Администрация города Нижнего Новгорода
Департамент образования
Муниципальное автономное общеобразовательное учреждение
«Гимназия № 67»

ул. Софьи Перовской, д. 5, г. Нижний Новгород, 603014, тел. (831) 270-03-69, факс (831) 270-03-69,
e-mail: lingym@list.ru

ОКПО 25662268 ОГРН 1025202844116 ИНН 5259012845

Научное общество учащихся

Научная работа по информатике

«Безопасный Интернет».

Выполнила: Казнина Анастасия Александровна,
ученица 9 «А» класса
Научный руководитель: Истомина Т.В.,
учитель информатики

2018 г.

Содержание

Введение

По своему значению для развития общества информация приравнивается к важнейшим ресурсам наряду с сырьем и энергией. В развитых странах большинство работающих заняты не в сфере производства, а в той или иной степени занимаются обработкой информации.

Вместе с тем можно отметить и новую тенденцию, заключающуюся во все большей информационной зависимости общества в целом и отдельного человека, в частности. Именно поэтому в последнее время появились такие категории, как «информационная политика», «информационная безопасность», «информационная война» и целый ряд других новых понятий, в той или иной мере связанных с информацией.

В современном деловом мире происходит процесс миграции материальных активов в сторону информационных. По мере развития организации усложняется ее информационная система, основной задачей которой является обеспечение максимальной эффективности ведения бизнеса в постоянно меняющихся условиях конкуренции на рынке.

Рассматривая информацию как товар, можно сказать, что информационная безопасность в целом может привести к значительной экономии средств, в то время как ущерб, нанесенный ей, приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и как следствие нарушения информационной безопасности, владелец технологии, а может быть и автор, потеряют часть рынка и т.д. С другой стороны, информация является субъектом управления, и ее изменение может привести к катастрофическим последствиям в объекте управления.

Информационная безопасность является одной из главных проблем, с которой сталкивается современное общество. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения» обработки и передачи информации.

Информационная безопасность в глобальной сети Интернет также является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки.

При работе в Интернете следует иметь в виду, что насколько ресурсы Всемирной сети открыты каждому клиенту, настолько же и ресурсы его компьютерной системы могут быть при определенных условиях открыты всем, кто обладает необходимыми средствами.

Для частного пользования этот факт не играет особой роли, но знать о нем необходимо, чтобы не допускать действий, нарушающих законодательства тех стран, на территории которых расположены серверы Интернета. К таким действиям относятся вольные или невольные попытки нарушить работоспособность компьютерных систем, попытки взлома защищенных систем, использование и распространение программ, нарушающих работоспособность компьютерных систем (в частности, компьютерных вирусов).

Цель данной работы: изучение сущности информационной безопасности при работе в глобальной сети Интернет.

Объект изучения: информационная безопасность.

Предмет изучения: современные интернет-технологии, связанные с информационными угрозами и информационной безопасностью.

Задачи работы:

1) изучить понятие информационной безопасности в Интернете;

2) рассмотреть достоинства и недостатки cookies;

3) изучить понятие понятие аутентификаци и ее механизмы;

4) изучить значение цифровых сертификатов в передаче информации по Интернету;

5) рассмотреть возможные этапы настройки безопасности web-браузера на примере Internet Explorer;

6) рассмотреть сущность цифрового кодирования информационных потоков.

1. Безопасность в Интернет

Основной особенностью любой сетевой системы, в частности, Интернета является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов (порций данных) обмена. Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы» к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по каналам связи.

Если проследить эволюцию локальной компьютерной сети практически любой организации, то можно увидеть, что изначально она строилась как средство обмена файлами и доступа к Интернету. Затем, с ростом организации, ее сеть начинала обзаводиться новыми сервисами:

— для упорядочения процессов обмена информацией появилась электронная почта; затем — система делопроизводства;

— потом возникла необходимость ведения архива документов и т.д.

Со временем сеть становится все сложнее, в ней хранится все больше информации. На определенной ступени этой эволюции организация сталкивается с проблемами:

— защиты самой информационной системы (поскольку ущерб организации наносится в результате воздействия вирусов или атак при наличиии самой простой информационной системы);

— разграничениями и ограничениями доступа пользователей к ресурсам Интернета;

— контролем за действиями пользователей в Интернет.

В качестве модулей защищенного доступа в Интернет используются:

1) Межсетевые экраны

· для пресечения возможности обхода средств контроля

· для регламентирования объемов загружаемой информации

2) Средства контроля содержимого

· для проверки входящих и исходящих почтовых сообщений;

· для проверки данных Web-сайтов и их содержимого.

3) Антивирусные средства — для проверки mail и web-трафика на наличие вредоносного программного обеспечения.

Предлагаемое решение позволяет:

· защититься от утечки секретной и конфиденциальной информации;

· пресечь рассылки рекламных сообщений нецелевого характера;

· бороться с непроизводительным использованием сервисов Интернета;

· пресечь распространения клеветнических сообщений;

· контролировать лояльность персонала;

· повысить эффективности использования информационных технологий;

· обнаруживать в электронных письмах конфиденциальную информацию, вирусы и другие нежелательные объекты, а также реагировать на это заданным образом.

2. Cookies

Ку́ки (слово не склоняется; от англ. cookie — печенье) — небольшой фрагмент данных в виде текстового файла, созданный веб-сервером и хранимый на компьютере пользователя в виде файла, который веб-клиент (обычно веб-браузер) каждый раз пересылает веб-серверу в запросе при попытке открыть страницу соответствующего сайта. Применяется для сохранения данных на стороне пользователя, на практике обычно используется для:

· аутентификации пользователя (предъявление данных идентификации пользователя);

· хранения персональных предпочтений и настроек пользователя;

· отслеживания состояния сессии доступа пользователя;

· ведения статистики о пользователях.

Cookie — это небольшая порция текстовой информации, которую сервер передает браузеру. Браузер будет хранить эту информацию и передавать ее серверу с каждым запросом при обращении. Одни значения cookie могут храниться только в течение одной сессии, они удаляются после закрытия браузера. Сами по себе cookies не могут делать ничего, это только лишь некоторая текстовая информация. Однако сервер может считывать содержащуюся в cookies информацию и на основании ее анализа совершать те или иные действия. Например, в случае авторизованного доступа к чему либо через Интернет в cookies сохраняется логин и пароль в течение сеанса работы, что позволяет пользователю не вводить их снова при запросах каждого документа, защищенного паролем. На компьютере пользователя cookies хранятся в виде файлов в специальной папке. Каждому сайту соответствует собственный файл. Кроме того, на cookies наложены определенные ограничения. Во-первых, каждый сервер может записывать и считывать информацию только из «своего» файла.

3. Отправка защищенной информации через Интернет

Одним из главных достоинств Internet является то, что она широкодоступна. Этот «святой источник» всех сетей может проникнуть практически в любое место, где есть телефон. Конечно, связь через Internet имеет свои недостатки, главным из которых является то, что она подвержена потенциальным нарушениям защиты и конфиденциальности. Используя Internet в качестве расширения собственной внутрикорпоративной сети, вы посылаете информацию по общедоступным каналам, и всякий, кто может установить на ее пути анализатор протоколов, имеет потенциальную возможность перехватить вашу информацию.

Виртуальные частные сети (VirtualPrivateNetwork — VPN) могут гарантировать, что направляемый через Internet трафик так же защищен, как и передачи внутри локальной сети, при сохранении всех финансовых преимуществ, которые можно получить, используя Internet.

Вот как это работает. VPN-устройство располагается между внутренней сетью и Internet на каждом конце соединения. Когда вы передаете данные через VPN, они исчезают «с поверхности» в точке отправки и вновь появляются только в точке назначения. Этот процесс принято называть «туннелированием». Как можно догадаться из названия, это означает создание логического туннеля в сети Internet, который соединяет две крайние точки. Благодаря туннелированию частная информация становится невидимой для других пользователей Web-технологий Интернета.

VPN, защищающие данные пользователей «в пути», могут быть устроены различными способами. Отдельный класс представлен VPN на основе разграничения трафика, которые туннелируют (но не шифруют!) трафик пользователей вдоль виртуальных соединений работающих в сетях провайдеров Интернет. Это эффективное решение, так как всю работу по защите данных пользователя выполняет провайдер, которому к тому же не нужно получать лицензию на шифрование данных. Однако пока такое решение работает только в пределах сети одного провайдера, а, значит, не может

использоваться, если офисы предприятия подключены к разным провайдерам. Другой класс VPN использует шифрование трафика (чаще всего такие средства и имеют в виду, когда говорят про VPN). Шлюз VPN шифрует пользовательские IP-пакеты, направляющиеся из внутренней сети в Интернет, и упаковывает их в новые IP-пакеты, которые он создает и отправляет от своего IP-адреса. В сети (или компьютере) получателя другой VPN-шлюз извлекает из такого пакета оригинальный IP-пакет и расшифровывает его. Образуется шифрованный туннель через Интернет, при этом злоумышленник может только удалить пакет, но не в состоянии прочитать его, подменить или исказить информацию.

Виртуальные частные сети часто используются в сочетании с межсетевыми экранами. Ведь VPN обеспечивает защиту корпоративных данных только во время их движения по Internet и не может защитить внутреннюю сеть от проникновения злоумышленников.

4. Аутентификация

Аутентификация (установление подлинности) — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

— набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);

— физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях — конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

5. Цифровые сертификаты

Цифровой сертификат — выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов.

Центр сертификации — это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами (ключами шифрования) пользователей. Открытые ключи и другая информация о пользователях хранится центрами сертификации в виде цифровых сертификатов, имеющих следующую структуру:

— серийный номер сертификата;

— объектный идентификатор алгоритма электронной подписи;

— имя удостоверяющего центра;

— срок годности;

— имя владельца сертификата (имя пользователя, которому принадлежит сертификат);

— открытые ключи владельца сертификата (ключей может быть несколько);

— алгоритмы, ассоциированные с открытыми ключами владельца сертификата;

— электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат преобразования всей информации, хранящейся в сертификате).

Отличием аккредитованного центра является то, что он находится в договорных отношениях с вышестоящим удостоверяющим центром и не является первым владельцем самоподписанного сертификата в списке удостоверенных корневых сертификатов. Таким образом корневой сертификат аккредитованного центра удостоверен вышестоящим удостоверяющим центром в иерархии системы удостоверения. Таким образом аккредитованный центр получает «техническое право» работы и наследует «доверие» от организации выполнившей аккредитацию.

Центр сертификации ключей имеет право: предоставлять услуги по удостоверению сертификатов электронной цифровой подписи и обслуживать сертификаты открытых ключей, получать и проверять информацию, необходимую для создания соответствия информации указанной в сертификате ключа и предъявленными документами.

Криптографическая система с открытым ключом (или Асимметричное шифрование,

Асимметричный шифр) — система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации ЭЦП и для расшифрования сообщения используется секретный ключ.

В частности, пакет приложений Microsoft Office XP использует технологию Microsoft Authenticode, позволяющую снабжать проекты макросов и файлы цифровой подписью с использованием цифрового сертификата.

Сертификат, используемый для создания подписи, подтверждает, что макрос или документ получен от владельца подписи, а подпись подтверждает, что макрос или документ не был изменен. Установив уровень безопасности, можно разрешить или запретить выполнение макроса в зависимости от того, входит ли подписавший его разработчик в список надежных источников.

6. Настройка безопасности браузера (Internet Explorer)

Обозреватель Internet Exp1oreг нельзя полностью обезопасить с помощью его программных настроек. Чтобы чувствовать себя в более менее безопасном состоянии, надо совместно с ним на компьютере использовать хороший брандмауэр (межсетевой экран).

Элементы управления, связанные с настройкой правил безопасности, сосредоточены на вкладках Дополнительно и Безопасность диалогового окна Свойства обозревателя

Откройте диалоговое окно Свойства обозревателя (Internet Exp1oreг > Сервис > Свойства обозревателя). Открой вкладку Дополнительно. В разделе Безопасность сбрось галочку Задействовать профиль. Если флажок оставить, браузер будет поставлять удаленным серверам по их запросу личные данные о пользователе.

В этом же разделе установите все галочки у строк, начинающихся словами Не сохранять..., Предупреждать..., Проверять… и Удалять.

В разделе Обзор необходимо сбросить следующие галочки:

— Автоматически проверять обновление Internet Exp1oreг;

— Включить установку по запросу;

— Использовать встроенное автозаполнение в проводнике;

— Использовать встроенное автозаполнение Web-адресов,

— Разрешить счетчик попаданий на страницы.

— Выполнив указанные настройки, щёлкни по кнопке Применить.

Откройте вкладку Безопасность диалогового окна Свойства обозревателя. На панели зон безопасности выбери зону Интернет

Откройте диалоговое окно настройки правил безопасности щелчком по кнопке Другой. Для всех операций, которым сопоставлено три метода взаимодействия с сервером: Отключить, Предлагать, Разрешить -включи переключатель Предлагать. В этом случае при потенциально опасных операциях будет открываться диалоговое окно с предложением подтвердить или отвергнуть действие.

7. Кодирование

Кодирование информации — это представление сообщений в конкретном виде при помощи некоторой последовательности знаков.

Одну и ту же информацию, например, сведения об опасности мы можем выразить разными способами: просто крикнуть; оставить предупреждающий знак (рисунок); с помощью мимики и жестов; передать сигнал «SOS» с помощью азбуки Морзе или используя семафорную и флажковую сигнализацию. В каждом из этих способов мы должны знать правила, по которым можно отобразить информацию. Такое правило назовем кодом.

Код — это набор условных обозначений (или сигналов) для записи (или передачи) некоторых заранее определенных понятий.

Кодирование информации – это процесс формирования определенного представления информации. В более узком смысле под термином «кодирование» часто понимают переход от одной формы представления информации к другой, более удобной для хранения, передачи или обработки.

Обычно каждый образ при кодировании (иногда говорят — шифровке) представлении отдельным знаком.

Знак — это элемент конечного множества отличных друг от друга элементов.

Знак вместе с его смыслом называют символом.

Набор знаков, в котором определен их порядок, называется алфавитом. Существует множество алфавитов:

• алфавит кириллических букв {А, Б, В, Г, Д, Е, ...}

• алфавит латинских букв {A, B, C, D, E, F,...}

• алфавит десятичных цифр{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

• алфавит знаков зодиака {картинки знаков зодиака} и др.

Особенно большое значение имеют наборы, состоящие всего из двух знаков:

• пара знаков {+, -}

• пара цифр {0, 1}

• пара ответов {да, нет}

Алфавит, состоящий из двух знаков, называется двоичным алфавитом. Двоичный знак (англ. binary digit) получил название «бит».

Шифрование — кодирование сообщения отправителя, но такое чтобы оно было не понятно несанкционированному пользователю.

Длиной кода называется такое количество знаков, которое используется при кодировании.

Количество символов в алфавите кодирования и длина кода — совершенно разные вещи. Например, в русском алфавите 33 буквы, а слова могут быть длиной в 1, 2, 3 и т.д. буквы.

Код может быть постоянной и непостоянной длины. Коды различной (непостоянной) длины в технике используются довольно редко. Исключением является лишь троичный код Морзе. В вычислительной технике в настоящее время широко используется двоичное кодирование с алфавитом (0, 1). Наиболее распространенными кодами являются ASCII (American standart code for information interchange — американский стандартный код для обмена информацией) и КОИ-8 (код обмена информации длиной 8 бит).

Одно и то же сообщение можно закодировать разными способами, т. е. выразить на разных языках. В процессе развития человеческого общества люди выработали большое число языков кодирования. К ним относятся:

• разговорные языки (русский, английский, хинди и др. — всего более 2000);

• язык мимики и жестов;

• язык рисунков и чертежей;• язык науки (математические, химические, биологические и другие символы);

• язык искусства (музыки, живописи, скульптуры и т. д.);

• специальные языки (эсперанто, морской семафор, азбука Морзе, азбука Брайля для слепых и др.).

Заключение

Продолжающееся бурное развитие компьютерных технологий и повсеместное внедрение в бизнес с использованием Интернета коренным образом изменяет устоявшиеся способы ведения бизнеса. Системы корпоративной безопасности, обеспечивающие бизнес, тоже не могут оставаться в стороне.

В настоящее время, например, средства электронной почты, используются не только для общения между людьми, а для передачи контрактов и конфиденциальной финансовой информации. Web сервера используются не только для рекламных целей, но и для распространения программного обеспечения и электронной коммерции. Электронная почта, доступ к Web серверу, электронная коммерция, VPN требуют применения дополнительных средств для обеспечения конфиденциальности, аутентификации, контроля доступа, целостности и идентификации.

Такой неотъемленый элемент интернет-технологии как куки имеет свои плюсы в необходимости использования и минусы в передаче конфиденциальных потоков данных. Cookies — это небольшие порции текста, которые веб-серверы могут передавать на компьютер пользователя. Они записываются в специальные файлы и в будущем могут передаваться обратно серверу. Сегодня у многих пользователей сложилось отрицательное отношение к cookies. Общепринятым стало мнение, что «печенье» (а именно так и переводится этот термин с английского) несет угрозу анонимности и безопасности пользователя. Естественно, подобные обвинения в адрес cookies нельзя назвать совсем уж беспочвенными. Тем не менее, эта технология нужна — в первую очередь, для обеспечения удобства пользователей.

Работая во Всемирной сети, следует помнить о том, что абсолютно все действия фиксируются и протоколируются специальными программными средствами и информация как о законных, так и о незаконных действиях обязательно где-то накапливается. Таким образом, к обмену информацией в Интернете следует подходить как к обычной переписке с использованием

почтовых открыток. Информация свободно циркулирует в обе стороны, но в общем случае она доступна всем участникам информационного процесса. Это касается всех служб Интернета, открытых для массового использования.

Однако даже в обычной почтовой связи наряду с открытками существуют и почтовые конверты. Использование почтовых конвертов при переписке не означает, что партнерам есть, что скрывать. Их применение соответствует давно сложившейся исторической традиции и устоявшимся морально-этическим нормам общения. Потребность в аналогичных «конвертах» для защиты информации существует и в Интернете. Сегодня Интернет является не только средством общения и универсальной справочной системой — в нем циркулируют договорные и финансовые обязательства, необходимость защиты которых как от просмотра, так и от фальсификации очевидна.

Начиная с 1999 года Интернет становится мощным средством обеспечения розничного торгового оборота, а это требует защиты данных кредитных карт и других электронных платежных средств.

Список литературы

1. Филимонова Е.В. Информационные технологии в профессиональной деятельности: Учебник. – Ростов н/Д: Феникс, 2004. – 352 с. (серия «СПО»).

2. Автоматизированные информационные технологии в экономике Ред.: Г.А.Титоренко Москва: Юнити, 2006.

3. Грошев С.В., Коцюбинский А.О., Комягин В.Б. Современный самоучитель профессиональной работы на компьютере: Практ. пособ. – М.: Триумф, 2005.

4. Левин А. Самоучитель полезных программ. – СПб.: Питер, 2007.

5. Юрьева, Т. Ю. Словарь информационных продуктов и услуг / Т.Ю. Юрьева. — Кемерово.: — РОСТИКС,2006.- 50 с.

6. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / Петр Николаевич Девянин. — М.: Издательский центр «Академия», 2005. — 144 с.

7. Копыл В.И. Поиск в Интернете./ В. И. Копыл.— М.: АСТ, Мн.: Харвест, 2006.— 64 с.

8. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. – Феникс, 2008.

9. Башлы П.Н. Информационная безопасность / П.Н. Башлы. —Ростов н/Д: Феникс, 2006. — 253 с.

10. Мельников В. П. Информационная безопасность: Учеб. пособие для сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. — М.: Издательский центр «Академия», 2005. — 336 с.

11. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006.