Содержание:

ВВЕДЕНИЕ

Проблема надежной защиты информации, т.е. предупреждение ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования информации в настоящее время приобретает все более важное значение. Особую остроту проблема защиты приобретает в связи с повсеместной и массовой компьютеризацией информационных процессов, широким внедрением информационно-вычислительных сетей с доступом к их ресурсам массы пользователей.

Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Это создает большое число угроз информации, которые могут быть реализованы как со стороны внешних, так и со стороны внутренних нарушителей.

Для решения проблем защиты информации следует подробно изучить виды и состав угроз. Обеспечение информационной безопасности в информационных системах является весьма важной задачей. Решение проблем защиты информации предполагает подробное изучение видов и составов угроз, способов и методов защиты информации, выявление и предупреждение угроз в информационных системах.

В работе рассматривается основные понятия информационной безопасности, классификация и виды угроз в информационных системах, а также методы их защиты.

Глава 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Угрозы безопасности информации

С технологической точки зрения информация является продукцией информационных систем. Как и для всякого продукта, для информации большое значение имеет её качество, то есть способность удовлетворять определённые информационные потребности.

Качественная информация должен обладать следующими свойствами: своевременность, актуальность, полнота, доступность, достоверность, адекватность, физическая целостность информации, логическая целостность информации, безопасность информации и другие. Из перечисленных свойств безопасность информации является одним из наиболее существенным показателем её качества.

Рассмотрим данное свойство информации на примере защиты информации, хранящаяся, обрабатываемая и передаваемая в компьютерных системах. Данный вид информации имеет двоичное представление во всех системах обработки информации, а также имеется большом количестве в компьютерных системах.

Ценная и полезная информация на материальных носителях подлежащее к защите имеет степень полезности зависящее от её истинности или достоверности. А истинной информацией является та, которая с достаточной точностью отражает объекты и процессы окружающего мира в определённых временных и пространственных рамках. Если информация искажена, то она является дезинформацией. Если к информации ограничен доступ, то такая информация является конфиденциальной. Такая информация может содержать государственную или коммерческую тайну. Таким образом информация в компьютерных системах подлежат к защите со стороны руководства проведением соответствующего уровня политики информационной безопасности, обеспечивающее на требуемом уровне защиту информации от возможных угроз.

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.[1]

1.2. Классификация угроз информационной безопасности

Угрозы безопасности информационных систем классифицируются по нескольким признакам[2]:

- нарушение конфиденциальности информации;

- нарушение целостности информации;

- нарушение доступности системы (отказ в обслуживании);

- случайные воздействия;

- преднамеренные воздействия.

Угрозы нарушения конфиденциальности направлены на получение (хищение) конфиденциальной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. Несанкционированный доступ к информации, хранящейся в информационной системе или передаваемой по каналам (сетям) передачи данных, копирование этой информации является нарушением конфиденциальности информации.

Угрозы нарушения целостности информации, хранящейся в информационной системе или передаваемой посредством сети передачи данных, направлены на изменение или искажение данных, приводящее к нарушению качества или полному уничтожению информации. Целостность информации может быть нарушена намеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему (помехи). Эта угроза особенно актуальна для систем передачи информации – компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется авторизованными пользователями с обоснованной целью.

Угрозы нарушения доступности системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым её ресурсам.

Причины случайных воздействий:

- аварийные ситуации из-за стихийных бедствий и отключения электроэнергии;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линии связи из-за воздействия внешней среды, а также вследствие плотного трафика в системе (характерно для беспроводных решений).

Преднамеренные воздействия связаны с целенаправленными действиями злоумышленника, в качестве которого может выступить любое заинтересованное лицо (конкурент, посетитель, персонал и т.д.). Действия злоумышленника могут быть обусловлены разными мотивами: недовольством сотрудника своей карьерой, материальным интересом, любопытством, конкуренцией, стремлением самоутвердиться любой ценой и т.п.

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Причинами возникновения таких угроз может послужить нездоровый климат в коллективе или неудовлетворенность от выполняемой работы некоторых сотрудников, которые могут предпринять действия по выдаче информации лицам, заинтересованным в её получении.

Также имеет место так называемый "человеческий фактор", когда человек не умышленно, по ошибке, совершает действия, приводящие к разглашению конфиденциальной информации или к нарушению доступности информационной системы. Большую долю конфиденциальной информации злоумышленник (конкурент) может получить при несоблюдении работниками-пользователями компьютерных сетей элементарных правил защиты информации. Это может проявиться, например, в примитивности паролей или в том, что сложный пароль пользователь хранит на бумажном носителе на видном месте или же записывает в текстовый файл на жестком диске и пр. Утечка конфиденциальной информации может происходить при использовании незащищенных каналов связи, например, по телефонному соединению.

Под внешними угрозами безопасности понимаются угрозы, созданные сторонними лицами и исходящие из внешней среды, такие как:

- атаки из внешней сети (например, Интернет), направленные на искажение, уничтожение, хищение информации или приводящие к отказу в обслуживании информационных систем предприятия;
- распространение вредоносного программного обеспечения;
- нежелательные рассылки (спам);
- воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения в информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем;

- перехват информации с использованием радиоприемных устройств;
- воздействие на информацию, осуществляемое путем несанкционированного использования сетей инженерных коммуникаций;
- воздействие на персонал предприятия с целью получения конфиденциальной информации.

В электронных платежах, Интернет-магазинах, электронных очередях и т.п., увеличивается риск именно внешних угроз. При этом несанкционированный доступ, перехват, хищение информации, передаваемой по каналам связи, проводится средствами технической разведки, такими как радиоприемные устройства, средства съема акустической информации, системы перехвата сигналов с компьютерных сетей и контроля телекоммуникаций, средства съема информации с кабелей связи и другие.

1.3. Компьютерные вирусы и вредоносные программы

Вредоносные программы представляют очень серьезную опасность для информационных систем. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. В то же время чрезмерное преувеличение угрозы вирусов негативно влияет на использование всех возможностей компьютерной сети. Следует своевременно организовать противодействие вирусам и свести к минимуму вероятность заражения и нанесения вреда компьютерным системам и информации.

О наличии вредоносных программ можно судить по следующим признакам:

- появление сообщений антивирусных средств о заражении или о предполагаемом заражении, "самопроизвольное" отключение антивирусных программных средств;
- явные проявления присутствия вируса, такие как: сообщения, выдаваемые на монитор или принтер, звуковые эффекты, неожиданный запуск программ, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в системе;
- неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств компьютерной системы – увеличение времени обработки той или иной

информации, необоснованное уменьшение свободного объёма на дисковых носителях, отказ выполнять программы-сканеры вирусной активности, зависание системы;
- рассылка писем, которые пользователем не отправлялись, по электронной почте и т.п.

Вредоносная программа может получить несанкционированный доступ на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа. Общепризнанной классификации вредоносного программного обеспечения пока не существует.

Вредоносные программы включают следующие категории: компьютерные вирусы и черви; троянские программы; подозрительные упаковщики и вредоносные утилиты.

Компьютерные вирусы – это небольшие исполняемые или интерпретируемые программы, обладающие свойством несанкционированного пользователем распространения и самовоспроизведения в компьютерах или компьютерных сетях. Полученные копии также обладают этой возможностью. Вирус может быть запрограммирован на изменение или уничтожение программного обеспечения или данных, хранящихся на объектах и устройствах компьютерной сети. В процессе распространения вирусы могут себя модифицировать.

Черви считаются тоже вирусами, но обладают характерными особенностями. Червь размножается, не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры. Червь – это отдельный файл, в то время как вирус – это код, который внедряется в существующие файлы.

Копия вируса попадает на другие компьютеры только в том случае, если заражённый объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

Черви ищут в сети удаленные компьютеры и копируют себя в каталоги, открытые на чтение и запись (если таковые обнаружены). При этом черви данного типа перебирают доступные сетевые каталоги, используя функции операционной

системы, и случайным образом ищут компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ.

Есть много видов червей, таких как, сетевой червь почтовый червь P2P-червь IM-червь IRC-червь и т.д.

Серьезную опасность для компьютерных систем также представляют поддельные антивирусы, размещенные на специально подготовленных сайтах и которые злоумышленники предлагают загрузить для "лечения" компьютера от вирусов. Как правило, сами эти сайты не опасны, но загружаемые оттуда программы-антивирусы содержат вредоносные коды сетевых червей или троянских программ.

Троянские программы внешне выглядят как легальный программный продукт, но при запуске осуществляют несанкционированные пользователем действия, направленные на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Существует большое разнообразие троянских программ выполняющих те или иные действия и отличающихся друг от друга целями и способами воздействия на "жертву"[3]. Рассмотрим некоторые типы троянских программ:

- Trojan-Banker – предназначена для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт.
- Trojan-Dropper – предназначена для несанкционированной пользователем скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в теле этого типа троянцев.
- Trojan-Proxy – предназначена для осуществления злоумышленником несанкционированного пользователем анонимного доступа к различным Интернет-ресурсам через компьютер-жертву.
- Trojan-Mailfinder – предназначена для несанкционированного пользователем сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику.
- Trojan-Clicker – предназначена для несанкционированного пользователем обращения к Интернет-ресурсам (обычно, к Web-страницам).

- Trojan-GameThief – предназначена для кражи пользовательской информации, относящейся к сетевым играм. Найденная информация передается злоумышленнику.
- Trojan-Ransom – предназначена для несанкционированной пользователем модификации данных на компьютере-жертве таким образом, чтобы сделать невозможным работу с ними, либо блокировать нормальную работу компьютера. После того как данные взяты злоумышленником под контроль, пользователю выдвигается требование выкупа.
- Trojan-PSW – предназначена для кражи пользовательских аккаунтов (логин и пароль) с пораженных компьютеров. Название PSW произошло от Password-Stealing-Ware.
- Trojan-DDoS – предназначена для проведения несанкционированной пользователем DoS-атаки с пораженного компьютера на компьютер-жертву по заранее определенному адресу.
- Trojan-IM – предназначена для кражи пользовательских аккаунтов (логин и пароль) от Интернет-пейджеров (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.).
- Trojan-SMS – предназначена для несанкционированной пользователем отсылки SMS-сообщений с пораженных мобильных устройств на дорогостоящие платные номера, которые "жестко" записаны в теле вредоносной программы.
- Trojan-ArcBomb – эти троянцы представляют собой архивы, специально сформированные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные – зависание или существенное замедление работы компьютера или заполнение диска большим количеством "пустых" данных. Особенно опасны "архивные бомбы" для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации – архивная бомба может просто остановить работу сервера.
- Trojan-Downloader – предназначена для несанкционированной пользователем загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки троянцев или рекламных систем. Загруженные из Интернета программы либо запускаются на выполнение, либо регистрируются троянцем на автозагрузку в соответствии с возможностями операционной системы.
- Trojan-Notifier – предназначена для несанкционированного пользователем сообщения своему "хозяину" о том, что заражённый компьютер сейчас находится "на связи". При этом на адрес злоумышленника отправляется

информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т.п.
- Trojan-Spy – предназначена для ведения электронного шпионажа за пользователем (вводимая с клавиатуры информация, снимки экрана, список активных приложений и т.д.). Найденная информация передается злоумышленнику.

1.4. Подозрительные упаковщики и вредоносные утилиты

Вредоносные программы часто сжимаются специфичными способами упаковки, включая использование многократных упаковщиков и совмещая упаковку с шифрованием содержимого файла для того, чтобы при распаковке усложнить анализ файла эвристическими методами.

К данному подклассу вредоносных программ относятся:

- MultiPacked – файловые объекты, многократно упакованные различными программами упаковки. Антивирус при детектировании такого объекта обнаруживает исполняемый файл, упакованный одновременно тремя и более упаковщиками.
- SuspiciousPacker – файловые объекты, сжатые специальными программами-упаковщиками, которые созданы для защиты вредоносного кода от детектирования антивирусным ПО.
- RarePacker – файловые объекты, сжатые различными редко встречающимися упаковщиками, например, реализовывающими какую-либо конкретную идею.

В отличие от вирусов, червей и троянских программ, вредоносные утилиты не представляют угрозы непосредственно компьютеру, на котором исполняются. Основным признаком, по которому различают вредоносные утилиты, являются совершаемые ими действия.

К данной категории вредоносных программ относятся:

- Constructor – программы, предназначенные для изготовления новых компьютерных вирусов, червей и троянских программ.
- HackTool – программы, используемые злоумышленниками при организации атак на локальный или удаленный компьютер (например,

несанкционированное пользователем внесение нелегального пользователя в список разрешенных посетителей системы; очистка системных журналов с целью сокрытия следов присутствия в системе; снифферы с выраженным вредоносным функционалом и т.д.).
- Spoofer – программы, позволяющие отправлять сообщения и сетевые запросы с поддельным адресом отправителя.
- DoS – программы, предназначенные для проведения DoS-атак на компьютер-жертву.
- Hoax – программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности.
- irToolV – программы, позволяющие злоумышленнику модифицировать другие вредоносные программы таким образом, чтобы они не детектировались антивирусным программным обеспечением.
- Flooder – программы, функцией которых является "забивание" бесполезными сообщениями сетевых каналов, отличных от почтовых, Интернет-пейджеров и SMS (например, IRC).
- Email-Flooder, IM-Flooder, SMS-Flooder – программы, функцией которых является "забивание" бесполезными сообщениями каналов электронной почты, каналов Интернет-пейджеров (ICQ, MSN Messenger и др.) и каналов передачи SMS-сообщений.

Вредоносные программы создаются для компьютерных систем определенного типа, работающих с конкретными операционными системами. Привлекательность ОС для создателей вирусов определяется следующими факторами:

- распространенность ОС;
- отсутствие встроенных антивирусных механизмов;
- относительная простота;
- продолжительность эксплуатации.

Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру.

Глава 2. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Классификация методов обеспечения безопасности информации

Методы и средства обеспечения информационной безопасности условно можно классифицировать следующим образом[4]:

1) средства защиты от несанкционированного доступа:

а) средства авторизации;

б) аудит;

2) системы мониторинга сетей:

а) системы мониторинга сетей;

б) анализаторы протоколов;

3) антивирусные средства:

а) антивирусные программы;

б) программные и иные антиспамовые средства;

в) межсетевые экраны;

4) криптографические средства:

а) шифрование данных;

б) электронная цифровая подпись;

5) системы бесперебойного питания;

6) системы аутентификации:

а) пароль;

б) ключ доступа (физический или электронный);

в) биометрия (анализаторы отпечатков пальцев, анализаторы

сетчатки глаза, анализаторы голоса, анализаторы геометрии ладони и др.).

2.1.1. Средства защиты от несанкционированного доступа

Безопасности операционных систем обусловлено их архитектурными особенностями и связано с правильной организацией идентификации и аутентификации, авторизации и аудита. Наиболее простой подход к аутентификации - применение пользовательского пароля. Для защиты аппаратных и программных средств устанавливаются права доступа к нему. Набор прав доступа определяет домен безопасности. Формальное описание модели защиты осуществляется с помощью матрицы доступа, которая может храниться в виде списков прав доступа или перечней возможностей.

Аудит системы заключается в регистрации специальных данных о различных событиях, происходящих в системе и так или иначе влияющих на состояние безопасности компьютерной системы.

Авторизацию используют для разграничение доступа к объектам ОС. Средства авторизации контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые были определены администратором, а также осуществляют контроль возможности выполнения пользователем различных системных функций.

Различают дискреционный способ управления доступом и полномочный. В первом случае определенные операции над конкретным ресурсом запрещаются или разрешаются пользователям или процессам, т.е. текущее состояние прав доступа описывается матрицей, в строках которой перечислены процессы или пользователи, в столбцах - процессор, сегменты памяти, принтер, диски и ленты объекты, файлы или программы, а в ячейках – операции (чтение, запись, добавление, удаление, изменение и т.д.).

Полномочный подход заключается в том, что все пользователи или процессы могут иметь уровни секретности и должна обеспечивать простое свойство секретности, т.е. пользователи или процессы может читать информацию только из объекта, уровень секретности которого не выше уровня секретности другого пользователя или процесса.

Но данные модель не гарантирует целостности данных. Например, пользователь с нижней привилегией имеет право писать в файлы пользователя с высшей

привилегией.

Обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения. Как правило, поведение взломщика отличается от поведения легального пользователя. Иногда эти различия можно выразить количественно, например, подсчитывая число некорректных вводов пароля во время регистрации.

Основным инструментом выявления вторжений является запись данных аудита. Отдельные действия пользователей протоколируются, а полученный протокол используется для выявления вторжений.

К числу таких действий относится следующие:

- вход или выход из системы;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- обращение к удаленной системе;
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Среди современных ОС вопросы безопасности лучше всего продуманы в ОС Windows NT.

Windows NT отслеживает и контролирует доступ как к объектам, которые пользователь может видеть посредством интерфейса (такие, как файлы и принтеры), так и к объектам, которые пользователь не может видеть (например, процессы и именованные каналы).

Система защиты ОС Windows NT состоит из следующих компонентов:

- Процедуры регистрации (Logon Processes), которые обрабатывают запросы пользователей на вход в систему. Они включают в себя начальную интерактивную процедуру, отображающую начальный диалог с пользователем на экране и удаленные процедуры входа, которые позволяют удаленным пользователям получить доступ с рабочей станции сети к серверным процессам Windows NT.
- Подсистемы локальной авторизации (Local Security Authority, LSA), которая гарантирует, что пользователь имеет разрешение на доступ в систему. Этот компонент - центральный для системы защиты Windows NT. Он порождает

маркеры доступа, управляет локальной политикой безопасности и предоставляет интерактивным пользователям аутентификационные услуги. LSA также контролирует политику аудита и ведет журнал, в котором сохраняются сообщения, порождаемые диспетчером доступа.
- Менеджера учета (Security Account Manager, SAM), который управляет базой данных учета пользователей. Эта база данных содержит информацию обо всех пользователях и группах пользователей. SAM предоставляет услуги по легализации пользователей, применяющиеся в LSA.
- Диспетчера доступа (Security Reference Monitor, SRM), который проверяет, имеет ли пользователь право на доступ к объекту и на выполнение тех действий, которые он пытается совершить. Этот компонент обеспечивает легализацию доступа и политику аудита, определяемые LSA. Он предоставляет услуги для программ супервизорного и пользовательского режимов, для того чтобы гарантировать, что пользователи и процессы, осуществляющие попытки доступа к объекту, имеют необходимые права.

2.1.2. Системы мониторинга сетей

Мониторинг сетевых устройств — это постоянное наблюдение за деятельностью данных устройств, поиск проблем и неисправностей в их работе, принятие решений о ликвидации проблем и неисправностей, повышению эффективности функционирования устройств.

Одно из самых часто используемых и наиболее важных средств мониторинга системы — это регистрация различных событий в журналах операционной системы Windows. Регистрацию событий в системе Windows осуществляет служба " Журнал событий " (Event Log).

В любой системе семейства Windows всегда присутствуют 3 журнала:

- журнал System (" system32\config\SysEvent.Evt ") - события, записанные в журнал компонентами ОС (например, сбой в запуске службы при перезагрузке);;
- журнал Security ("system 32\config\SecEvent.Evt ") - регистрация событий, относящихся к системе безопасности (например, попытки регистрации пользователей, изменения в политиках безопасности, попытки доступа к различным ресурсам);

- журнал Application (" system32\config\AppEvent.Evt ") — события, порожденные различными приложениями (например, сбой MS SQL при доступе к базе данных);

При установке в системе каких-либо компонент могут появиться журналы, регистрирующие события, относящиеся к работе данных компонент. Например, при установке службы DNS появляется журнал DNS-сервер ("system32\config\DNSEvent.Evt "), регистрирующий события, связанные с работой службы DNS.

При создании контроллера домена в системе появляются журналы:

- журнал Directory Service;
- журнал File Replication Service.

Системные журналы можно можно открыть так:

- открыть консоль " Управление компьютером " и в разделе " Служебные программы " открыть оснастку " Просмотр событий ";

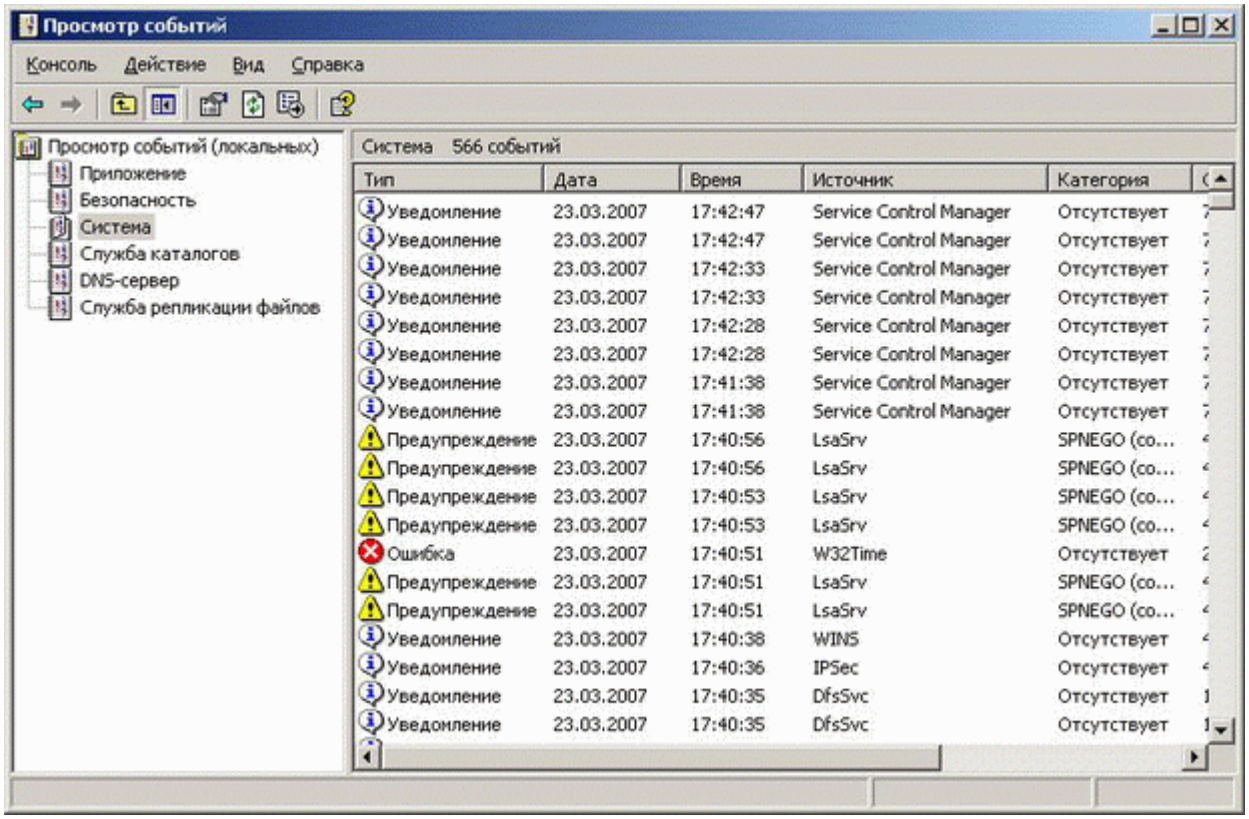

Рисунок 1. **Оснастка «Просмотр событий»**

В большинстве журналов события бывают трех видов:

- уведомление — информация о событии, связанным с успешным действием (например, успешный запуск или останов службы, успешное завершение операции какой-либо службы);
- предупреждение — информация о событиях, которые в будущем могут вызвать проблемы в работе системы;
- ошибка — сообщение об ошибке (например, сбой при запуске службы).

В журнале " Безопасность " — 2 типа событий:

- Аудит успехов — событие, связанное с успешным выполнением действия, связанного с системой безопасности (например, успешный вход в систему или успешный доступ к сетевому ресурсу);
- Аудит отказов — событие, связанное со сбоем в выполнении действия, связанного с системой безопасности (например, отказ в аутентификации пользователя при входе в систему по причине ввода неверного пароля, блокировка учетной записи после нескольких неудачных попыток входа в систему, отказ в доступе к сетевому ресурсу).

В столбцах журнала, кроме типа события, содержатся следующие данные:

- Дата и время регистрации события;
- Источник — приложение, служба или системная компонента, записавшие событие в журнал;
- Категория — категория события, иногда используемая для его более подробного описания;
- Событие — код события;
- Пользователь — учетная запись пользователя, действовавшая в момент события;
- Компьютер — имя компьютера, на котором произошло событие.

Системы обнаружения вторжений (IDS) используются также для мониторинга сетей и оповещения в реальном времени о событии, представляющем интерес для лиц, обеспечивающих безопасность. Использование узловой системы обнаружения вторжений помогает при проверке журналов аудита, дает возможность просмотра файлов журналов. Сетевая IDS используется для мониторинга сети на предмет атак или трафика посредством выдачи предупреждений и оповещений при наличии необычной активности в системе.

2.1.3. Самостоятельное обнаружение вредоносных программ

В общем случае за обнаружение присутствия вирусов на компьютере должны отвечать антивирусы. Однако известно, что ни один антивирус не обеспечивает полную защиту от всех вредоносных программ. Следовательно, возможно заражение компьютера, даже если на нем установлен антивирус. При отсутствии антивируса, вероятность проникновения на компьютер вредоносных программ многократно возрастает.

Прежде чем судить о подозрительности файлов и процессов, нужно сначала их выделить из общего числа. Чтобы получить список процессов, нужно вызвать диспетчер задач комбинацией клавиш Ctrl + Shift + Esc или вызвать контекстное меню в системной панели и выбрать пункт Диспетчер задач.

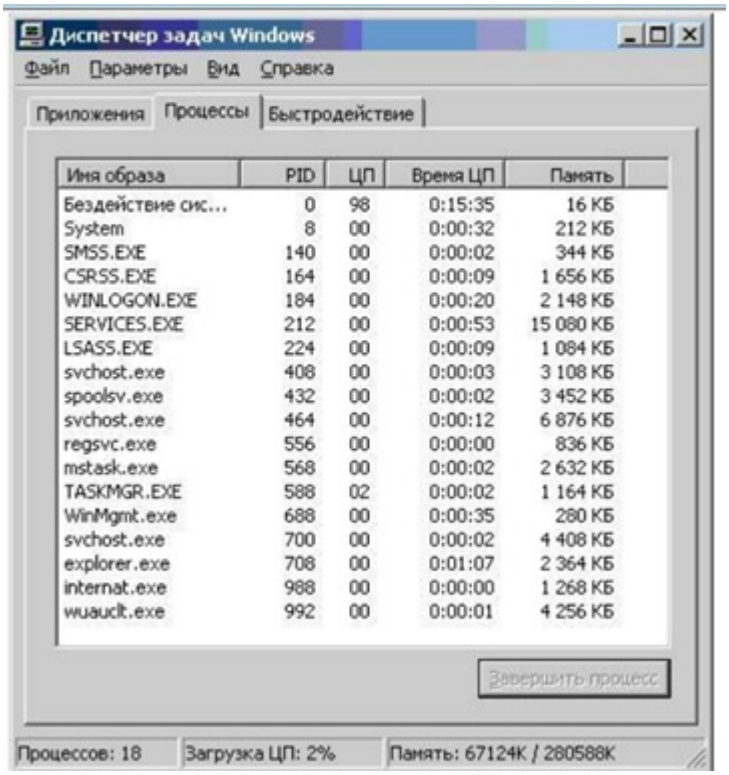

Рисунок 2.**Диспетчер задач**

Процессы, которые видны на рисунке являются стандартными для Windows.

Самостоятельно запускающие файлы ищем в системном реестре. Системный реестр Windows - это основное хранилище большинства настроек операционной системы и многих приложений. Для доступа к системному реестру используется

системная утилита regedit.exe.

В зависимости от настроек Windows и установленных программ ключи автозапуска могут содержать множество различных строк для запуска различных программ. Поэтому все на первый взгляд подозрительные файлы нужно перепроверять - они могут оказаться вполне обычными программами.

Ни в коем случае не следует изменять настройки системного реестра наугад - это может привести к полной неработоспособности компьютера и необходимости переустанавливать операционную систему. Вносить изменения в реестр можно только будучи абсолютно уверенным в своих действиях.

Настроить автозапуск программ можно и в системных файлах Windows - system.ini и win.ini.

В файле system.ini есть строка, через которую чаще всего запускаются вирусы, расположена в секции [boot]:

shell =<имя программной оболочки Windows>

Во всех версиях Windows стандартной программной оболочкой является explorer.exe. Если в строке shell= указано что-то отличное от explorer.exe, это с большой вероятностью вредоносная программа.

Чтобы собирать информацию об автоматически запускаемых приложениях из разных источников, можно воспользоваться системной утилитой msconfig.exe.

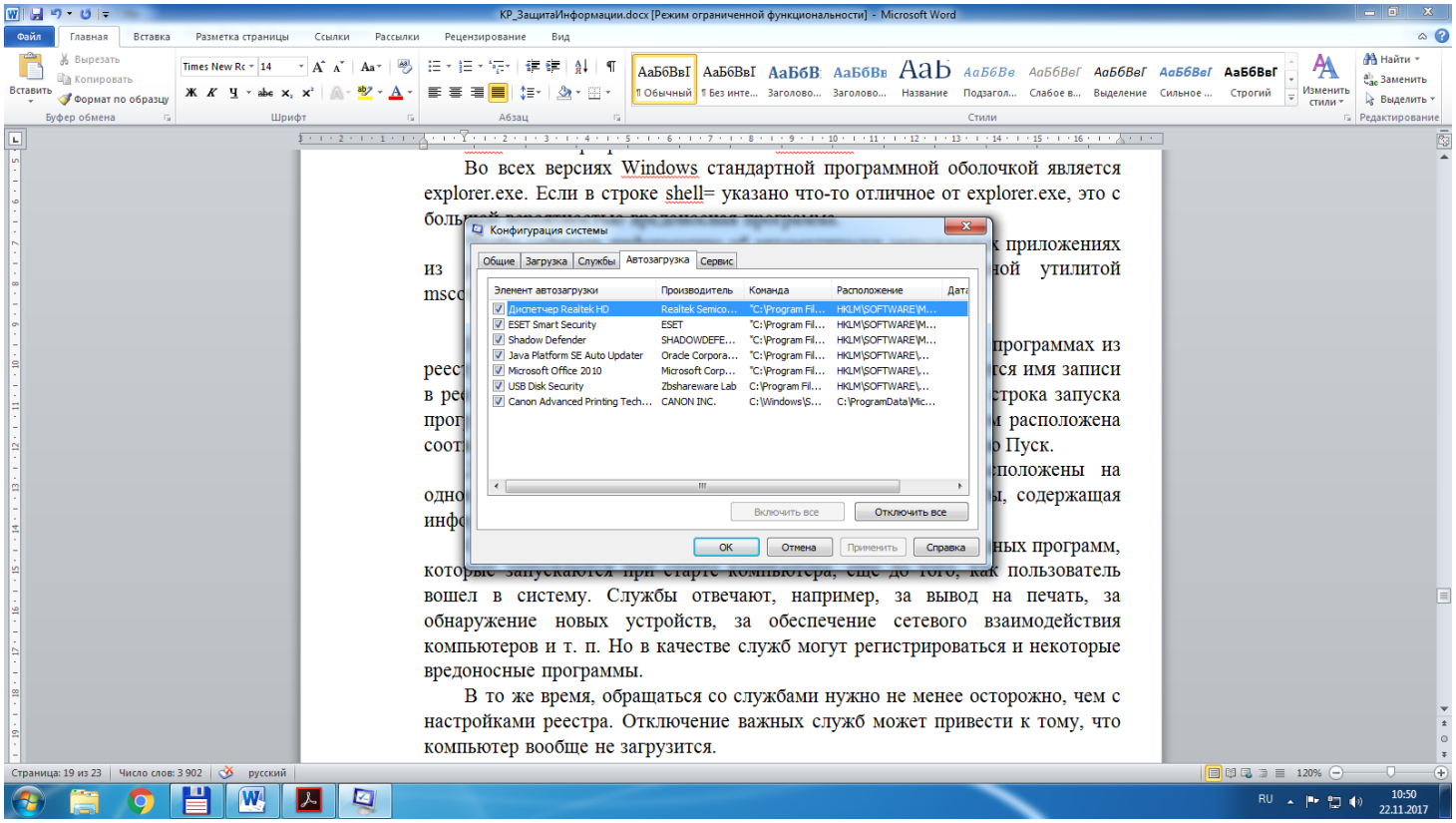

Рисунок 3. **Утилита msconfig.exe**

На закладке Автозагрузка собраны данные о запускаемых программах из реестра и меню Пуск. В колонке Элемент автозагрузки приводится имя записи в реестре или имя ярлыка в меню Пуск. В колонке Команда - строка запуска программы, в колонке Расположение - ключ реестра, в котором расположена соответствующая запись, или Common Startup - для ярлыков меню Пуск.

Данные о настройках файлов system.ini и win.ini расположены на одноименных закладках. Кроме этого имеется закладка Службы, содержащая информацию о запускаемых службах в Windows XP.

Службы - это служебные компоненты Windows или прикладных программ, которые запускаются при старте компьютера, еще до того, как пользователь вошел в систему. Службы отвечают, например, за вывод на печать, за обнаружение новых устройств, за обеспечение сетевого взаимодействия компьютеров и т. п. Но в качестве служб могут регистрироваться и некоторые вредоносные программы.

Обращаться со службами нужно осторожно, потому что отключение важных служб может привести к тому, что компьютер вообще не загрузится.

2.1.4. Антивирусные средства

Из всех методов антивирусной защиты можно выделить две основные группы:

- сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов
- эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами.

Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют антивирусную базу. Лучшим антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех.

Для получения сигнатуры необходимо иметь образец вируса, поэтому сигнатурный метод непригоден для защиты от новых вирусов, т. к. до тех пор, пока вирус не попал на анализ к экспертам, создать его сигнатуру невозможно. Именно поэтому все наиболее крупные эпидемии вызываются новыми вирусами. В защите от новых вирусов помогают дополнительные средства защиты, рассмотренные выше, а также эвристические методы, используемые в антивирусных программах.

Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных.

По этому методу определяют вредоносные программы так или иначе стремятся нанести вред компьютеру, т.е. не выполняют ли такие вредоносные действия как, например:

- Удаление файла
- Запись в файл
- Запись в определенные области системного реестра

- Открытие порта на прослушивание
- Перехват данных вводимых с клавиатуры
- Рассылка писем

Каждый антивирус должен содержать модуль обновления. Для того чтобы сигнатурный анализ эффективно справлялся с самыми последними вирусами, антивирусные эксперты постоянно анализируют образцы новых вирусов и выпускают для них сигнатуры.

Во многих антивирусах есть специальные технологии, которые защищают от возможной потери данных в результате действий антивируса. Перед лечением или удалением файлов следует сохранить их резервные копии, тогда если окажется, что файл был удален ошибочно или была потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

С помощью антивирусной программы также можно защитить данные не следующих уровнях:

- Уровень защиты рабочих станций и сетевых серверов
- Уровень защиты почтовых серверов
- Уровень защиты шлюзов

2.1.5. Криптографические средства

Основным достоинством криптографических методов является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме. Однако, и этот метод имеет свои недостатки к которым относится:

- значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
- трудности совместного использования зашифрованной (подписанной) информации, связанные с управлением ключами (генерация, распределение и т.д.);
- высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.

Криптография делится на два класса: криптография с симметричными ключами и криптография с открытыми ключами.

В криптографии с симметричными ключами абоненты используют один и тот же (общий) ключ (секретный элемент) как для шифрования, так и для расшифрования данных. Их преимущества состоит в относительно высокой производительности алгоритмов, высокой криптографической стойкости алгоритмов на единицу длины ключа.

В криптографии с открытыми ключами используется не один секретный, а пара ключей: открытый (публичный) ключ и секретный (личный, индивидуальный) ключ, известный только одной взаимодействующей стороне. В отличие от секретного ключа, который должен сохраняться в тайне, открытый ключ может распространяться публично. Зашифрованный файл может быть прочитан только владельцем секретного ключа, т.е. получателем.

Для реализации юридически значимого электронного взаимодействия двух сторон необходимо заключить договор, предусматривающий обмен сертификатами. Сертификат представляет собой документ, связывающий личностные данные владельца и его открытый ключ. В бумажном виде он должен содержать рукописные подписи уполномоченных лиц и печати.

Эта процедура заключается в том, что каждая сторона при личной встрече удостоверяет подписью уполномоченного лица и печатью бумажный документ - распечатку содержимого открытого ключа другой стороны. Этот бумажный сертификат является, во-первых, обязательством стороны использовать для проверки подписи под входящими сообщениями данный ключ, и, во-вторых, обеспечивает юридическую значимость взаимодействия. Действительно, рассмотренные бумажные сертификаты позволяют однозначно идентифицировать мошенника среди двух партнеров, если один из них захочет подменить ключи.

В системах, где отсутствует возможность предварительного личного контакта партнеров, необходимо использовать цифровые сертификаты удостоверяющего или сертификационного центра.

2.1.6. Системы бесперебойного питания и системы аутентификации

Для обеспечения бесперебойного питания используются современные и мощные источники бесперебойного питания. В основном используются источники бесперебойного питания, выполненные по технологии двойного преобразования

(online). Они легко сочетаются с дизель-генераторными установками, которые являются неотъемлемой частью системы электропитания. Когда перебои в электроэнергии составляют небольшое количество времени, источник бесперебойного питания может обеспечить электропитанием в течение 40-60 минут. За это время для защиты информации можно резервировать необходимые данные.

Текстовый ввод логина и пароля вовсе не является единственным методом аутентификации. Всё большую популярность набирает аутентификация с помощью электронных сертификатов, пластиковых карт и биометрических устройств, например, сканеров радужной оболочки глаза, отпечатков пальцев или ладони.

Всё чаще применяется расширенная или многофакторная аутентификация. Она построена на использовании нескольких компонент, таких как: информация, которую пользователь знает (пароль), использовании физических компонентов (например, идентификационные брелоки или смарт-карты), и технологии идентификации личности (биометрические данные).

В процедуре аутентификации при этом используются весьма сложные криптографические протоколы, обеспечивающие защиту линии связи от прослушивания или подмены одного из участников взаимодействия.

ЗАКЛЮЧЕНИЕ

В настоящее время актуальность защиты информации связана с ростом возможностей вычислительной техники. Развитие информационных технологий достигло такого высокого уровня, что сегодняшнюю деятельность любого предприятия в целом и каждого пользователя в отдельности, уже невозможно представить без электронной почты, Web-рекламы, общения в режиме «online».

Поэтому защита информации – это более важная задача для любой компании. Ведь когда кампания начинает расти, то поток обрабатываемой информации увеличивается, за счет этого нагрузка на корпоративные вычислительные сети становится все более высокой, как и ценность самой информации.

Для защиты, обработки и хранения информации следует создать специальные Data-центры, в котором имеются мощные серверы, обеспечивающее хранение и обработку информации, сетевое оборудование, отвечающее за обмен данными с

внешним миров, инженерные системы, обеспечивающие жизнедеятельность Data-центра, системы безопасности, которые защищают Data-центры от нежелательных вторжений.

В работе мною были рассмотрены виды и состав угроз, способы и методы защиты информации, проанализированы угрозы, рассмотрены методы и средства защиты информации. И все эти проблемы можно решить созданием Data-цента, основной функцией которого будет - повышение надежности обработки и хранения информации. Такой центр дает возможность хранить и не терять важную информацию на протяжении всего ее жизненного цикла.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Галатенко В.А. Стандарты информационной безопасности: курс лекций: учебное пособие/ Второе издание. Под редакцией академика РАН Бетелина В,Б./ – М.:ИНТУИТ.РУ «Интернет-университет информационных технологий”, 2006.
2. Мэйволд Эрик. Безопасность сетей. Практическое пособие. Серия «Шаг за шагом» / Пер. с англ. – М.: «СП ЭКОМ», 2008.
3. Новиков Е.А., Шитов Ю.А. Криптографические методы защиты информации. – Красноярск – 2008. – С.178.
4. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. М.:Нац-ный Открытый Университет ИНТУИТ», 2016.
5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. Пособие.- М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства – М:. ДМК Пресс, 2008.

ЭЛЕКТРОННЫЕ РЕСУРСЫ

http://www.microsoft.com 18.10.2017 10:25

http://www.securitylab.ru 18.10.2017 15:40

https://ru.wikipedia.org/wiki 20.10.2017 9:45

1. http://works.doklad.ru/view/pgyTBEd7SsI.html 22.10.2017 11:20

1. https://ru.wikipedia.org/wiki 20.10.2017 9:45 ↑

2. А.В. Пролетарский, А.М. Суровов, Е.В. Смирнова, Н.А. Руденков. Технологии защиты информации в компьютерных сетях. ↑

3. http://works.doklad.ru/view/pgyTBEd7SsI.html 22.10.2017 11:20 ↑

4. Э. Мэйволд . Network Security: A Beginner's Guide ↑