Безопасность информационных систем

Информационная система современной организации или предприятия является сложным образованием, построенным в многоуровневой архитектуре клиент-сервер, которое пользуется многочисленными внешними серверами, а также предоставляет во вне собственные серверы.

Современные информационные системы сложны, а значит, опасны уже сами по себе, даже без учета вмешательства злоумышленников. Постоянно обнаруживаются новые ошибки и уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Под ***безопасностью ИС*** понимается защищенность системы, т.е. ее способность противостоять различным воздействиям.

Высокие темпы развития информационных технологий делают весьма актуально проблему защиты информации, ее пользователей, информационных ресурсов и каналов передачи данных, а также требуют постоянного совершенствования механизмов защиты.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Угроза - *целенаправленное действие, которое повышает уязвимость накапливаемой, хранимой и обрабатываемой системы информации и приводит к ее случайному или предумышленному изменению или уничтожению.*

Угрозы бывают *случайные* (непреднамеренные) и *умышленные* (преднамеренные).

Случайные угрозы:

- ошибки обслуживающего персонала и пользователей;
- случайное уничтожение или изменение данных;
- сбои оборудования и электропитания;

- сбои кабельной системы;
- сбои дисковых систем;
- сбои систем архивирования данных;
- сбои работы серверов, рабочих станций, сетевого оборудования;
- некорректная работа программного обеспечения;
- заражение системы компьютерными вирусами;
- неправильное хранение конфиденциальной информации.

Из случайных угроз самыми частыми и самыми опасными (с точки зрения размера ущерба) является пресловутый «человеческий фактор» - непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. По опубликованным данным до 65% информации бесследно исчезает именно из-за этого.

Трудно предсказуемыми источниками угроз информации являются аварии и стихийные бедствия. На безопасность ИС существенное влияние оказывает тот факт, что безошибочных программ, в принципе не существует. Это касается не только отдельных программ, но и целого ряда программных продуктов фирм, известных во всем мире, например, Microsoft. Информационно-аналитический сайт www.securitylab.ru постоянно публикует информацию об уязвимостях, найденных в операционных системах и приложениях. По данным этого источника, ежедневно обнаруживаются в среднем 5-10 новых уязвимостей.

Преднамеренные угрозы:

- несанкционированный доступ к информации и сетевым ресурсам;
- раскрытие и модификация данных и программ, их копирование;
- раскрытие, модификация или подмена трафика вычислительной сети;
- разработка и распространение компьютерных вирусов, ввод в программное обеспечение логических бомб;
- кража магнитных носителей и технической документации;

- разрушение архивной информации или умышленное ее уничтожение;
- фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
- перехват и ознакомление с информацией, передаваемой по каналам связи;
- незаконное использование привилегий;
- несанкционированное использование информационных ресурсов.

Несанкционированный доступ (НСД) - наиболее распространенный вид компьютерных нарушений. Он заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно целью злоумышленника является нарушение конфиденциальности данных. Самое сложное - определить, кто и к каким данным может иметь доступ, а кто - нет. Наиболее распространенными путями несанкционированного доступа к информации являются:

- применения подслушивающих устройств (закладок);
- перехват электронных излучений;
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- маскировка под запросы системы;
- использование программных ловушек;
- использование недостатков языков программирования;
- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к

информации;

- злоумышленный вывод из строя механизмов защиты;
- информационные инфекции.

Перечисленные выше пути несанкционированного доступа требуют специальных технических знаний и соответствующих аппаратных и программных разработок. Однако есть и достаточно примитивные пути несанкционированного доступа:

- хищение носителей информации и документальных отходов;
- склонение к сотрудничеству со стороны взломщиков;
- подслушивание,
- наблюдение и т.д.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу, как для организации, так и для пользователей. Большинство из перечисленных путей несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности.

Анализируя возможные угрозы с точки зрения наибольшей опасности, изощренности и разрушительности, следует выделить вредоносное программное обеспечение. Вредоносное программное обеспечение – это любая программа, написанная с целью нанесения ущерба или для использования ресурсов атакуемого компьютера. О вредоносном программном обеспечении известно больше, чем о каких-либо других опасностях и повреждениях компьютерной техники. Вредоносное программное обеспечение можно разделить на три группы: *Компьютерные вирусы, хакерское ПО и спам.*

Вирусы – самое старое вредоносное ПО, существует уже более 20 лет. Подробная классификация вирусов и их характеристика даны в курсе «Экономическая информатика»

Вредоносное действие вируса может проявиться в следующем:

-появление в процессе работы компьютера неожиданных эффектов (падение символов на экране, неожиданные звуковые эффекты, появление неожиданных картинок и т.п.);

-замедление работы компьютера;

-сбои и отказы в работе прикладных программ;

-порча исчезновение файлов с магнитного диска;

-вывод из строя операционной системы;

-разрушение файловой системы компьютера;

-вывод из строя аппаратуры компьютера.

Исторически сначала появились вирусы , поражающие программные файлы, потом загрузочные вирусы, распространяющиеся через загрузочные области магнитных дисков. Основным средством распространения являются дискеты. Позднее появились макровирусы, распространяющиеся с документами офисных приложений, таких, как *Microsoft Exce1*. Для запуска вирусов этого вида достаточно открыть зараженный документ.

Наряду с совершенствованием механизмов распространения вирусов авторы-вирусописатели улучшали и улучшают скрытность вирусов. Один из способов повышения скрытности вируса, затрудняющий его обнаружение, - это использование шифрования. Шифрующиеся вирусы шифруют собственный код, используя различные ключи и алгоритмы шифрования. В результате каждая новая копия вируса приобретает новый вид. Внедрение ЛВС облегчило процедуру распространения вирусов. Достаточно заразить один компьютер и вирус начнет распространяться по сети, заражая все доступные сетевые диски.

Еще более благоприятную почву для распространения вирусов предоставляют Интернет и электронная почта. Зараженную программу (почтовый вирус) можно получить как приложение к электронному письму. Существуют вирусы, которые могут распространяться через электронную почту без использования приложений, так называемые черви. Для заражения машины не требуется запускать какой-либо приложенный файл, достаточно

лишь просмотреть письмо. В его html-коде содержится автоматически запускающийся скрипт, выполняющий вредоносное действие. После активации червь рассылает письмо-ловушку по всем записям, находящимся в адресной книге на зараженном компьютере.

Сеть Интернет предоставляет дополнительные возможности для распространения вирусов. Использование технологии объектов *Active X* создает потенциальную угрозу проникновения вирусов. Такой объект размещается на сервере WWW и при обращении к нему загружается в память удаленного компьютера. Объект *Active X* представляет собой программу, которая автоматически запускается на компьютере удаленного пользователя и может делать там практически все что угодно. В частности, не исключено, что она может получить доступ к файловой системе и заразить компьютер вирусом.

Программы, составленные на языке Java, не представляют угрозу для распространения вирусов, так как они не имеют доступа к файловой системе удаленного компьютера. Плата за безопасность — меньшая функциональность по сравнению с объектами *Active X.*

Хакерское ПО — это инструмент для взлома и хищения конфиденциальных данных. Существуют инструменты для сбора данных о потенциальных жертвах и поиска уязвимостей в компьютерных сетях. К ним относятся программы для сканирования сети с целью определения IP-адресов компьютеров и «открытых» портов. Программы «прослушивания» сетевого трафика незаметно перехватывают IP-пакеты в сети и анализируют их в целях определения адресов отправителей и получателей и, может быть, выявления секретных данных типа имен и паролей, передаваемых в открытом виде. Формат почтовых сообщений является открытым, следовательно, электронное письмо может быть легко прочитано.

Есть инструменты хакеров, предназначенные для взлома компьютеров и сетей. К ним относятся программы подбора паролей, фальсификации IP-пакетов путем подмены адреса отправителя/ получателя. Отдельного

рассмотрения требуют программы-троянцы (трояны), представляющие в настоящее время главную угрозу и занимающие лидирующее положение среди вредоносного ПО.

Название «троян» («троянский конь») возникло из-за того, что вначале вредоносный код маскировался в некоторой полезной или интересной программе, которую пользователь по доброй воле устанавливал на компьютер. Это могла быть какая-либо утилита, повышающая удобство работы на компьютере, или компьютерная игра. Сейчас троянцы распространяются и по электронной почте, также их можно загрузить на рабочий компьютер с какого-нибудь сайта, просматривая интересные страницы.

Троян незаметно для пользователя (под «прикрытием» полезной программы или будучи внедренным в операционную систему) выполняет ряд действий в интересах хакера:

- соединение с сервером хакера и пересылка на него всех вводимых с клавиатуры данных, адресов электронной почты;
- рассылка электронной почты по заданным адресам;
- •выполнение команд, получаемых с хакерского сервера.

Таким образом, троян «открывает» компьютерную сеть или отдельный компьютер для хакера.

Спам заслуженно считается одной из важных проблем Интернета. Более 80% всех получаемых электронных писем являются спамом, т.е. ненужными пользователю. Природа спама такая же, как у телевизионной рекламы, и пока рассылка спама приносит деньги, вряд ли он может быть искоренен. Пользователю спам причиняет гораздо меньший вред, чем ранее рассмотренные вредоносные программы. В конечном итоге, удаление ненужных писем занимает не очень много времени — обычно несколько минут. Побочный эффект спама — удаление в общей массе мусора «нужных» писем. Но методы рассылки спама заслуживают внимания, так как в этот процесс может быть непроизвольно вовлечен компьютер пользователя.

Если раньше спамеры осуществляли рассылку писем со своих компьютеров и самостоятельно формировали списки рассылки, то теперь для этого используется вредоносное ПО. В качестве примера приведем схему работы спам-бота. *Спам-бот* — это троянская программа, осуществляющая рассылку спама с зараженного компьютера. Для распространения спам-ботов применяются почтовые и сетевые черви. После своего внедрения спам-бот устанавливает соединение с одним из заранее ему известных серверов, принадлежащих спамеру, и получает информацию об адресах серверов, с которых он должен запрашивать данные для рассылки. Далее он связывается с этими серверами, получает *e-mail-адреса* и шаблоны для писем и производит рассылку. В дополнение спам-бот отправит на сервер спамера отчет о недоставленных письмах и адреса из адресной книги зараженного компьютера для актуализации списков рассылки, используемых спамером.

Помимо специального ПО для взлома компьютерных сетей и внедрения вредоносного ПО хакеры активно применяют методы социальной инженерии. Самый простой пример - рассылка зараженных писем, в которых указана тема, интересующая получателя ели вызывающая у него любопытство (поздравительная открытка, приглашение куда-нибудь и т.п.). Главная задача - спровоцировать получателя открыть письмо.

Метод фишинга используется для того, чтобы «выудить» у пользователя сведения для доступа к каким-либо ресурсам. Например, можно получить письмо, адрес отправителя в котором очень похож на адрес провайдера услуг Интернета, содержащее просьбу администратора подтвердить *login* и пароль. Серьезную угрозу фишинг представляет для клиентов интернет-банков. Злоумышленник посылает письмо с подделанным обратным адресом, т.е. внешне письмо выглядит как посланное из банка. В письме сообщается, что требуется сменить пароль, и указан адрес сайта, на котором необходимо выполнить это действие. Перейдя по этой ссылке, клиент попадает на сайт, внешне не отличающийся от настоящего, и благополучно раскрывает свои персональные данные.

Недавно специалистами компании "Доктор Веб" был обнаружен компьютерный вирус, похищающий информацию о владельцах банковских карт прямо в банкоматах. По некоторым данным, вирус атаковал банкоматы уже нескольких российских банков. Служба вирусного мониторинга получила образец вируса через сервис онлайн-сканера и классифицировала его как Trojan.Skimer. Вредоносная программа собирает информацию о кредитных картах и PIN-кодах к ним, после чего отправляет ее злоумышленникам. В итоге те получают доступ к данным своих потенциальных жертв и могут лишить их всех имеющихся на карточке денег. По информации компании "Доктор Веб", это первый вирус, способный перехватывать данные о банковских картах пользователей, которые ранее пользовались зараженным банкоматом. Хотя вирусные атаки на банкоматы регистрировались и раньше, в худшем случае они просто выводили банкомат из строя, не угрожая пользователям.

В последнее время можно заметить снижение количества крупных всеобщих вирусных эпидемий и увеличение количества целенаправленных атак. Можно говорить о закате эры «вирусописателей-романтиков», создающих вирусы ради самоутверждения, и о появлении организованной киберпреступности. Растет число атак с последующим шантажом и вымогательством. Соответственно, все большее распространение получают вирусы (трояны) со шпионской функцией и развитыми средствами маскировки. Цель - создание распределенных сетей компьютеров-зомби (владельцы компьютеров и не подозревают об этом) для рассылки спама и проведения *Dos-атак* против выбранной компании.

В распространении вирусов намечается переход от почты и червей к сайтам, т.е. увеличивается количество взломов сайтов для размещения на них вредоносных кодов. Таким образом, можно говорить о том, что по мере увеличения роли информации и информационных систем в современном мире растут и угрозы их нормальному функционированию. В противовес угрозам развиваются методы и средства защиты информации и

информационных систем.

Методы и средства защиты информационных систем

Сегодня рождается новая современная технология – технология защиты информации в компьютерных информационных системах и в сетях передачи данных, т.е. для защиты информации организовывается целый комплекс мер, использующих специальные средства, методы и мероприятия с целью предотвращения потери информации.

Организационные мероприятия и процедуры, используемые для решения проблемы безопасности информации, решаются на всех этапах проектирования и в процессе эксплуатации ИТ.

Современные ИТ обладают следующими основными признаками:

- наличием информации различной степени конфиденциальности;
- необходимостью криптографической защиты информации различной степени конфиденциальности при передаче данных;
- иерархичностью полномочий субъектов доступа и программ к АРМ, файл-серверам, каналам связи и информации системы, необходимостью оперативного изменения этих полномочий;
- - организацией обработки информации в диалоговом режиме, в режиме разделения времени между пользователями и в режиме реального времени;
- обязательным управлением потоками информации как в локальных сетях, так и при передаче по каналам связи на далекие расстояния;
- необходимостью регистрации и учета попыток несанкционированного доступа, событий в системе и документов, выводимых на печать;
- обязательным обеспечением целостности программного обеспечения и информации в ИТ;
- наличием средств восстановления системы защиты информации;

- обязательным учетом магнитных носителей;

- наличием физической охраны средств вычислительной техники и магнитных носителей.

*Основными **методами защиты** информации являются:*

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (посты охраны на охраняемых объектах)

Управление доступом – включает:

- идентификацию пользователей, персонала и ресурсов системы;

- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

- регистрацию (протоколирование) обращений к защищаемым ресурсам; и т.д.

Маскировка - метод защиты информации путем ее криптографического закрытия (криптографические коды информации);

Регламентация – метод защиты информации, при которых возможности несанкционированного доступа к ней сводятся к минимуму (организационные – использование паролей, ключей правила разграничения доступа и т.д.);

Принуждение – материальная, административная или уголовная ответственности;

Побуждение - такой метод защиты формируется за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных.)

*К основным **средствам защиты** относят:*

- ***Технические средства** – электрические, электромеханические и электронные устройства;*

- ***Физические средства** – замки на дверях, решетки на окнах и т.д.*

- ***Программные средства** (ПО), выполняющее функции защиты информации*

- ***Организационные средства*** *защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники.(строительство помещений, проектирование компьютерной информационной системы банковской или любой другой деятельности)*

- ***Морально-этические средства*** *– нормы и правила, которые сложились традиционно в обществе.*

- ***Законодательные средства*** *– законодательные акты страны (против хакеров)*

Создание системы информационной безопасности

В любой вычислительной сети важна защита информации от случайной порчи, потери, несанкционированного доступа. Возможных путей потери информации существует много: перехват электронных излучений, считывание информации другого пользователя, незаконное подключение и др.

Наиболее распространенными путями несанкционированного доступа к информации являются:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и документальных отходов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- незаконное подключение к аппаратуре и линиям связи;
- внедрение и использование компьютерных вирусов.

Основные виды защиты:

- ***Защита информации от несанкционированного доступа путем:*** регистрации входа (выхода) субъектов доступа в систему (из системы) либо регистрацию загрузки и инициализации операционной системы и ее программного останова, регистрации и учета выдачи печатных (графических) документов на твердую копию и т.д.

- ***Защита информации в системах связи путем криптогра***фии и специальных связных протоколов.

- ***Защита юридической значимости электронных документов путем применения "цифровых подписей"*** (шифрование данных криптографической контрольной суммой с использованием секретного ключа)

- ***Защита данных от утечки по электромагнитным излучениям путем экранирования помещений;***

- ***Защита информации от компьютерных вирусов и других опасных воз***действий по каналам распространения программ путем разграничения доступа, самоконтроля и самовосстановления, применения специальных программ – анализаторов или антивирусных, выслеживающих отклонения в деятельности прикладных программ и наличие вирусов, и по возможности их устранение.

- ***Защита от несанкционированного копирования и распространения прогр***амм и ценной компьютерной информации путем парольной защиты, ключей, проверки рабочей ПЭВМ по ее уникальным характеристикам, шифрование файлов, содержащих исполняемый код программы и т.д.

Криптография – это наука об обеспечении секретности и/ или аутентичности (подлинности) передаваемых сообщений. Ее сущность в том, что передаваемое сообщение шифруется, преобразуется в шифрограмму (криптограмму), а при получении санкционированным пользователем дешифруется, т.е. превращается в исходный текст. Для этого используется

специальный алгоритм. Действие такого алгоритма запускается уникальным числом, или битовой последовательностью,(шифрующим ключом). Шифрование может быть симметричным (используется один и тот же ключ для шифрования и дешифрования) и ассиметричным (для шифрования используется один общедоступный ключ, а для дешифрования – другой секретный.)

Криптографические системы помогают решить проблему аутентификации принятой информации, т.к. подслушивающее лицо будет иметь дело только с зашифрованным текстом. Таким образом, истинный получатель, приняв эти сообщения, закрытые известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.