Защита информации в Internet.

Содержание.

1. Введение.

2. Проблемы защиты информации.

3. Защита Web-серверов:

3.1 Ограничение доступа в WWW-серверах.

3.2 WWW-сервер и проблемы безопасности.

3.3 Java, Javascript и проблемы безопасности.

4. Заключение.

5. Специальные термины.

6. Список литературы.

1.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 распределенного 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 "коммерциализация" сети (80-90% средств поступает из частного сектора).

2. Проблемы защиты информации

 Internet и информационная безопасность несовместны по самой природе Internet. Она родилась 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.

 Бурный рост Internet вместе с существенным набором новых возможностей и услуг приносит и ряд новых проблем, наиболее неприятной из которых, безусловно является проблема безопасности. Даже беглый анализ компьютерной прессы показывает, что проблема безопасности и сохранности информации, помещаемой в Internet или во внутренние корпоративные Intranet-системы, стоит достаточно остро. Поэтому неудивительно, что все компании-производители ПО для Internet вводят в свои продукты все более совершенные средства защиты информации.

 Что же определяет бурный рост Internet, характеризующийся ежегодным удвоением числа пользователей? Ответ прост - “халява”, то есть 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.

 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.

 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.

 Что же может произойти с вашей информацией, если не заботиться о ее безопасности ?

Во-первых, это утрата конфиденциальности.

Ваша личная информация может остаться в целостности, но конфиденциальна больше не будет, например кто-нибудь в Интернете получит номер вашей кредитной карточки.

Во-вторых, это Модификация.

Ваша информация будет модифицирована, например ваш заказ в on-line магазине или ваше резюме.

В-третьих, подмена информации, которая может быть 2 типов.

1)WWW сервер может выдавать себя за другой, каковым он не является.

2)WWW сервер может действительно существовать под этим именем и заявлять, например, что это online магазин, но в действительности никогда не посылать никаких товаров, а только собирать номера кредитных карточек.

 Атака на информацию может быть совершена несколькими путями.

Во-первых, это атака на систему клиента со стороны сервера.

Хакер, у которого есть свой WWW сервер, может постараться при помощи Java некорректных апплетов и JavaScript приложений, встроенных в HTML документ, вывести из строя пользовательскую систему, или получить информацию о ней, которая позволит ему взломать машину пользователя.

Во-вторых, атака на сервер со стороны клиента.

Хакер может через www клиента может попытаться вывести пользовательскую систему или www сервер из строя, или получить доступ к информации, доступа к которой у него нет. Для этого он может использовать дырки в безопасности в CGI приложениях, плохую настройку сервера, попытаться подменить CGI приложение.

И наконец, информация может быть украдена третьей стороной при ее передаче.

 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 на сто процентов.

 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.

3.ЗАЩИТА WEB-СЕРВЕРОВ

 Сервер Web организации обеспечивает ее присутствие в Internet. Однако распространяемые этим сервером данные могут содержать сведения частного характера, не предназначенные для чужих глаз. К сожалению, серверы Web представляют собой лакомую приманку для злоумышленников. Широкую огласку получили случаи "нападения" на серверы Министерства юстиции и даже ЦРУ: злоумышленники подменяли домашние страницы этих организаций на непристойные карикатуры. Поборники прав животных проникли на сервер Kriegsman Furs и заменили домашнюю страницу ссылкой на узлы, посвященные защите братьев наших меньших. Схожая судьба постигла серверы Министерства юстиции США, ЦРУ, Yahoo! и Fox. Дэн Фармер, один из создателей программы SATAN, для поиска брешей в защите сетей использовал еще не завершенную официально версию своего сканера для зондирования Web-серверов Internet и установил, что почти две трети из них имеют серьезные изъяны в защите.

 Очевидно, что серверы Web защищены далеко не так надежно, как хотелось бы. В некоторых простых случаях все дело в незаметных, но небезопасных огрехах в сценариях CGI. В других ситуациях угрозу представляет недостаточная защита операционной системы хоста.

 Простейший способ укрепить защиту сервера Web состоит в размещении его за брандмауэром. Однако, действуя таким образом, пользователь как бы переносит проблемы защиты во внутрикорпоративную сеть, а это не самый удачный выход. Пока сервер Web располагается "по другую сторону" брандмауэра, внутренняя сеть защищена, а сервер - нет. Побочным эффектом от такого шага является усложнение администрирования сервера Web.

 Лучшим выходом было бы компромиссное решение: размещение сервера Web в его собственной сети, запрет внешних соединений или ограничение доступа к внутренним серверам.

 Наряду с обеспечением безопасности программной среды, 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).

**3.1. 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: Агентство 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

Рисунок 2.2.7 Пример списка вестников издательства.

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

Рисунок 2.2.8

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

Рисунок 2.2.9 Окно неправильного ввода пароля.

**3.2 World wide web серверы и проблема безопасности информации.**

Среди WWW серверов отличаются отсутствием известных проблем с безопаcностью Netscape серверы, WN и apache.

WN сервер.

 Это свободно распространяемый сервер, доступный для множества UNIX платформ. Основными целями при его создании были безопасность и гибкость. WN сервер содержит в каждой директории маленькую базу данных (список) документов содержащихся в ней. Если документ не перечислен в базе данных, клиент получить его не может. Базы данных либо генерируется специальной программой автоматически для всех файлов в дереве директорий, либо другой программой создаются из текстовых описаний, которые создаются вручную. В эти файлы, кроме перечисления документов можно вставлять HTML текст, т.к это аналог index.html в этом сервере.

 Администратору web узла разбираться в сгенерированных файлах особой необходимости нет, но в принципе они аналогичны .cache файлам gopher. Сам сервер имеет разновидность для одновременной обработки gopher и http запросов к одним и тем же документам.

 Безопасность выполнения CGI приложений обеспечивается выставлением uid/gid для нужного файла этой базы данных. Безо всякого программирования и особой настройки WN сервер обеспечивает 8 возможностей поиска внутри документов, имеет интерфейс к WAIS серверу. Вы можете включать одни документы внутрь других на серверной стороне (например стандартные сообщения вначале и в конце документа ) Можете применять фильтры к любому документу, для получения необходимого документа на выходе ( например подстановка слов ). Для обращения к документу можно использовать URL типа <http://host/dir/foo;lines=20-30, чтобы получить строки с 20 по 30. Документация к серверу очень хорошая, устанавливается он быстро, обнаруженные ошибки исправляются в течении нескольких дней.

 Apache сервер - это свободно распространяемый WWW сервер для различных UNIX платформ и Windows NT, один из самых популярных в мире. Сейчас apache работает на 36 процентах от общего количества всех HTTP серверов в мире. Это быстрый и стабильный сервер. В сервер можно встроить SSL протокол, рассмотренный ниже на примере Netscape сервера.

Netscape Enterprise сервер.

Netscape Enterprise Server - это высокопроизводительный, защишенный World Wide Web сервер для создания, распространения, публикации информации в Интернете и выполнения сетевых интернетовских приложений, используя средства, базирующиеся на языках Java и JavaScript.

Netscape FastTrack сервер.

Netscape FastTrack сервер - это решение для тех, кого не устраивает цена и сложность Netscape Enterprise сервера. Он прост в использовании, разработанного чтобы позволить новичкам создавать и администрировать WWW сервер.

 Серверы Netscape имеют встроенные средства безопасности коммерческой информации и коммуникаций. Гибкая авторизация пользователя контролирует доступ к отдельным файлам и директориям, используя имя пользователя и пароль, имя домена, имя машины, IP адрес, клиентские сертификаты (client-side certificates ), именованные группы. Дополнительные черты безопасности обеспечиваются протоколом Secure Socket Layer 3.0 (SSL 3.0) и механизмом открытых ключей.

 SSL 3.0 - это последняя версия широко распространенного в Интернете стандарта, разработанного Netscape Communications corporation.

 SSL протокол обеспечивает конфиденциальность, целостность и аутентичность информации.

 Конфиденциальность и целостность информации обеспечивается посредством шифрования с открытым ключом. Аутентификация обеспечивается посредством цифровых сертификатов, которые почти невозможно подделать. Сертификат необходимо получать от третьей стороны, которой обе стороны доверяют.

SSL протокол - это схема шифрования низкого уровня, используемая для шифрования транзакций в протоколах высокого уровня, таких как HTTP, NNTP и FTP. SSL протокол содержит методы для идентификации сервера для клиента, шифрование данных при передаче и дополнительно, верификации клиента для сервера. Из коммерческих систем SSL протокол сейчас реализован в Netscape навигаторах и Netscape серверах. ( Реализованы шифрование данных и авторизация сервера, авторизация клиента нет).

 Существует также свободно распространяемая версия SSL, называемая SSLeay. Она содержит исходный код на C, который может быть встроен в такие приложения, как Telnet и FTP. Поддерживаются также свободно распространяемые Unix Web серверы Apache и NCSA httpd и несколько Web клиентов, включая Mosaic. Этот пакет может быть использован бесплатно для коммерческих и некоммерческих приложений.

Механизм открытых ключей обеспечивает шифрование данных при помощи открытого ключа(public key). В традиционных системах шифрования один и тот же ключ использовался для шифрования и дешифрования. В новом открытом или асимметричных системах шифрования ключи идут парами: один ключ используется для кодирования, другой для декодирования. Один из этих ключей, называемый открытым ключом, свободно распространяемый и используется для кодирования сообщений. Другой ключ, называемый личным ключом (private key) засекречен и используется для декодирования поступающего сообщения. В этой системе пользователь, посылающий сообщение второму пользователю может зашифровать сообщение открытым ключом второго пользователя.

 Сообщение может дешифровано владельцем секретного личного ключа второго пользователя. Эта система может быть использована для создания неподделываемых цифровых подписей. В Netscape Enterprise Server администраторы могут динамически изменять ключи для сервера, что позволяет оперативно изменять политику авторизации.

 Netscape серверы и навигаторы осуществляют шифрование используя или 40-битный ключ или 128-битный ключ. В принципе можно взломать 40-битный ключ, перебирая каждую возможную комбинацию ( всего 2^40 ) пока Вы не обнаружите, что сообщение расшифровано. Взломать 128 битный ключ практически нереально.

**3.3.Java, JavaScript и проблема безопасности.**

Java и JavaScript - это тот раздел безопасности Web, который касается не администраторов и создателей Web серверов, а пользователей и администраторов пользовательских сетей.

 Несмотря на сходство в именах Java и JavaScript это две различных продукта. Java - это язык программирования разработанный SunSoft. Java программы прекомпилируются в компактную форму и хранятся на сервере. HTML документы могут ссылаться на миниприложения, называемые Java аплетами. WWW клиенты, которые поддерживают Java апплеты, загружают откомпилированные Java приложения и выполняют их на машине клиента. JavaScript это набор расширений к HTML, интерпретируемых WWW клиентом. В принципе, несмотря на то что JavaScript имеет более длинную историю проблем, связанных с безопасностью, хакерская программа на Java может активно и успешно вывести пользовательскую систему из строя, про JavaScript до сих пор известны только случаи передачи конфиденциальной информации клиента на Web сервер. Java апплеты выполняются на клиентской стороне, а не на серверной, и поэтому увеличивают риск атаки со стороны сервера. Нужно ли беспокоится об этом ?

 В Java встроены средства для ограничения доступа к клиентской машине. Апплетам не разрешается выполнять системные команды, загружать системные библиотеки, или открывать системные устройства, такие как диски. Апплетам, в зависимости от WWW клиента или запрещены все дисковые операции ( Netscape ), или почти все ( HotJava ).Апплетам разрешается устанавливать соединение по сети только к серверу, откуда аплет был загружен. Но Drew Dean ( ddean@cs.princenton.edu ) обнаружил, что можно написать апплет, который будет устанавливать соединение к любому компьютеру в интернете, то есть аплет из Интернета, загруженный на вашу локальную машину WWW клиентом может подсоединиться по TCP/IP к любой машине на вашей локальной сети, даже если она защищена через firewall. Эта проблема связана с тем, что Java выполняет верификацию для соединения через Domain.

Name System (DNS). Взломщик используя свой собственный DNS сервер может создать некорректную ссылку в DNS, чтобы заставить Java систему считать, что апплету разрешено соединение с компьютером к которому у него нет права подсоединяться. Ошибка была исправлена в Netscape навигаторе 2.01 и JDK 1.0.1.

 David Hopwood обнаружил, что загружая апплеты с 2 разных WWW серверов хэкер может нарушить пространство имен Java Virtual Machine. Это позволяет преобразовывать типы переменных друг в друга, преобразовывать целые в ссылки и т.д. В результате апплет может читать и писать локальные файлы, выполнять машинный код. Безо всяких проблем в UNIX может быть создан файл .rhosts. Эта ошибка проявляется, как минимум на HotJava, код может быть написан целиком на Java и быть платформонезависимым.

В настоящих версиях Java возможны трюки с вызовом конструктора суперкласса, в результате чего этот вызов может быть пропущен. Это связано с алгоритмом, который сейчас использует интерпретатор Java. Возможные пути для этого:

-super внутри try.

-super внутри if.

-cathcer/thrower.

JavaScript - это встроен в Netscape навигатор. Периодически в Netscape навигаторе обнаруживались проблемы с безопасностью в связи с JavaScript, которые Netscape периодически устраняет в новых версиях навигатора. Andy Augustine в своем JavaScript FAQ описывает следующие проблемы: 1)Чтение пользовательской истории URL - исправлено в Netscape 2.0.

2)Чтение пользовательского кэша URL - исправлено в Netscape 2.0.

3)Чтение пользовательского e-mail адреса и передача его по Интернету исправлено в Netscape 2.01.

4)Получение рекурсивного оглавления файловой системы - исправлено в Netscape 2.01.

5)Открытие окна размером 1 пиксел, получение URL открытых документов и передача их удаленному серверу. Эта общая проблема сетевых графических систем, имеющая длинную историю. Пользователи x-windows, которые запускают команду `xhost +` без аргументов могут столкнуться с чужим невидимым окошком, которое передает ввод пользователя по Интернету хакеру.

Для того чтобы работать с Java и JavaScript приложениями без проблем с безопасностью рекомендуется:

-Не пользоваться старыми версиями WWW клиентов, которые поддерживают Java и JavaScript. Производители web клиентов исправляют свои программы, если обнаруживается новая ошибка в безопасности.

-Следить за текущим состоянием дел с безопасностью Java и Javascript. Javasoft имеет страницу, посвященную Java и безопасности. У netscape есть аналогичная страница про JavaScript. Каждый производитель web клиента имеет на своем сервере страницу посвященную безопасности.

В заключение несколько общих правил, которые помогут Вам избежать многих проблем.

1.При создании web сервера используйте надежный продукт. Используйте web сервер, который подходит под ваши нужды, не обязательно самый всеобъемлющий и модный.

2.Читайте документацию сервера. Недостатки в настройке чаще создают проблемы с безопасностью нежели ошибки в самом сервере.

3.Не забывайте про SSL протокол, если речь идет о коммерческой информации.

4.Заботьтесь о безопасности CGI приложений, так как это части самого сервера. Не забывайте проверять и чужие CGI приложения, если у Вас многопользовательский сервер.

5.Не пользуйтесь старыми версиями Web клиентов с поддержкой Java и JavaScript. Следите за обновлениями.

**4.Заключение.**

 В данной работе мною были рассмотрены проблемы защиты информации в глобальной сети Internet. Проблема эта была и остается актуальной по сей день, так как никто еще не может гарантировать на сто процентов того, что ваша информация будет защищена или в ваш компьютер не попадет вирус. Актуальность этой проблемы подтверждает еще и то, что ей посвещено огромное количество страниц в Internet. Однако большая часть информации идет на английском языке, что затрудняет работу с ней. Разумеется в данной работе рассмотрена лишь часть проблемы (не рассмотрена, например, защита информации при помощи брандмауэров(сетевых экранов)). Проведенные исследования показывают, что разработано множество способов защиты информации: разграничение доступа, защита при помощи паролей, шифрование данных и.т.п. Однако, несмотря на все это, до сих пор мы то и дело слышим о взломах хакерами различных серверов и компьютерных систем. Это говорит о том, что проблема защиты информации еще не решена и на ее решение будет потрачено множество сил и времени.

**5. Список специальных терминов**

ARP (Address Resolution Protocol) - протокол определения адреса, преобразует адрес компьютера в сети Internet в его физический адрес.

ARPA (Advanced Research Projects Agency) - бюро проектов передовых исследований министерства обороны США.

Ethernet - тип локальной сети. Хороша разнообразием типов проводов для соединений, обеспечивающих пропускные способности от 2 до 10 миллионов bps(2-10 Mbps). Довольно часто компьютеры, использующие протоколы TCP/IP, через Ethernet подсоединяются к Internet.

FTP (File Transfer Protocol) - протокол передачи файлов, протокол, определяющий правила пересылки файлов с одного компьютера на другой.

FAQ (Frequently Asked Qustions) - часто задаваемые вопросы. Раздел публичных архивов сети Internet в котором хранится информация для "начинающих" пользователей сетевой инфраструктуры.

Gopher - интерактивная оболочка для поиска, присоединения и использования ресурсов и возможностей Internet. Интерфейс с пользователем осуществлен через систему меню.

HTML (Hypertext Markup Language)- язык для написания гипертекстовых документов. Основная особенность - наличие гипертекстовых связей между документами находящимися в различных архивах сети; благодаря этим связям можно непосредственно во время просмотра одного документа переходить к другим документам.

Internet - глобальная компьютерная сеть.

IP (Internet Protocol) - протокол межсетевого взаимодействия, самый важный из протоколов сети Internet, обеспечивает маршрутизацию пакетов в сети.

IР-адрес - уникальный 32-битный адрес каждого компьютера в сети Internet.

Telnet - удаленный доступ. Дает возможность абоненту работать на любой ЭВМ сети Internet как на своей собственной.

TCP\IP - под TCP\IP обычно понимается все множество протоколов поддерживаемых в сети Internet.

TCP (Transmission Control Protocol) - протокол котроля передачи информации в сети. TCP - протокол транспортного уровня, один из основных протоколов сети Internet. Отвечает за установление и поддержание виртуального канала (т.е. логического соединения), а также за безошибочную передачу информации по каналу.

UDP (User Datagram Protocol) - протокол транспортного уровня, в отличие от протокола TCP не обеспечивает безошибочной передачи пакета.

Unix - многозадачная операционная система, основная операционная среда в сети Internet. Имеет различные реализации: Unix-BSD, Unix-Ware, Unix-Interactive.

UUCP - протокол копирования информации с одного Unix-хоста на другой. UUCP - не входит в состав протоколов TCP/IP, но тем не менее все-еще широко используется в сети Internet. На основе протокола UUCP - построены многие системы обмена почтой, до сих пор используемые в сети.

WWW (World Wide Web) - всемирная паутина. Система распределенных баз данных, обладающих гипертекстовыми связями между документами.

**6.Список литературы.**

1.Http://www.lanmag.ru/

2. Игер Б. Работа в Internet / Под ред. А. Тихонова; Пер. c англ. - М.: БИНОМ, 1998. - 313 c.

3.LAN/NetworkSolutionMagazine #7-8 1998.

4. Левин В.К. Защита информации в информационно-вычислительных cистемах и сетях // Программирование. - 1994. - N5. - C. 5-16.