэтому внешний межсетевой экран должен учитывать специфику этих протоколов. Для внутренних экранов ситуация сложнее, здесь следует принимать во внимание помимо TCP/IP по крайней мере протоколы SPX/IPX, применяемые в сетях Novell NetWare. Иными словами, от внутренних экранов нередко требуется многопротокольность.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, является, скорее, исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования (Рис. 2.3.2). В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

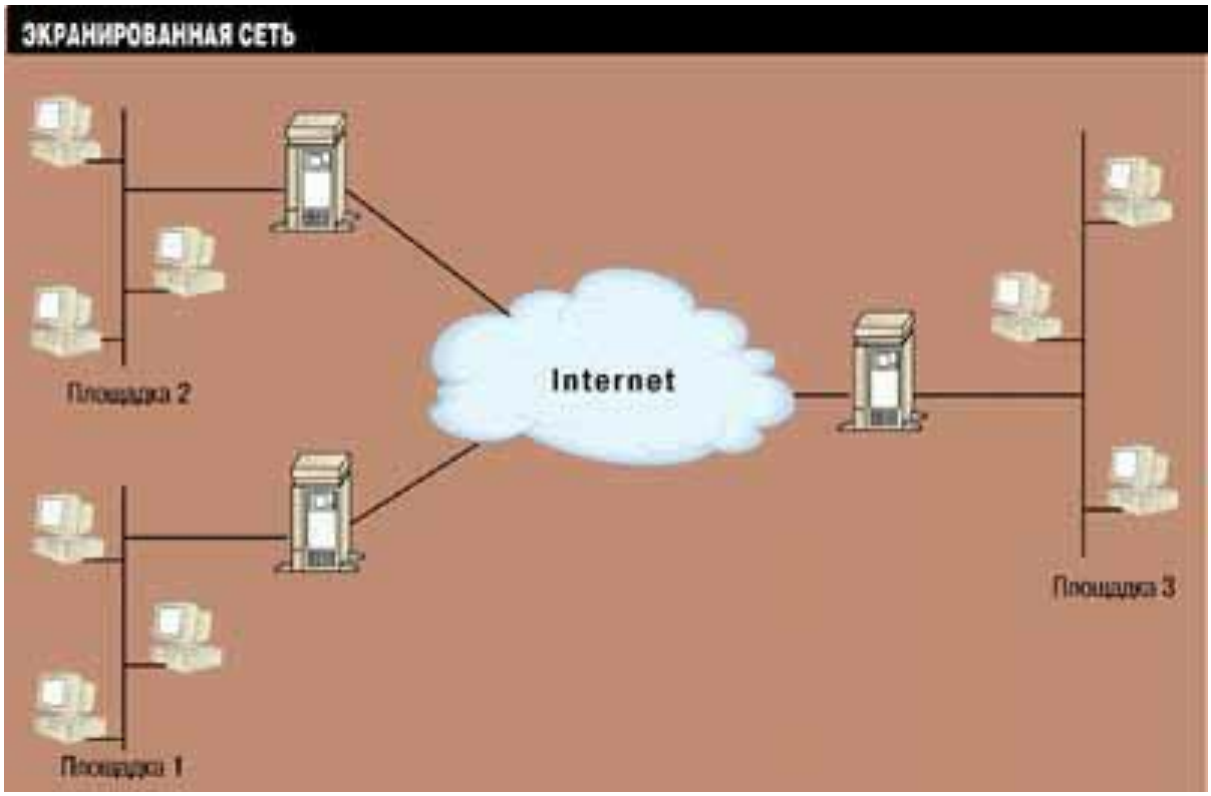

Рисунок 2.3.2. Экранирование корпоративной сети, состоящей из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования.

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по тому, на каком уровне производится фильтрация - канальном, сетевом, транспортном или прикладном. Соответственно, можно говорить об экранирующих концентраторах (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

В данной работе мы не будем рассматривать экранирующие концентраторы, поскольку концептуально они мало отличаются от экранирующих маршрутизаторов.

При принятии решения “пропустить/не пропустить”, межсетевые экраны могут использовать не только информацию, содержащуюся в фильтруемых потоках, но и данные, полученные из окружения, например текущее время.

Таким образом, возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует экран, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее экран может быть сконфигурирован. В то же время фильтрация на каждом из перечисленных выше уровней обладает своими достоинствами, такими как дешевизна, высокая эффективность или прозрачность для пользователей. В силу этой, а также некоторых других причин, в большинстве случаев используются смешанные конфигурации, в которых объединены разнотипные экраны. Наиболее типичным является сочетание экранирующих маршрутизаторов и прикладного экрана (Рис. 2.3.3).

Приведенная конфигурация называется экранирующей подсетью. Как правило, сервисы, которые организация предоставляет для внешнего применения (например “представительский” Web-сервер), целесообразно выносить как раз в экранирующую подсеть.

Помимо выразительных возможностей и допустимого количества правил качество межсетевого экрана определяется еще двумя очень важными характеристиками - простотой применения и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при задании правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. При выполнении централизованного администрирования следует еще позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность.

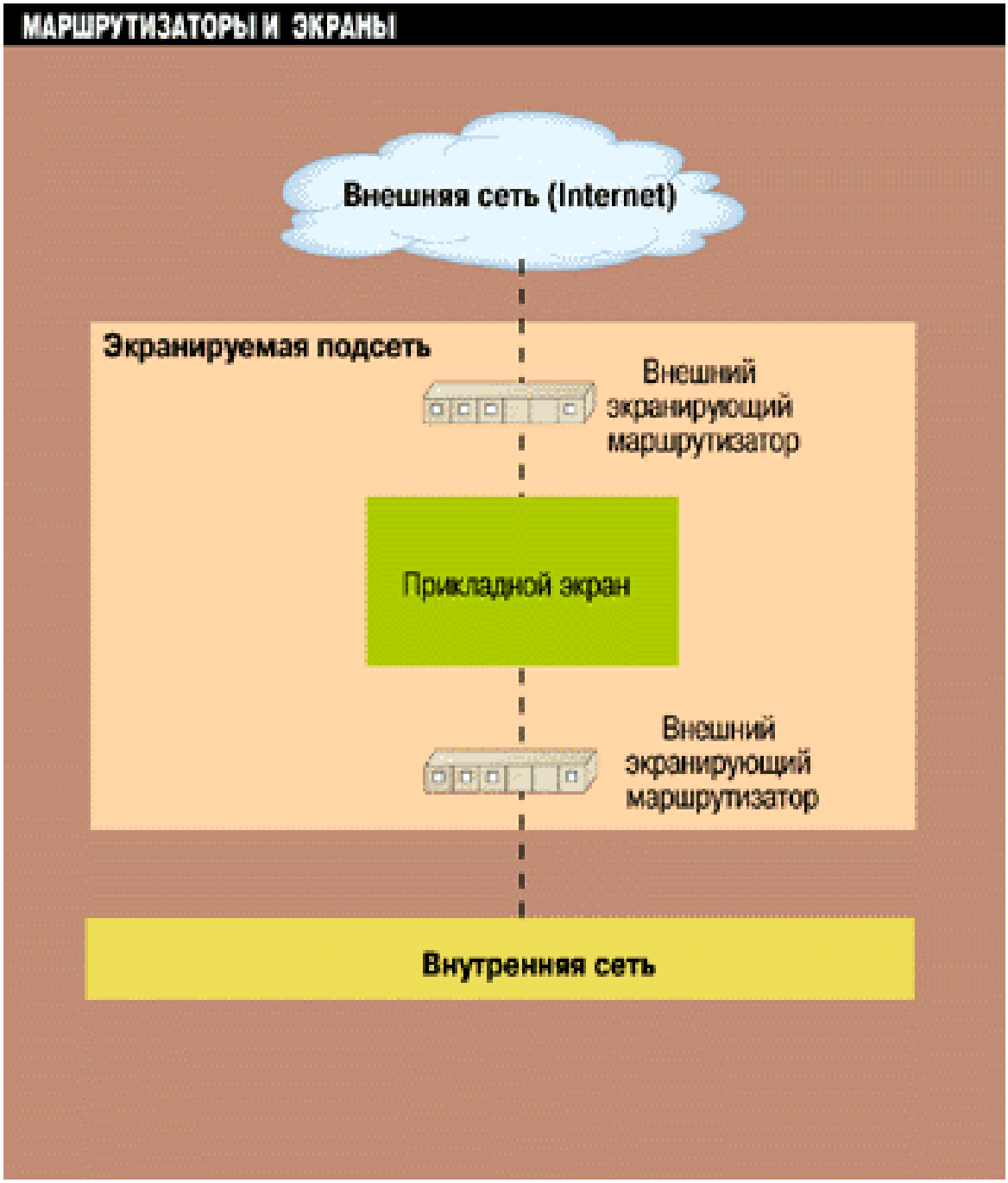

Рисунок 2.3.3. Сочетание экранирующих маршрутизаторов и прикладного экрана.

Хотелось бы подчеркнуть, что природа экранирования (фильтрации), как механизма безопасности, очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Так, прикладной экран может осуществлять действия от имени субъектов внутренней сети, в результате

чего из внешней сети кажется, что имеет место взаимодействие исключительно с межсетевым экраном (Рис. 2.3.4). При таком подходе топология внутренней сети скрыта от внешних пользователей, поэтому задача злоумышленника существенно усложняется.

Рисунок 2.3.4. Истинные и кажущиеся информационные потоки.

Более общим методом сокрытия информации о топологии защищаемой сети является трансляция “внутренних” сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый видит лишь то, что ему положено.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, в частности таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация баз данных.

Безопасность программной среды

Идея сетей с так называемыми активными агентами, когда между компьютерами передаются не только пассивные, но и активные исполняемые данные (то есть программы), разумеется, не нова. Первоначально цель состояла в том, чтобы уменьшить сетевой трафик, выполняя основную часть обработки там, где располагаются данные (приближение программ к данным). На практике это означало

перемещение программ на серверы. Классический пример реализации подобного подхода - это хранимые процедуры в реляционных СУБД.

Для Web-серверов аналогом хранимых процедур являются программы, обслуживающие общий шлюзовый интерфейс (Common Gateway Interface - CGI).

CGI-процедуры располагаются на серверах и обычно используются для динамического порождения HTML-документов. Политика безопасности организации и процедурные меры должны определять, кто имеет право помещать на сервер CGI-процедуры. Жесткий контроль здесь необходим, поскольку выполнение сервером некорректной программы может привести к сколь угодно тяжелым последствиям. Разумная мера технического характера состоит в минимизации привилегий пользователя, от имени которого выполняется Web-сервер.

В технологии Intranet, если заботиться о качестве и выразительной силе пользовательского интерфейса, возникает нужда в перемещении программ с Web-серверов на клиентские компьютеры - для создания анимации, выполнения семантического контроля при вводе данных и т.д. Вообще, активные агенты - неотъемлемая часть технологии Intranet.

В каком бы направлении ни перемещались программы по сети, эти действия представляют повышенную опасность, т.к. программа, полученная из ненадежного источника, может содержать непреднамеренно внесенные ошибки или целенаправленно созданный зловредный код. Такая программа потенциально угрожает всем основным аспектам информационной безопасности:

- доступности (программа может поглотить все наличные ресурсы);
- целостности (программа может удалить или повредить данные);
- конфиденциальности (программа может прочитать данные и передать их по сети).

Проблему ненадежных программ осознавали давно, но, пожалуй, только в рамках системы программирования Java впервые предложена целостная концепция ее решения.

Java предлагает три оборонительных рубежа:

- надежность языка;
- контроль при получении программ;
- контроль при выполнении программ.

Впрочем, существует еще одно, очень важное средство обеспечения информационной безопасности - беспрецедентная открытость Java-системы. Исходные тексты Java-компилятора и интерпретатора доступны для проверки, поэтому велика вероятность, что ошибки и недочеты первыми будут обнаруживать честные специалисты, а не злоумышленники.

В концептуальном плане наибольшие трудности представляет контролируемое выполнение программ, загруженных по сети. Прежде всего, необходимо определить, какие действия считаются для таких программ допустимыми. Если исходить из того, что Java - это язык для написания клиентских частей приложений, одним из основных требований к которым является мобильность, загруженная программа может обслуживать только пользовательский интерфейс и осуществлять сетевое взаимодействие с сервером. Программа не может работать с файлами хотя бы потому, что на Java-терминале их, возможно, не будет. Более содержательные действия должны производиться на серверной стороне или осуществляться программами, локальными для клиентской системы.

Интересный подход предлагают специалисты компании Sun Microsystems для обеспечения безопасного выполнения командных файлов. Речь идет о среде Safe-Tcl (Tool Comman Language, инструментальный командный язык). Sun предложила так называемую ячеечную модель интерпретации командных файлов. Существует главный интерпретатор, которому доступны все возможности языка.

Если в процессе работы приложения необходимо выполнить сомнительный командный файл, порождается подчиненный командный интерпретатор, обладающий ограниченной функциональностью (например, из него могут быть удалены средства работы с файлами и сетевые возможности). В результате потенциально опасные программы оказываются заключенными в ячейки, защищающие пользовательские системы от враждебных действий. Для выполнения действий, которые считаются привилегированными, подчиненный интерпретатор может обращаться с запросами к главному. Здесь, очевидно, просматривается аналогия с разделением адресных пространств операционной системы и пользовательских процессов и использованием последними системных вызовов. Подобная модель уже около 30 лет является стандартной для многопользовательских ОС.

Защита Web – серверов

Наряду с обеспечением безопасности программной среды (см. предыдущий раздел), важнейшим будет вопрос о разграничении доступа к объектам Web-сервиса. Для решения этого вопроса необходимо уяснить, что является объектом, как идентифицируются субъекты и какая модель управления доступом - принудительная или произвольная - применяется.

В Web-серверах объектами доступа выступают универсальные локаторы ресурсов (URL - Uniform (Universal) Resource Locator). За этими локаторами могут стоять различные сущности – HTML - файлы, CGI-процедуры и т.п.

Как правило, субъекты доступа идентифицируются по IP-адресам и/или именам компьютеров и областей управления. Кроме того, может использоваться парольная аутентификация пользователей или более сложные схемы, основанные на криптографических технологиях.

В большинстве Web-серверов права разграничиваются с точностью до каталогов (директорий) с применением произвольного управления доступом. Могут предоставляться права на чтение HTML-файлов, выполнение CGI-процедур и т.д.

Для раннего выявления попыток нелегального проникновения в Web-сервер важен регулярный анализ регистрационной информации.

Разумеется, защита системы, на которой функционирует Web-сервер, должна следовать универсальным рекомендациям, главной из которых является максимальное упрощение. Все ненужные сервисы, файлы, устройства должны быть удалены. Число пользователей, имеющих прямой доступ к серверу, должно быть сведено к минимуму, а их привилегии - упорядочены в соответствии со служебными обязанностями.

Еще один общий принцип состоит в том, чтобы минимизировать объем информации о сервере, которую могут получить пользователи. Многие серверы в случае обращения по имени каталога и отсутствия файла index. HTML в нем, выдают HTML-вариант оглавления каталога. В этом оглавлении могут встретиться имена файлов с исходными текстами CGI-процедур или с иной конфиденциальной информацией. Такого рода “дополнительные возможности” целесообразно отключать, поскольку лишнее знание (злоумышленника) умножает печали (владельца сервера).

Аутентификация в открытых сетях

Методы, применяемые в открытых сетях для подтверждения и проверки подлинности субъектов, должны быть устойчивы к пассивному и активному прослушиванию сети. Суть их сводится к следующему.

- Субъект демонстрирует знание секретного ключа, при этом ключ либо вообще не передается по сети, либо передается в зашифрованном виде.
- Субъект демонстрирует обладание программным или аппаратным средством генерации одноразовых паролей или средством, работающим в режиме “запрос-ответ”. Нетрудно заметить, что перехват и последующее воспроизведение одноразового пароля или ответа на запрос ничего не дает злоумышленнику.
- Субъект демонстрирует подлинность своего местоположения, при этом используется система навигационных спутников.

Виртуальные частные сети

Одной из важнейших задач является защита потоков корпоративных данных, передаваемых по открытым сетям. Открытые каналы могут быть надежно защищены лишь одним методом - криптографическим.

Отметим, что так называемые выделенные линии не обладают особыми преимуществами перед линиями общего пользования в плане информационной безопасности. Выделенные линии хотя бы частично будут располагаться в неконтролируемой зоне, где их могут повредить или осуществить к ним несанкционированное подключение. Единственное реальное достоинство - это гарантированная пропускная способность выделенных линий, а вовсе не какая-то повышенная защищенность. Впрочем, современные оптоволоконные каналы способны удовлетворить потребности многих абонентов, поэтому и указанное достоинство не всегда облечено в реальную форму.

Любопытно упомянуть, что в мирное время 95% трафика Министерства обороны США передается через сети общего пользования (в частности через Internet). В военное время эта доля должна составлять “лишь” 70%. Можно предположить, что Пентагон - не самая бедная организация. Американские военные полагаются на сети общего пользования потому, что развивать собственную инфраструктуру в условиях быстрых технологических изменений - занятие очень дорогое и бесперспективное, оправданное даже для критически важных национальных организаций только в исключительных случаях.

Представляется естественным возложить на межсетевой экран задачу шифрования и дешифрования корпоративного трафика на пути во внешнюю сеть и из нее. Чтобы такое шифрование/дешифрование стало возможным, должно произойти начальное распределение ключей. Современные криптографические технологии предлагают для этого целый ряд методов.

После того как межсетевые экраны осуществили криптографическое закрытие корпоративных потоков данных, территориальная разнесенность сегментов сети проявляется лишь в разной скорости обмена с разными сегментами. В остальном вся сеть выглядит как единое целое, а от абонентов не требуется привлечение каких-либо дополнительных защитных средств.

Простота и однородность архитектуры

Важнейшим аспектом информационной безопасности является управляемость системы. Управляемость - это и поддержание высокой доступности системы за счет раннего выявления и ликвидации проблем, и

возможность изменения аппаратной и программной конфигурации в соответствии с изменившимися условиями или потребностями, и оповещение о попытках нарушения информационной безопасности практически в реальном времени, и снижение числа ошибок администрирования, и многое, многое другое.

Наиболее остро проблема управляемости встает на клиентских рабочих местах и на стыке клиентской и серверной частей информационной системы. Причина проста - клиентских мест гораздо больше, чем серверных, они, как правило, разбросаны по значительно большей площади, их используют люди с разной квалификацией и привычками. Обслуживание и администрирование клиентских рабочих мест - занятие чрезвычайно сложное, дорогое и чреватое ошибками. Технология Intranet за счет простоты и однородности архитектуры позволяет сделать стоимость администрирования клиентского рабочего места практически нулевой. Важно и то, что замена и повторный ввод в эксплуатацию клиентского компьютера могут быть осуществлены очень быстро, поскольку это “клиенты без состояния”, у них нет ничего, что требовало бы длительного восстановления или конфигурирования.

На стыке клиентской и серверной частей Intranet-системы находится Web-сервер. Это позволяет иметь единый механизм регистрации пользователей и наделения их правами доступа с последующим централизованным администрированием. Взаимодействие с многочисленными разнородными сервисами оказывается скрытым не только от пользователей, но и в значительной степени от системного администратора.

Задача обеспечения информационной безопасности в Intranet оказывается более простой, чем в случае произвольных распределенных систем, построенных в архитектуре клиент/сервер. Причина тому - однородность и простота архитектуры Intranet. Если разработчики прикладных систем сумеют в полной мере воспользоваться этим преимуществом, то на программно-техническом уровне им будет достаточно нескольких недорогих и простых в освоении продуктов. Правда, к этому необходимо присовокупить продуманную политику безопасности и целостный набор мер процедурного уровня.

3. РАЗРАБОТКА И РЕАЛИЗАЦИЯ ПРОГРАММЫ ДЛЯ АЛГОРИТМА IDEA

3.1. Принципы работы алгоритма IDEA

IDEA (International Data Encryption Algorithm) является блочным симметричным алгоритмом шифрования, разработанным Сюдзя Лай (Xuejia Lai) и Джеймсом Массей (James Massey) из швейцарского федерального института технологий. Первоначальная версия была опубликована в 1990 году. Пересмотренная версия алгоритма, усиленная средствами защиты от дифференциальных криптографических атак, была представлена в 1991 году и подробно описана в 1992 году.

IDEA является одним из нескольких симметричных криптографических алгоритмов, которыми первоначально предполагалось заменить DES.

Принципы разработки

IDEA является блочным алгоритмом, который использует 128-битовый ключ для шифрования данных блоками по 64 бита.

Целью разработки IDEA было создание относительно стойкого криптографического алгоритма с достаточно простой реализацией.

Криптографическая стойкость

Следующие характеристики IDEA характеризуют его криптографическую стойкость:

1. **Длина блока**: длина блока должна быть достаточной, чтобы скрыть все статистические характеристики исходного сообщения. С другой стороны, сложность реализации криптографической функции возрастает экспоненциально в соответствии с размером блока. Использование блока размером в 64 бита в 90-е годы означало достаточную силу. Более того, использование режима шифрования CBC говорит о дальнейшем усилении этого аспекта алгоритма.
2. **Длина ключа**: длина ключа должна быть достаточно большой для того, чтобы предотвратить возможность простого перебора ключа. При длине ключа 128 бит IDEA считается достаточно безопасным.
3. **Конфузия**: зашифрованный текст должен зависеть от ключа сложным и запутанным способом.
4. **Диффузия**: каждый бит незашифрованного текста должен влиять на каждый бит зашифрованного текста. Распространение одного незашифрованного бита на большое количество зашифрованных битов скрывает статистическую структуру незашифрованного текста.

Определить, как статистические характеристики зашифрованного текста зависят от статистических характеристик незашифрованного текста, должно быть непросто. IDEA с этой точки зрения является очень эффективным алгоритмом.

В IDEA два последних пункта выполняются с помощью трех операций. Это отличает его от DES, где все постороено на использовании операции XOR и маленьких нелинейных S-boxes.

Каждая операция выполняется над двумя 16-битными входами и создает один 16-битный выход. Этими операциями являются:

1. Побитовое исключающее OR, обозначаемое как $\oplus$.
2. Сумма целых по модулю 2^{16} (по модулю 65536), при этом входы и выходы трактуются как беззнаковые 16-битные целые. Эту операцию обозначим как +.
3. Умножение целых по модулю $2^{16} + 1$ (по модулю 65537), при этом входы и выходы трактуются как беззнаковые 16-битные целые, за исключением того, что блок из одних нулей трактуется как 2^{16}. Эту операцию обозначим как •.

Эти три операции являются несовместимыми в том смысле, что:

1. Не существует пары из трех операций, удовлетворяющих дистрибутивному закону. Например

$a \bullet (b + c) <> (a \bullet b) + (a \bullet c)$

2. Не существует пары из трех операций, удовлетворяющих ассоциативному закону. Например

$a + (b \oplus c) <> (a + b) \oplus c$

Использование комбинации из этих трех операций обеспечивает комплексную трансформацию входа, делая криптоанализ более трудным, чем в таком алгоритме как DES, основанном исключительно на функции XOR.

Шифрование

Рассмотрим общую схему шифрования IDEA. Как и в любом алгоритме шифрования, здесь существует два входа: незашифрованный блок и ключ. В данном случае незашифрованный блок имеет длину 64 бита, ключ имеет длину 128 бит.

Алгоритм IDEA состоит из восьми раундов, за которыми следует заключительное преобразование. Алгоритм разделяет блок на четыре 16-битных подблока. Каждый раунд получает на входе четыре 16-битных подблока и создает четыре 16-битных выходных подблока. Заключительное преобразование также получает на входе четыре 16-битных подблока и создает четыре 16-битных подблока. Каждый раунд использует шесть 16-битных ключей, заключительное преобразование

использует четыре подключа, т.е. всего в алгоритме используется 52 подключа.

Рис. 3.1. Алгоритм IDEA

Последовательность преобразований отдельного раунда

Рассмотрим последовательность преобразований отдельного раунда.

Одним из основных элементов алгоритма, обеспечивающих диффузию, является структура, называемая MA (умножение/сложение):

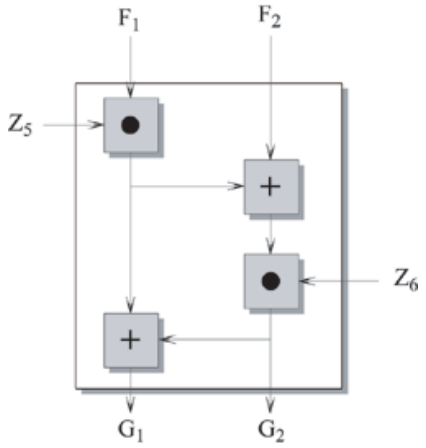

Рис. 3.2. Структура MA (умножение/сложение)

На вход этой структуре подаются два 16-битных значения и два 16-битных подключа, на выходе создаются два 16-битных значения. Исчерпывающая компьютерная проверка показывает, что каждый бит

выхода этой структуры зависит от каждого бита входов незашифрованного блока и от каждого бита подключей. Данная структура повторяется в алгоритме восемь раз, обеспечивая высокоэффективную диффузию.

Раунд начинается с преобразования, которое комбинирует четыре входных подблока с четырьмя подключами, используя операции сложения и умножения. Четыре выходных блока этого преобразования комбинируются, используя операцию XOR для формирования двух 16-битных блоков, которые являются входами MA структуры. Кроме того, MA структура имеет на входе еще два подключа и создает два 16-битных выхода.

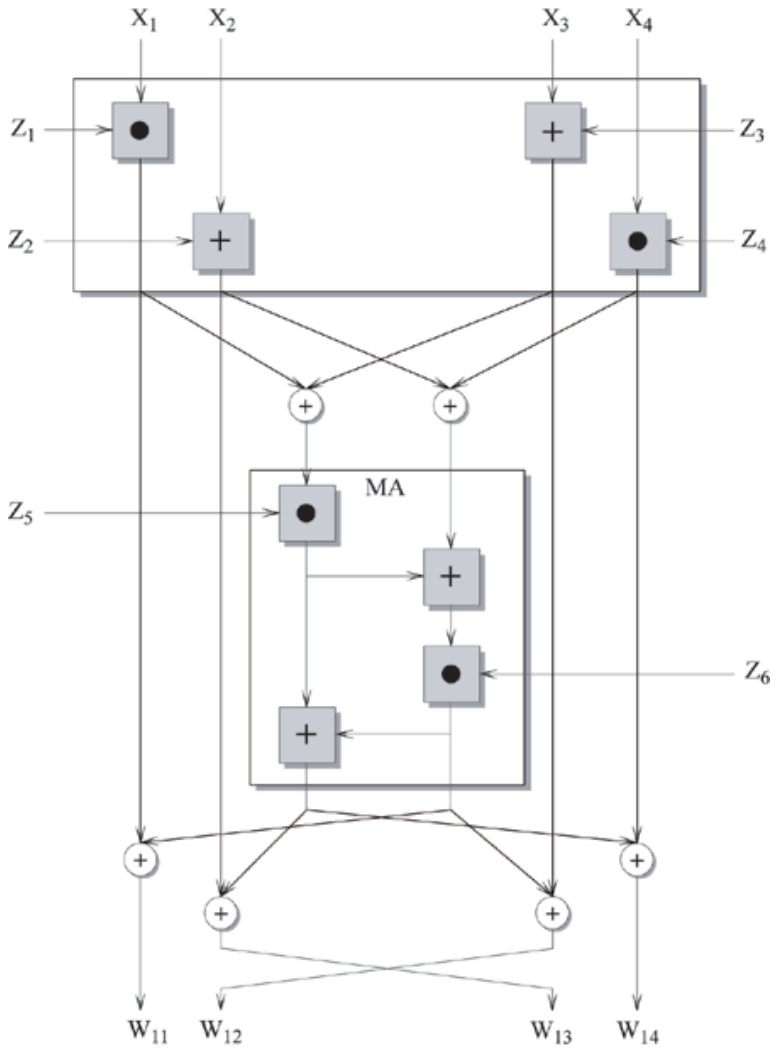

Рис. 3.3. I-ый раунд IDEA

В заключении четыре выходных подблока первого преобразования комбинируются с двумя выходными подблоками MA структуры, используя XOR для создания четырех выходных подблоков данной итерации. Заметим, что два выхода, которые частично создаются вторым и

третьим входами (X_2 и X_3), меняются местами для создания второго и третьего выходов (W_{12} и W_{13}). Это увеличивает перемешивание битов и делает алгоритм более стойким для дифференциального криптоанализа.

Рассмотрим девятый раунд алгоритма, обозначенный как заключительное преобразование. Это та же структура, что была описана выше. Единственная разница состоит в том, что второй и третий входы меняются местами. Это сделано для того, чтобы дешифрование имело ту же структуру, что и шифрование. Заметим, что девятая стадия требует только четыре входных подключа, в то время как для первых восьми стадий для каждой из них необходимо шесть входных подключей.

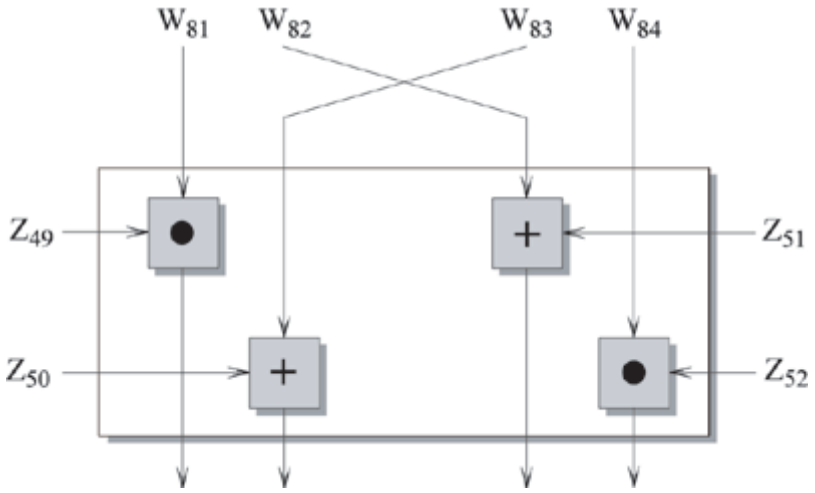

Рис. 3.4. Заключительное преобразование

Создание подключей

Пятьдесят два 16-битных подключа создаются из 128-битного ключа шифрования следующим образом. Первые восемь подключей, которые обозначим как Z_1, Z_2, ..., Z_8, получаются непосредственно из ключа, при этом Z_1 равен первым 16 битам, Z_2 равен следующим 16 битам и т.д. Затем происходит циклический сдвиг ключа влево на 25 битов, и создаются следующие восемь подключей. Эта поцедура повторяется до тех пор, пока не будут созданы все 52 подключа.

Заметим, что каждый первый подключ раунда получен из своего подмножества битов ключа. Если весь ключ обозначить как $Z_{[1..128]}$, то первыми ключами в восьми раундах будут:

$Z_1 = Z_{[1..16]}$ $Z_{25} = Z_{[76..91]}$

$Z_7 = Z_{[97..112]}$ $Z_{31} = Z_{[44..59]}$

$Z_{13} = Z_{[90..105]}$ $Z_{37} = Z_{[37..52]}$

$Z_{19} = Z_{[83..98]}$ $Z_{43} = Z_{[30..45]}$

Хотя на каждом раунде за исключением первого и восьмого используются только 96 битов подключа, множество битов ключа на

каждой итерации не пересекаются, и не существует отношения простого сдвига между подключами разных раундов. Это происходит потому, что на каждом раунде используется только шесть подключей, в то время как при каждой ротации ключа получается восемь подключей.

Дешифрование

Процесс дешифрования аналогичен процессу шифрования. Дешифрование состоит в использовании зашифрованного текста в качестве входа в ту же самую структуру IDEA, но с другим набором ключей. Дешифрующие ключи $U_1, \ldots, U_{52}$ получаются из шифрующих ключей следующим образом:

1. Первые четыре подключа i-ого раунда дешифрования получаются из первых четырех подключей (10-i)-го раунда шифрования, где стадия заключительного преобразования считается 9-м раундом. Первый и четвертый ключи дешифрования эквивалентны мультипликативной инверсии по модулю $(2^{16} + 1)$ соответствующих первого и четвертого подключей шифрования. Для раундов со 2 по 8 второй и третий подключи дешифрования эквивалентны аддитивной инверсии по модулю (2^{16}) соответствующих третьего и второго подключей шифрования. Для раундов 1 и 9 второй и третий подключи дешифрования эквивалентны аддитивной инверсии по модулю (2^{16}) соответствующих второго и третьего подключей шифрования.
2. Для первых восьми раундов последние два подключа i раунда дешифрования эквивалентны последним двум подключам $(9 - i)$ раунда шифрования.

Для мультипликативной инверсии используется нотация Z_j^{-1}, т.е.:

$Z_j \bullet Z_j^{-1} = 1 \bmod (2^{16} + 1)$

Так как $2^{16} + 1$ является простым числом, каждое ненулевое целое $Z_j \leq 2^{16}$ имеет уникальную мультипликативную инверсию по модулю $(2^{16} + 1)$. Для аддитивной инверсии используется нотация $(-Z_j)$, таким образом, мы имеем: $-Z_j + Z_j = 0 \bmod (2^{16})$

Для доказательства того, что алгоритм дешифрования с соответствующими подключами имеет корректный результат, рассмотрим одновременно процессы шифрования и дешифрования. Каждый из восьми раундов разбит на две стадии преобразования, первая из которых называется трансформацией, а вторая шифрованием.

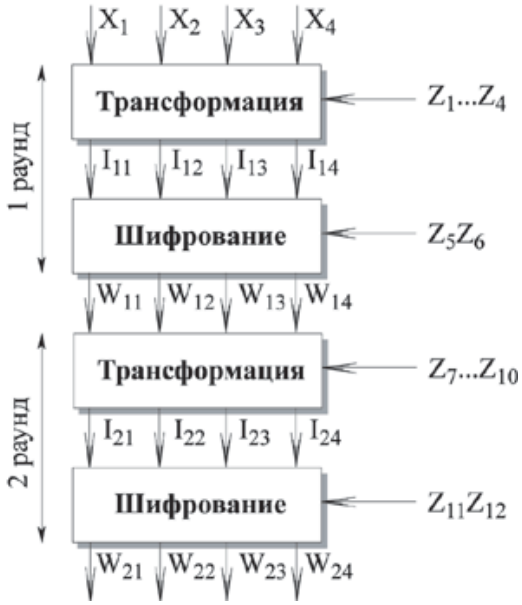

Рис. 3.5. Шифрование IDEA

Рис. 3.6. Дешифрование IDEA

Рассмотрим преобразования, выполняемые в прямоугольниках на обоих рисунках. При шифровании поддерживаются следующие соотношения на выходе трансформации:

$Y_1 = W_{81} \bullet Z_{49}$ $Y_3 = W_{82} + Z_{51}$

$Y_2 = W_{83} + Z_{50}$ $Y_4 = W_{84} \bullet Z_{52}$

Первая стадия первого раунда процесса дешифрования поддерживает следующие соотношения:

$J_{11} = Y_1 \bullet U_1$ $J_{13} = Y_3 + U_3$

$J_{12} = Y_2 + U_2$ $J_{14} = Y_4 \bullet U_4$

Подставляя соответствующие значения, получаем:

$J_{11} = Y_1 \bullet Z_{49}^{-1} = W_{81} \bullet Z_{49} \bullet Z_{49}^{-1} = W_{81}$

$J_{12} = Y_2 + -Z_{50} = W_{83} + Z_{50} = W_{83} + Z_{50} + -Z_{50} = W_{83}$

$J_{13} = Y_3 + -Z_{51} = W_{82} + Z_{51} + -Z_{51} = W_{82}$

$J_{14} = Y_4 \bullet Z_{52}^{-1} = W_{84} \bullet Z_{52} \bullet Z_{52}^{-1} = W_{84}$

Таким образом, выход первой стадии процесса дешифрования эквивалентен входу последней стадии процесса шифрования за исключением чередования второго и третьего блоков. Теперь рассмотрим следующие отношения:

$W_{81} = I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$

$W_{82} = I_{83} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$

$W_{83} = I_{82} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$

$W_{84} = I_{84} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})$

Где $MA_R(X, Y)$ есть правый выход MA структуры с входами X и Y , и $MA_L(X, Y)$ есть левый выход MA структуры с входами X и Y. Теперь получаем

$V_{11} = J_{11} \oplus MA_R (J_{11} \oplus J_{13}, J_{12} \oplus J_{14}) =$

$W_{81} \oplus MA_R(W_{81} \oplus W_{82}, W_{83} \oplus W_{84}) = I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus$

$MA_R[I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{83} \oplus$

$MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}), I_{82} \oplus$

$MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{84} \oplus$

$MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})] = I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus$

$MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) = I_{81}$

Аналогично мы имеем

$V_{12} = I_{83}$

$V_{13} = I_{82}$

$V_{14} = I_{84}$

Таким образом, выход второй стадии процесса дешифрования эквивалентен входу предпоследней стадии процесса шифрования за исключением чередования второго и третьего подблоков. Аналогично можно показать, что

$V_{81} = I_{11}$

$V_{82} = I_{13}$

$V_{83} = I_{12}$

$V_{84} = I_{14}$

Наконец, так как выход трансформации процесса дешифрования эквивалентен первой стадии процесса шифрования за исключением чередования второго и третьего подблоков, получается, что выход всего процесса шифрования эквивалентен входу процесса шифрования.

3.2. Реализации алгоритма шифрования IDEA

В алгоритме IDEA для шифрования применяются 52 субключа, каждый длиной 16 бит. Исходный текст в IDEA делится на четыре группы по 16 бит. Для того чтобы комбинировать 16 битные коды, используется три операции: сложение, умножение и исключающее ИЛИ. Сложение

представляет собой обычную операцию по модулю 65536 с переносом. При составлении таблицы умножения принимаются специальные меры для того, чтобы операция была обратимой. По этой причине вместо нуля используется код 65536. Рассмотрим алгоритм IDEA.

Пусть четыре четверти исходного текста имеют имена A, B, C и D, а 52 субключа - K(1), K(2),., K(52). Перед реализацией алгоритма выполняются операции:

A = A*K(1); B = B + K(2); C = C + K(3); D = D * K(4);

Первый цикл вычислений включает в себя:

E = A XOR C; F = B XOR D

E = E * K(5)

F = F + E

F = F * K(6)

E = E + F

A = A XOR F

C = C XOR F

B = B XOR E

D = D XOR E

Меняем местами B и C.

Повторяем это всё 8 раз, используя K(7) - K(12) для второго раза и, соответственно, K(43) - K(48) - для восьмого. После восьмого раза B и C местами не меняются. Выполняем после этого операции:

A = A * K(49)

B = B + K(50)

C = C + K(51)

D = D * K(52)

В результате закодированный текст имеет ту же длину, что и исходный. Схема этого весьма запутанного алгоритма может быть пояснена на рис. 3.7. По своему характеру алгоритм напоминает процедуры вычисления хэш-функции.

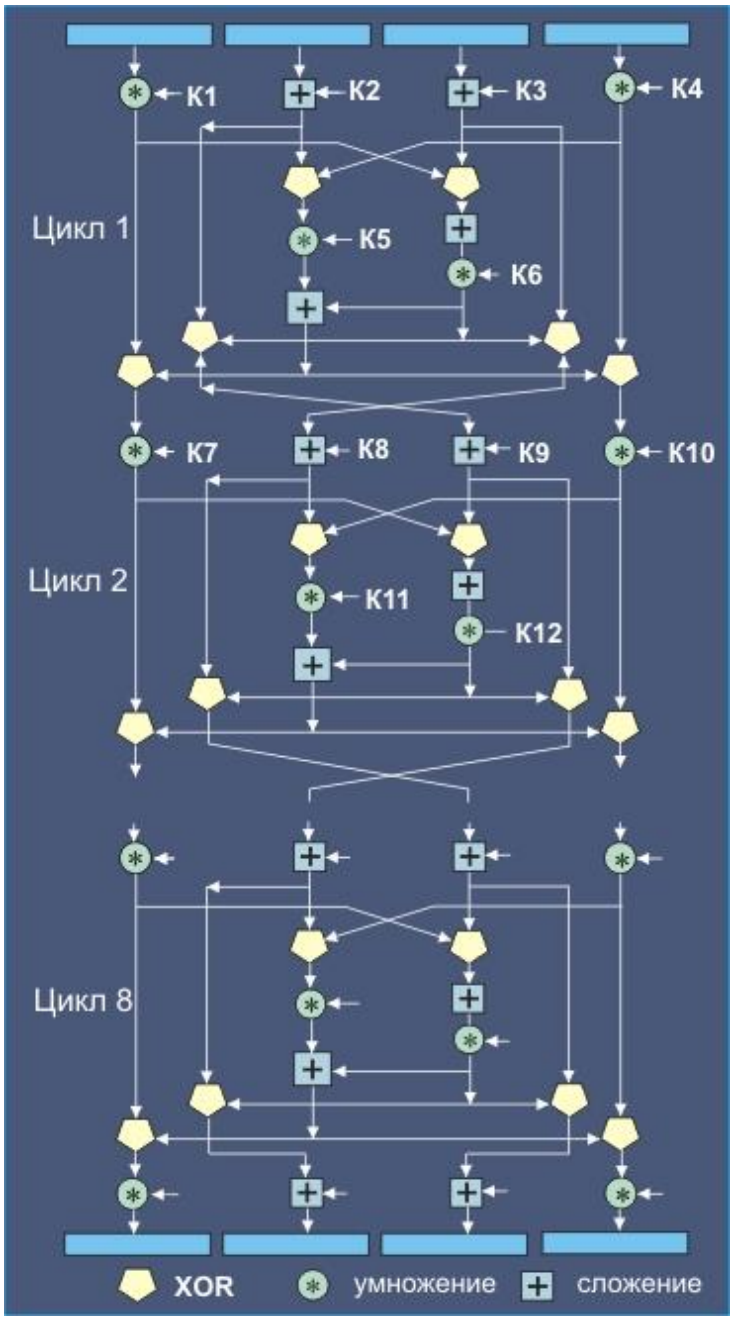

Рис. 3.7. Схема реализации алгоритма шифрования IDEA

При дешифровке используется тот факт, что A XOR B не изменяется, если C A и B будет произведена операция XOR C использованием любого числа. Это утверждение справедливо для любых значений A и B. Операции сложения (слагаемые заменяются их дополнением по модулю 2) и умножения (множители заменяются из обратными величинами по модулю 65537) также допускают инверсию. Первые четыре ключа дешифровки (KD) определяются несколько иначе, чем остальные.

KD(1) = 1/K(49);

KD(2) = -K(50);

KD(3) = -K(51);

KD(4) = 1/K(52);

Последующие операции производятся восемь раз с добавлением 6 к индексу ключей дешифрования и вычитанием 6 из индекса ключей шифрования.

KD(5) = K(47)

KD(6) = K(48)

KD(7) = 1/K(43)

KD(8) = -K(45)

KD(9) = -K(44)

KD(10) = 1/K(46)

Субключи IDEA генерируются следующим образом. 128-битовый ключ IDEA определяет первые восемь субключей (128=8*16). Последующие ключи (44) получаются путем последовательности циклических сдвигов влево этого кода на 25 двоичных разрядов.

3.3. Программа шифрование по алгоритму IDEA

Данная разработанная программа позволяет зашифровать текстов и файлов любого формата по алгоритму IDEA. Программа в основном состоит из двух форм, с которого переключается с помощью кнопок «Текст» и «Файл»:

1. Форма шифрование текстов;
2. Форма шифрование файлов.

Форма шифрование текстов

Данная форма программы позволяет зашифровать тексты или чисел с помощью алгоритма IDEA и состоит из двух основных панелей (рис.3.8):

1. Панель «Шифрование» - этот панель предназначена для установления исходные данные, такие как шифруемые данные и ключ шифрования. В поле «Исходные» вводятся тексты или чисел в шестнадцатеричным системе исчисление. В поле «Зашифрованные» будет отображаться зашифрованные данные по алгоритму IDEA. В поле «Расшифрованные» будет отображаться расшифрованные данные по алгоритму IDEA. В поле «Пароль» устанавливается ключ (пароль) шифрования данных.

2. Панель «Кнопки» - предназначена проводить шифрование и дешифрование данных по алгоритму IDEA и состоит из двух кнопок. При нажатии кнопки «Шифровать» производиться шифрование данных приведенные в поле «Исходные» с помощью ключа установленное в поле «Пароль». При нажатии кнопки «Дешифровать» производиться дешифрование данных приведенные в поле «Зашифрованные» с помощью

ключа установленное в поле «Пароль» и дешифрованные данные переноситься в поле «Расшифрованные».

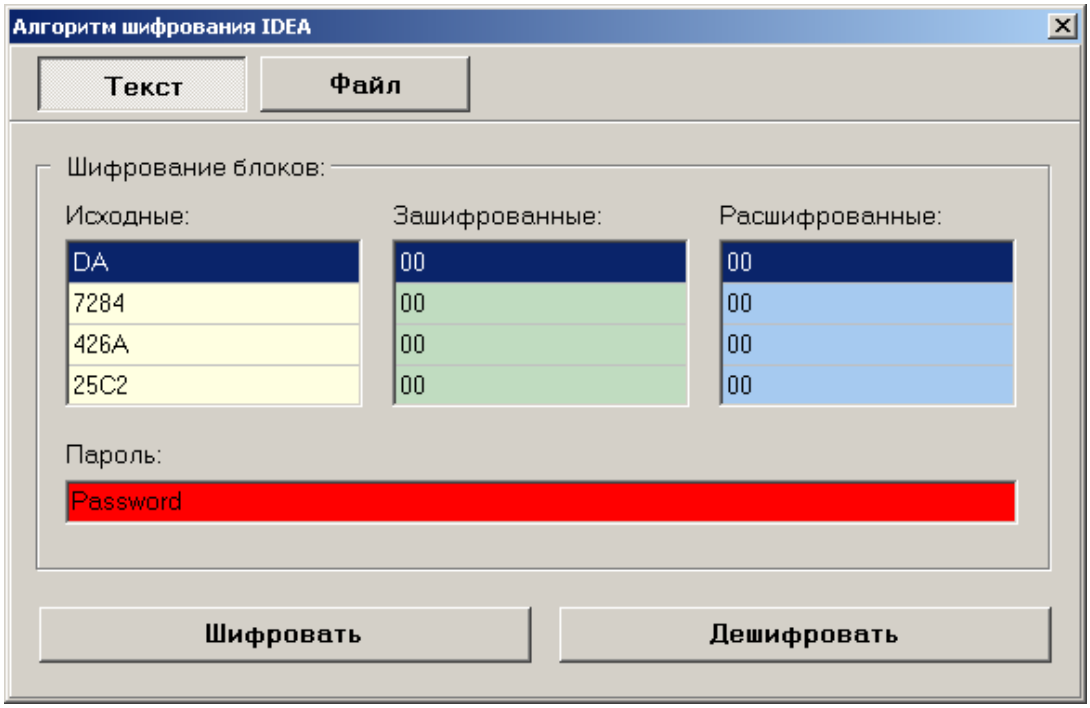

Рис. 3.8. Форма шифрования тестов и чисел.

Форма шифрование файлов

Данная форма программы позволяет нам зашифровать файлы данных любого формата с помощью алгоритма IDEA и состоит из двух основных панелей (рис.3.9):

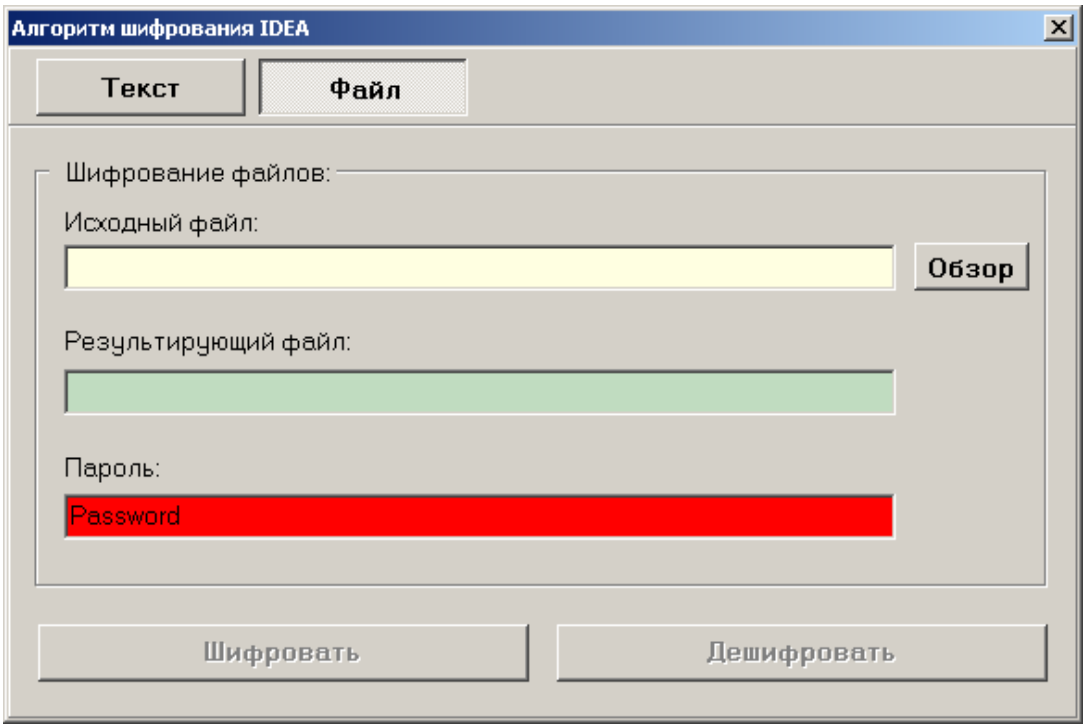

Рис. 3.9. Форма шифрования файлов.

1. Панель «Шифрование» - этот панель предназначена для установления исходные данные, такие как имя файла и его пути для шифрования, имя файла и его пути для создания зашифрованного файла и ключ шифрования. В поле «Исходный файл» вводится имя файла и его путь нахождения в диске или выбирается файл с помощью кнопки «Обзор» для шифрования. В поле «Результирующий файл» вводится имя файла и его путь нахождения в диске для создания зашифрованного файла по алгоритму IDEA. В поле «Пароль» устанавливается ключ (пароль) шифрования данных.

2. Панель «Кнопки» - предназначена проводить шифрование и дешифрование файлов по алгоритму IDEA и состоит из двух кнопок. При нажатии кнопки «Шифровать» производиться шифрование установленного файла в поле «Исходный файл» с помощью ключа установленное в поле «Пароль» и создается новый зашифрованный файл согласно параметрам установленное в поле «Результирующий файл». При нажатии кнопки «Дешифровать» производиться дешифрование файла приведенные в поле «Исходный файл» с помощью ключа установленное в поле «Пароль» и создается другой расшифрованный файл согласно параметрам установленное в поле «Результирующий файл».

Таким образом, с помощью этой программы мы можем зашифровать и расшифровать данные и файлы данных для обеспечения их конфиденциальности.

ЗАКЛЮЧЕНИЕ

В процессе дипломного проектирования были исследованы 15 пакетов абонентского программного обеспечения. В пакетах абонентского программного обеспечения изучались их возможности в операционных средах MS-DOS и MS-Windows, методы настройки, режимы работы, а также простота функционирования. По результатам исследований для каждого пакета абонентского программного обеспечения были даны рекомендации о возможности использования того или иного пакета в глобальной информационной сети работающей на базе протоколов TCP\IP.

Для сравнения пакетов абонентского программного обеспечения между собой и выбора лучшего была написана программа экспертного выбора.

На основании проведенных исследований можно сделать следующие выводы.

Для операционной среды MS-DOS лучшим пакетом абонентского программного обеспечения с точки зрения пользователя является пакет Minuet, разработанный университетом Миннесоты (США). Пакет Minuet обладает полным спектром услуг сети Internet, а также отличным пользовательским интерфейсом. Minuet прост в использовании, может работать как по ЛВС так и по коммутируемым линиям и, самое главное, значительно дешевле своих аналогов. Без сомнения пакет Minuet в настоящее время является лучшим абонентским пакетом для ОС MS-DOS. Он может быть рекомендован практически всем категориям абонентов сети.

Для операционной среды MS-DOS лучшим пакетом абонентского программного обеспечения с точки зрения специалиста является пакет KA9Q. Пакет KA9Q распространяется вместе с исходными текстами и имеет в своем составе весь спектр сетевых услуг, он может быть рекомендован специалистам сети в качестве исходного материала при разработке нового пакета абонентского программного обеспечения.

Для операционной среды MS-Windows лучшим пакетом абонентского программного обеспечения может быть признан пакет Chameleon, являющийся разработкой фирмы NetManage (США). Пакет Chameleon обладает полным набором услуг сети Internet. Кроме этого Chameleon имеет в своем составе NFS-сервер, а также может работать маршрутизатором сети. На сегодняшний день Chameleon может быть признан лучшим пакетом для операционной среды MS Windows. Пакет Chameleon может быть рекомендован тем абонентам сети, которым необходим пакет абонентского программного обеспечения для MS-Windows. Он также может быть рекомендован в качестве маршрутизатора для связи небольшой ЛВС с сетью

Лучшим почтовым пакетом для операционной среды MS-DOS является безусловно пакет MAIL2, разработанный фирмой PC-центр Техно (Россия). Пакет Mail2 обладает отличным пользовательским интерфейсом, прост в настройке и недорог. Он может работать как в ЛВС, так и по коммутируемым линиям. Он может рекомендоваться всем категориям пользователей сети.

Лучшим почтовым пакетом для операционной среды MS-Windows можно считать пакет DMail for Windows, разработанный фирмой Демос (Россия). Пакет DMail может быть рекомендован к использованию тем абонентам, которые нуждаются в электронной почте и привыкли работать в среде Windows.

Лучшим пакетом для наиболее полного использования информационных ресурсов сети Internet является пакет Mosaic, разработанный NCSA (National Centre of Supercomputing Applications) США. Mosaic - наиболее мощный инструмент для путешествия по сети Internet. С помощью Mosaic пользователи могут получать доступ к гипертекстовым библиотекам WWW, к обычным базам данных сети Internet и системам поиска информации в них.

В ходе дипломного пректирования для пакетов Minuet, Mail2 и были разработаны инструкции по установке и эксплуатации данных пакетов абонентского программного обеспечения. Пакеты Chameleon и Dmail продаются вместе с полным комплектом фирменной документации, пакет Mosaic распространяется свободно вместе с довольно полной документацией.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Браун С. “Мозаика” и “Всемирная паутина” для доступа к Internet: Пер. с англ. - М.: Мир: Малип: СК Пресс, 1996. - 167с.
2. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: "Единая Европа", 1994. - 264 с.
3. Гилстер П. Новый навигатор Internet: Пер с англ. -Киев: Диалектика, 1996. - 495 с.
4. Игер Б. Работа в Internet / Под ред. А. Тихонова; Пер. с англ. - М.: БИНОМ, 1996. - 313 с.
5. Кент П. Internet / Пер. с англ. В.Л. Григорьева. - М.: Компьютер, ЮНИТИ, 1996. - 267 с.
6. Колесников О.Э. Интернет для делового человека. - М.: МЦФ. Издат. фирма “Яуза”, 1996. - 281 с.
7. Крол Эд. Все об Internet: Руководство и каталог / Пер. с англ. С.М. Тимачева. - Киев: BNV, 1995. 591 с.
8. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование. - 1994. - N5. - С. 5-16.
9. Нольден М. Ваш первый выход в Internet: Для начинающих пльзователей Internet и широкого круга пользователей PC / Гл. ред. Е.В. Кондукова; Пер с нем. К.А. Шиндер. - Спб.: ИКС, 1996. - 238 с.
10. Продукты года // LAN - русское издание. - апрель 1995. - том 1. - номер 1. - С. 6-25.

11. Об информации, информатизации и защите информации: Федеральный Закон // Российская газета. - 1995. - 22 февраля. - С. 4.
12. Фролов А.В., Фролов Г.В. Глобальные сети компьютеров. Практическое введение в Internet, E-mail, FTP, WWW, и HTML, программирование для Windiws Sockets. - Диалог - МИФИ, 1996. - 283 с.
13. Хоникат Д. Internet Windows 95: Руководство пользователя / Пер. с англ. В. Неклюдова. - М.: БИНОМ, 1996. - 334 с.
14. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. - Addison-Wesley, 1994. - 275 с.
15. An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994. - 310 с.