МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Хакасский государственный университет им. Н. Ф. Катанова»
Колледж педагогического образования, информатики и права

ПЦК естественнонаучных дисциплин, математики и информатики

РЕФЕРАТ

на тему:

Система защиты информации в интернете

Автор реферата: _____ Найденова В. Ю.
(подпись) (инициалы, фамилия)

Специальность: 09.02.03 - Программирование в компьютерных системах

Курс: II
Группа: И-21
Зачет/незачет:_____

Руководитель: _____ Когумбаева О. П.
(подпись, дата) (инициалы, фамилия)

г. Абакан, 2015 г.

Содержание

Введение

Интернет - глобальная компьютерная сеть, охватывающая весь мир. Интернет 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.

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

Фактически интернет состоит из множества локальных и глобальных сетей, принадлежащих различным компаниям и предприятиям, связанных между собой различными линиями связи. В архивах свободного доступа сети интернет можно найти информацию практически по всем сферам человеческой деятельности, начиная с новых научных открытий до прогноза погоды на завтра.

Кроме того, интернет предоставляет уникальные возможности дешевой, надежной и конфиденциальной глобальной связи по всему миру.

В настоящее время интернет испытывает период подъема, во многом благодаря активной поддержке со стороны правительств европейских стран и США.

Целью данной работы стало изучение видов защиты информации в интернете, терминологию в данной предметной области.

Задачи данной работы:

1. Виды информации в интернете

2. Изучить способы и проблемы размещения информации в интернете

3. Способы защиты web-серверов и информации в интернете
4. Принцип достаточности защиты
5. World wide web серверы и проблема безопасности информации

1. Виды информации в интернете

Основные виды информации по ее форме представления, способам ее кодирования и хранения, что имеет наибольшее значение для информатики, это:

- Графическая или изобразительная — первый вид, для которого был реализован способ хранения информации об окружающем мире в виде наскальных рисунков, а позднее в виде картин, фотографий, схем, чертежей на бумаге, холсте, мраморе и др. материалах, изображающих картины реального мира;
- звуковая— мир вокруг нас полон звуков и задача их хранения и тиражирования была решена с изобретение звукозаписывающих устройств в 1877 г ее разновидностью является музыкальная информация — для этого вида был изобретен способ кодирования с использованием специальных символов, что делает возможным хранение ее аналогично графической информации;
- текстовая— способ кодирования речи человека специальными символами — буквами, причем разные народы имеют разные языки и используют различные наборы букв для отображения речи; особенно большое значение этот способ приобрел после изобретения бумаги и книгопечатания;
- числовая — количественная мера объектов и их свойств в окружающем мире; особенно большое значение приобрела с развитием торговли, экономики и денежного обмена; аналогично текстовой информации для ее отображения используется метод кодирования специальными символами — цифрами, причем системы кодирования (счисления) могут быть разными;
- видеоинформация — способ сохранения «живых» картин окружающего мира, появившийся с изобретением кино.

Существуют также виды информации, для которых до сих пор не изобретено способов их кодирования и хранения — это тактильная

информация, передаваемая ощущениями, органолептическая, передаваемая запахами и вкусами и др.

2.Проблемы защиты информации

Интернет и информационная безопасность несовместны по самой природе интернет. Как известно, чем проще доступ в Сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в интернете - 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.

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

Во-первых, ликвидировать физическую связь между будущей интеренет (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

интернет, 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.

В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью.

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.

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).

4. Способы защиты информации в интернете

Проведение финансовых операций с использованием Интернета, заказ товаров и услуг, использование кредитных карточек, доступ к закрытым информационным ресурсам, передача телефонных разговоров требуют обеспечения соответствующего уровня безопасности.

Конфиденциальная информация, которая передается по сети Интернет, проходит через определенное количество маршрутизаторов и серверов, прежде чем достигнет пункта назначения. Обычно маршрутизаторы не отслеживают проходящие сквозь них потоки информации, но возможность того, что информация может быть перехвачена, существует. Более того, информация может быть изменена и передана адресату в измененном виде. К сожалению, сама архитектура сети Интернет всегда оставляет возможность для недобросовестного пользователя осуществить подобные действия.

Всегда существует проблема выбора между необходимым уровнем защиты и эффективностью работы в сети. В некоторых случаях пользователями или потребителями меры по обеспечению безопасности могут быть расценены как меры по ограничению доступа и эффективности. Однако такие средства, как, например, криптография, позволяют значительно усилить степень защиты, не ограничивая доступ пользователей к данным.

4.1.Принципы защиты информации

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на четыре основных типа:

перехват информации - целостность информации сохраняется, но ее конфиденциальность нарушена;

модификация информации - исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;

подмена авторства информации;

перехват сообщения с его изъятием.

Данная проблема может иметь серьезные последствия.

В соответствии с перечисленными проблемами при обсуждении вопросов безопасности под самим термином "безопасность" подразумевается совокупность трех различных характеристик обеспечивающей безопасность системы:

Аутентификация - это процесс распознавания пользователя системы и предоставления ему определенных прав и полномочий. Каждый раз, когда заходит речь о степени или качестве аутентификации, под этим следует понимать степень защищенности системы от посягательств сторонних лиц на эти полномочия.

Целостность - состояние данных, при котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях различных воздействий. В частности, в случае передачи данных под целостностью понимается идентичность отправленного и принятого.

Секретность - предотвращение несанкционированного доступа к информации. В случае передачи данных под этим термином обычно понимают предотвращение перехвата информации.

4.2.Криптография

Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа.

В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм - это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Зашифрованное послание может быть интерпретировано только с помощью ключа.

Очевидно, чтобы зашифровать послание, достаточно алгоритма. Однако использование ключа при шифровании предоставляет два существенных преимущества. Во-первых, можно использовать один алгоритм с разными ключами для отправки посланий разным адресатам. Во-вторых, если секретность ключа будет нарушена, его можно легко заменить,

не меняя при этом алгоритм шифрования. Таким образом, безопасность систем шифрования зависит от секретности используемого ключа, а не от секретности алгоритма шифрования. Многие алгоритмы шифрования являются общедоступными.

Количество возможных ключей для данного алгоритма зависит от числа бит в ключе.

Поскольку столь важное место в системах шифрования уделяется секретности ключа, то основной проблемой подобных систем является генерация и передача ключа. Существуют две основные схемы шифрования: симметричное шифрование (его также иногда называют традиционным или шифрованием с секретным ключом) и шифрование с открытым ключом (иногда этот тип шифрования называют асимметричным).

При симметричном шифровании отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные. При симметричном шифровании используются ключи небольшой длины, поэтому можно быстро шифровать большие объемы данных. Симметричное шифрование используется, например, некоторыми банками в сетях банкоматов. Однако симметричное шифрование обладает несколькими недостатками. Во-первых, очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей. Во-вторых, для каждого адресата необходимо хранить отдельный секретный ключ. В третьих, в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом.

В схеме шифрования с открытым ключом для шифрования послания используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго - расшифровывается. Таким образом, требуемой безопасности можно добиться, сделав первый ключ общедоступным (открытым), а второй ключ хранить только у получателя

(закрытый, личный ключ). В таком случае любой пользователь может зашифровать послание при помощи открытого ключа, но расшифровать послание способен только обладатель личного ключа. При этом нет необходимости заботиться о безопасности передачи открытого ключа, а для того чтобы пользователи могли обмениваться секретными сообщениями, достаточно наличия у них открытых ключей друг друга.

Недостатком асимметричного шифрования является необходимость использования более длинных, чем при симметричном шифровании, ключей для обеспечения эквивалентного уровня безопасности, что сказывается на вычислительных ресурсах, требуемых для организации процесса шифрования.

4.3.Электронная цифровая подпись

Даже если послание, безопасность которого мы хотим обеспечить, должным образом зашифровано, все равно остается возможность модификации исходного сообщения или подмены этого сообщения другим. Одним из путей решения этой проблемы является передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют контрольной суммой, или дайджестом сообщения.

Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений. Алгоритмы расчета контрольных сумм разработаны так, чтобы они были по возможности уникальны для каждого сообщения. Таким образом, устраняется возможность подмены одного сообщения другим с сохранением того же самого значения контрольной суммы.

Однако при использовании контрольных сумм возникает проблема передачи их получателю. Одним из возможных путей ее решения является включение контрольной суммы в так называемую электронную подпись.

При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим

определенные права отправителем. Электронные цифровые подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число - порядковый номер. олее подробно о электронной цифровой подписи (ЭЦП) читайте в разделе курса ОСВМ Аутентификация информации

С 2012 года в Казахстане функционирует свой Национальный удостоверяющий центр, в котором граждане и организации Казахстана могут получить свои закрытые ключи и программные пакеты для формирования своей цифровой подписи для ведения электронных юридических операций с ее использованием. Необходимо, однако, заметить, что данная система еще очень сырая и позволяет злоумышленникам легко воспользоваться чужой электронной подписью для совершения подложных сделок. Это происходит по следующим причинам: выдача файлов электронных подписей совершается "вручную", то есть оператор, выдающий подпись всегда может иметь ее копию на своем USB-носителе, пароль выдается на всех один (!!!) - 123456. При попытке смены пароля файл электронной подписи записанный на стираемом носителе, фатально повреждается, и, если владелец подписи не сделал предварительно копию, то он лишается возможности подписывать документы до получения новой подписи из НУЦ, ЦОН или у программистов районного налогового комитета.

На сегодня уже известно множество фиктивных сделок с недвижимостью и иным имуществом, а также незаконным получением документов с помощью чужой электронной подписи. Поэтому, единственно разумным действием, предохраняющим человека от лишения его собственности, является безусловный отказ от получения ЭЦП, а если таковая уже получена, то подача заявления о ее утере (отказе от оной).

4.4.Аутентификация

Аутентификация является одним из самых важных компонентов организации защиты информации в сети. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдает.

При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передает управление серверу аутентификации. После получения положительного ответа сервера аутентификации пользователю предоставляется запрашиваемый ресурс.

При аутентификации используется, как правило, принцип, получивший название "что он знает", - пользователь знает некоторое секретное слово, которое он посылает серверу аутентификации в ответ на его запрос. Одной из схем аутентификации является использование стандартных паролей. Эта схема является наиболее уязвимой с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Чаще всего используются схемы с применением одноразовых паролей. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получить следующий пароль из предыдущего является крайне трудной задачей. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы, представляющие собой устройства, вставляемые в слот компьютера. Знание секретного слова необходимо пользователю для приведения этого устройства в действие. Одной из наиболее простых систем, не требующих дополнительных затрат на оборудование, но в то же время обеспечивающих хороший уровень защиты, является S/Key, на примере которой можно продемонстрировать порядок представления одноразовых паролей.

В процессе аутентификации с использованием S/Key участвуют две стороны - клиент и сервер. При регистрации в системе, использующей схему аутентификации S/Key, сервер присылает на клиентскую машину

приглашение, содержащее зерно, передаваемое по сети в открытом виде, текущее значение счетчика итераций и запрос на ввод одноразового пароля, который должен соответствовать текущему значению счетчика итерации. Получив ответ, сервер проверяет его и передает управление серверу требуемого пользователем сервиса. Подробнее о технологии аутентификации

4.5.Защита сетей

В последнее время корпоративные сети все чаще включаются в Интернет или даже используют его в качестве своей основы. Учитывая то, какой урон может принести незаконное вторжение в корпоративную сеть, необходимо выработать методы защиты. Для защиты корпоративных информационных сетей используются брандмауэры. Брандмауэр - это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью предприятия и Интернетом, хотя ее можно провести и внутри. Однако защищать отдельные компьютеры невыгодно, поэтому обычно защищают всю сеть.

Брандмауэр пропускает через себя весь трафик и для каждого проходящего пакета принимает решение - пропускать его или отбросить. Для того чтобы брандмауэр мог принимать эти решения, для него определяется набор правил.

Брандмауэр может быть реализован как аппаратными средствами (то есть как отдельное физическое устройство), так и в виде специальной программы, запущенной на компьютере.

Как правило, в операционную систему, под управлением которой работает брандмауэр, вносятся изменения, цель которых - повышение защиты самого брандмауэра. Эти изменения затрагивают как ядро ОС, так и соответствующие файлы конфигурации. На самом брандмауэре не разрешается иметь разделов пользователей, а следовательно, и потенциальных дыр - только раздел администратора. Некоторые

брандмауэры работают только в однопользовательском режиме, а многие имеют систему проверки целостности программных кодов.

Брандмауэр обычно состоит из нескольких различных компонентов, включая фильтры или экраны, которые блокируют передачу части трафика. Все брандмауэры можно разделить на два типа:

пакетные фильтры, которые осуществляют фильтрацию IP-пакетов средствами фильтрующих маршрутизаторов;

серверы прикладного уровня, которые блокируют доступ к определенным сервисам в сети. Таким образом, брандмауэр можно определить как набор компонентов или систему, которая располагается между двумя сетями и обладает следующими свойствами:

весь трафик из внутренней сети во внешнюю и из внешней сети во внутреннюю должен пройти через эту систему;

только трафик, определенный локальной стратегией защиты, может пройти через эту систему.

5. Принцип достаточности защиты

Защита публичным ключом(впрочем, как и большинство других видов защиты информации) не является абсолютно надежной. Дело в том, что поскольку каждый желающий может получить использовать чей-то публичный ключ, то он может сколь угодно подробно изучить алгоритм работы механизма шифрования и пытаться установить метод расшифровки сообщения, то есть реконструировать закрытый ключ.

Тонкость заключается в том, что знание алгоритма еще не означает возможности провести реконструкцию ключа в разумно приемлемые сроки. Количество комбинаций, которое надо проверить при реконструкции закрытого ключа, не столь велико, однако защиту информации принято считать достаточной, если затраты на ее преодоление превышают ожидаемую ценность самой информации. В этом состоит принцип достаточности защиты, которым руководствуются при использование симметричных средств шифрования данных. Он предполагает, что защита не абсолютна, и приемы ее снятия известны, но она все же достаточна для того, чтобы сделать это мероприятие нецелесообразным. При появлении иных средств ,позволяющих получить зашифрованную информацию в разумные сроки, изменяют принцип работы алгоритма, и проблема повторяется на более высоком уровне.

Разумеется, не всегда реконструкцию закрытого ключа производят методами простого перебора комбинаций. Для этого существуют специальные методы, основанные на исследовании особенностей взаимодействия открытого ключа с определенными структурами данных.Область науки, посвященная этим исследованиям, называется криптанализом, а средняя продолжительность времени, необходимого для реконструкции закрытого ключа по его опубликованному открытому ключу, называется криптостойкостью алгоритма шифрования.

Для многих методов не симметричного шифрования крипто стойкость, полученная в результате крипанализа, существенно отличается от величин, заявляемых разработчиками алгоритмов на основании теоретических оценок. Поэтому во многих странах вопрос применения алгоритмов шифрования данных находится в поле законодательного регулирования. В частности, в России к использованию в государственных и коммерческих организациях разрешены только те программные средства шифрования данных, которые прошли государственную сертификацию в административных органах, в частности, в Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

6.World wide web серверы и проблема безопасности информации

Среди WWW серверов отличаются отсутствием известных проблем с безопасностью 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.

Заключение

В ходе работы я изучила основные положения по теме «Защита информации в Интернете», представив их в наиболее удобном для последующего изучения виде.

Несмотря на имеющиеся способы защиты информации в глобальной сети Internet, нельзя недооценивать возможности многочисленных хакеров и других взломщиков. Любая, даже, на ваш взгляд, незначительная информация, находящаяся в более менее свободном или плохо защищенном доступе может быть использована против вас. Поэтому всегда следует интересоваться последними новинками в данной теме.

Список литературы

1. Браун С. Система защиты информации в интернете / С. Браун // Мир: Малип: СК Пресс. – М.1996. – С. 167.

2. Колесников О.Э. Интернет для делового человека / О.Э. Колесников // МЦФ. Издат. фирма “Яуза”. – М. 1996. – С. 281 .

3. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // В.К Левин // Программирование. - М., - 1994. - N5.- С. 5-16.

4. Нольден М. Ваш первый выход в Internet: Для начинающих пльзователейInternet и широкого круга пользователей PC / М. Нольден // ИКС. - Спб., 1996. - С. 238 с.

5. Хоникат Д. InternetWindows 95: Руководство пользователя/ Д. Хоникат // БИНОМ. - М., 1996. – С. 334 .

6. Гайкович В., Першин А. Безопасность электронных банковских систем /В. Гайкович, А. Першин //"Единая Европа". - М.- 1994. – С. 264.

7. Гилстер П. Новый навигатор Internet / П. Гилстер // Диалектика. - Киев. - 1996. - С.495.

8. Фролов А.В. Глобальные сети компьютеров. /А.В. Фролов // МИФИ.- М. 1996. - С. 283 .

9. Григорьева В.Л. Защита информации в интернете. / В.Л. Григорьева // Санкт -Петербургский Государственный Университет Экономики и Финансов. – Спб. –2007. – 1 декабря [Электронный ресурс] URL: http://www.bestreferat.ru/referat-143086.html(Дата обращения: 27.01.16)

10. Защита информации в Интернете: реферат.- Санкт-Петербургский Государственный Университет Экономики и Финансов. – Спб. - 2007. URL: http://refoteka.ru/r-143086.html (Дата обращения: 27.01.16)