Основы защиты информации и сведений, составляющих государственную тайну.

Методы защиты информации

Информационная безопасность и ее составляющие
Защита от несанкционированного вмешательства
Компьютерные вирусы и средства антивирусной защиты
Специфика обработки конфиденциальной информации

Введение

- Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум разрешая одни проблемы непременно сталкивается при этом с другими новыми и этот процесс обречен на бесконечность в своей последовательности. Хотя если уж быть точным новые проблемы это всего лишь обновленная форма старых. Вечная проблема **защита информации.** На различных этапах своего развития человечество решало эту проблему.
- В современном мире - информация стратегический национальный ресурс, одно из основных богатств экономически развитого государства.
- Компьютерные преступления приобрели в странах с развитой информационно телекоммуникационной инфраструктурой широкое распространение.

Что такое защита информации

*Под **защитой информации*** понимается обеспечение ее сохранности на машинных носителях и запрет несанкционированного доступа к ней.

Защита информации обеспечивается:

- резервированием файлов;
- архивным копированием файлов;
- ограничением доступа к информации;
- применением антивирусных средств.

Резервирование файлов

Резервированием файлов называют создание их копий на машинных носителях информации и систематическое их обновление в случае изменения резервируемых файлов.

Необходимость резервирования вызывается различными обстоятельствами. Например, жесткий диск может быть полностью заполнен, и на него нельзя будет записать новую информацию без разрушения старой. Или при работе ЭВМ может произойти порча или полное разрушение информации на дисках. Это может случиться по разным причинам:

- воздействие компьютерных вирусов;
- неправильные действия или случайное уничтожение файлов;
- физическая порча диска или дисковода жесткого диска;
- умышленные действия некоторых лиц.

В этом способе резервирования получается простая копия одного или нескольких файлов или файловой структуры, то есть дерева каталогов с входящими в них файлами на том же или другом носителе информации (диске, магнитной ленте, CD, flesh и т.д.).Резервные копии занимают столько же места, сколько занимают исходные файлы.

В MS-DOS – это команды COPY, XCOPY, DISKCOPY. В - Norton Commander, FAR и др. – есть аналогичные команды.

Копирование файлов, каталогов и дисков в Windows выполняется при помощи буфера обмена или другим способом.

Резервирование файлов применяется также при транспортировке файлов с одной ЭВМ на другую, если они не объединены в сеть.

Архивное копирование файлов

- Основная особенность архивного копирования файлов — это сжатие файлов с целью уменьшения занимаемого архивной копией пространства на машинном носителе информации.
- При таком резервировании создается один архивный файл, представляющий собой набор из одного или нескольких сжатых файлов, откуда их можно извлечь в первоначальном виде. Размер сжатого файла от двух до десяти раз меньше размера файла-оригинала.
- Степень сжатия зависит, во-первых, от типа файла, а во-вторых, от программы-архиватора. Больше всех сжимаются файлы баз данных и текстовые файлы, а меньше всех — двоичные программные файлы (типа EXE и COM).
- Процесс записи файлов в архивный файл называется ***архивированием (упаковкой),*** извлечение файлов из архива — ***разархивированием (распаковк****ой),* а архивный файл — ***архивом.***

Архив

Архивный файл содержит оглавление, позволяющее узнать, какие файлы содержатся в архиве. Некоторые архиваторы могут создавать многотомные архивы, размещающиеся на нескольких дискетах, если архивный файл не помещается на одной дискете.

Архивирование производится при помощи программ-архиваторов. Наиболее распространенные программы-архиваторы имеют приблизительно одинаковые возможности, и ни одна из них не превосходит другие по всем параметрам: одни программы работают быстрее, другие обеспечивают лучшую степень сжатия файлов.

Функции, выполняемые архиватором:

- помещение файлов в архив;
- извлечение файлов из архива;
- просмотр оглавления архива;
- пересылка файлов в архив и из архива (после пересылки файлы из источника удаляются);
- архивирование каталогов;
- проверка целостности архива;
- восстановление поврежденных архивов;
- защита архивов с помощью пароля.

Ограничение доступа к информации

Под ***ограничением доступа к информации*** понимается исключение несанкционированного доступа к ней.

Оно обеспечивается программными и техническими средствами:

- применение ***паролей,***
- ***шифрование файлов,***
- ***уничтожение*** файлов после их удаления,
- использование ***электронных ключей,***
- изготовление ЭВМ в специальном ***защищенном*** исполнении.

Пароли

Пароли применяются для идентификации пользователей и разграничения их прав в сети ЭВМ и для ограничения доступа пользователей, работающих на одной ЭВМ, к различным логическим дискам, каталогам и файлам.

Могут быть установлены различные уровни парольной защиты. Например, чтение диска возможно без ввода пароля, а для изменения, удаления или сохранения файла на защищенном диске пароль нужен.

Парольная защита файлов не предполагает обязательное их шифрование.

Шифрование

Шифрование — такое преобразование данных, в результате которого их можно прочесть только при помощи ключа.

Шифрованием занимается наука, которая называется ***криптографией***.

В криптографии любой незашифрованный текст называется *открытым* текстом, а зашифрованные данные называются *зашифрованным* текстом.

Современные алгоритмы шифрования представляют собой сложную математическую задачу, для решения которой без знания дешифрующего ключа требуется выполнить гигантский объем вычислений и получить ответ, возможно, через несколько лет.

Защита дисков

При включении ***защиты дисков*** от несанкциониро-ванной записи в память загружается резидентный модуль, который выводит на экран сообщение о попытке записи.

В ответ пользователь должен разрешить или запретить запись. Такой вид защиты уменьшает вероятность разрушения информации из-за ошибочных действий пользователя, а также позволяет обнаружить возможные действия вирусов.

Отображение (визуализация) процесса чтения или записи на диск обращает внимание пользователя на этот процесс, чтобы пользователь мог оценить правомерность доступа к диску.

Защита локальной сети

Для защиты локальной сети от попыток несанкционированного доступа, в том числе через глобальную сеть, например Internet, применяются специальные программные (и/или аппаратные) средства, называемые ***брандмауэрами.***

Среди функций, выполняемых брандмауэрами, — аутентификация пользователей и контроль за содержанием информационного потока на основе заданных правил.

Электронные ключи

Электронные ключи относятся к аппаратным средствам защиты программ и данных.

Электронный ключ представляет собой специализированную заказную микросхему (чип) с площадью размером немного больше спичечного коробка.

Ключ имеет два разъема; одним он подключается к параллельному порту компьютера, а другой служит для подключения принтера. При этом ключ не мешает нормальной работе принтера. Ключ сохраняет записанную в него информацию при отключении его от компьютера.

Если электронный ключ защищает программу, то последняя при ее запуске проверяет наличие «своего» ключа. Если такой ключ найден, программа выполняется, иначе она выдает сообщение об ошибке и прерывает свою работу. В защитном механизме электронного ключа может быть реализована защита файлов баз данных.

Применение программно-аппаратных комплексов

Перспективным направлением является применение программно-аппаратных комплексов защиты, которые выполняют следующие функции защиты:

- обеспечение возможности доступа к компьютеру и загрузки операционной системы только по предъявлению личной электронной карты пользователя (электронного ключа) Touch Memory и вводу личного пароля;
- уничтожение полиморфных вирусов (мутантов); защиту системных файлов операционной системы;
- автоматическую и принудительную блокировку компьютера с гашением экрана дисплея на время отсутствия пользователя;
- обеспечение возможности уничтожения файлов при их удалении;
- защиту файлов пользователя от несанкционированного доступа и контроль целостности дисков;
- сохранение образа системных областей компьютера на дискете;
- разграничение полномочий пользователей по доступу к ресурсам компьютера;
- регистрацию в системных журналах всех событий по входу, выходу и работе пользователей.

Кроме того, комплекс оснащен дополнительными утилитами, расширяющими возможности защиты компьютера:

- мощная защита от вирусов;
- возможность создания дополнительных защищенных логических разделов и каталогов пользователей, защита при помощи индивидуального пароля пользователя;
- шифрование файлов для их надежного хранения.

Защищенное изготовление ЭВМ

ЭВМ, изготовленные в специальном защищенном исполнении, излучение информационных сигналов на уровне естественного шума. Такая мера защиты противодействует попыткам получить дистанционный доступ к конфиденциальной информации при помощи специальной подслушивающей аппаратуры.

Кроме этого предусмотрены:

- средства криптографической защиты;
- система разграничения доступа с электронным ключом Touch Memory;
- съемный накопитель на жестком магнитном диске.

Специфика обработки конфиденциальной информации

- Применение криптографии (тайнопись) – специальная система изменения обычного письма с целью сделать текст понятным лишь для ограниченного числа лиц, знающих эту систему,
- Применение стеганографии (👉),
- Использование электронной цифровой подписи и т.д.

Стеганографические системы

- Задача надежной защиты информации от несанкционированного доступа является одной из древнейших и нерешенных до настоящего времени проблем.
- В современном понимании ***стеганографическая система*** (или просто *стегосистема*) – это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации. Общий процесс стеганографии выражается простой формулой:

Контейнер + скрываемое сообщение + стегоключ = стегоконтейнер

- *Контейнер* - любая информация, предназначенная для сокрытия тайных сообщений.
- *Скрываемое (встраиваемое) сообщение* – тайное сообщение, встраиваемое в контейнер.
- *Стегоключ* - секретный ключ, необходимый для скрытия (шифрования) информации.

Стеганографический канал

- В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.
- *Стегоконтейнер* – контейнер, содержащий встроенное сообщение.
- *Стеганографический канал (стегоканал)* – канал скрытой передачи информации. Чтобы не вызывать подозрений, в результате описанных выше преобразований передаваемый стегоконтейнер для стороннего наблюдателя практически ничем не должен отличаться от исходного контейнера. Но этого мало. Чтобы стегосистема была надежной, при ее построении необходимо исходить из предположения, что наш пресловутый «цензор» имеет полное представление о применяемой стеганографической системе и деталях ее реализации. Единственной неизвестной ему величиной является стегоключ. Исходя из этого предположения, стегосистема должна быть сконструирована таким образом чтобы только обладатель стегоключа имел возможность выделить из стегоконтейнера встроенное сообщение, и, главное, чтобы только обладатель стегоключа имел возможность установить факт присутствия скрытого сообщения.

Компьютерная стеганография

В настоящее время в связи с развитием цифровой техники и средств телекоммуникаций возникло новое направление – *компьютерная стеганография*.

- ***Компьютерная стеганография*** – это часть стеганографии, которая занимается вопросами реализации стегосистем с использованием компьютерной техники.

Поскольку цифровая информация обычно передается в виде файлов, то в компьютерной стегосистеме используются понятия *файл-контейнер* и *файл-сообщение*. Для того, чтобы посторонние не заподозрили факт передачи сообщения, файл-сообщение особым образом (при помощи стегоключа) "смешивают" с файлом-контейнером. При этом, как и принято в "классической" стеганографии, файл-контейнер должен выглядеть вполне безобидно, а подмешивание секретной информации не должно изменять его основных свойств.

Тем не менее, компьютерная стеганография может использовать только ей присущие специфические методы, основанные, например, на использовании специальных свойств компьютерных форматов. Простейший пример использование компьютерной стегосистемы очень похож на использование симпатических чернил. Можно белыми буквами на стандартном белом фоне редактора Microsoft Word в тексте рекламы очередного стирального порошка написать несколько строчек секретного послания. Белые буквы на белом фоне не видны, а сделать их видимыми может даже начинающий пользователь. Конечно, надежность этой простейшей стегосистемы крайне низка.

Примеры

- Не очень сложные компьютерные стегосистемы уже реально применяются злоумышленниками (в частности, "виросописателями"). Известен, например, вирус, имеющий кодовое название "W32/Perrun". Этот вирус "прячет" свое тело объемом 18К в файле *.jpg. Точнее говоря, он просто добавляет свой код в конец *.jpg файла. С точки зрения стеганографии (впрочем, и с точки зрения вирусологии) это весьма примитивный вирус. Но он показывает метод, как внедрить в систему программу – закладку большого объема. Нужно сделать эту программу двухкомпонентной. Стартовая часть, которая только ищет основное тело программы в других файлах, может быть очень маленькой, что облегчает ее внедрение. Объем же основной части программы может быть очень большим, и при этом риск ее обнаружения может быть сведен к минимуму.
- Возможности современных методов компьютерной стеганографии можно хорошо прочувствовать, поэкспериментировав, например, со свободно распространяемыми стегопрограммами. Одна из самых распространенных утилит, умеющая прятать информацию в графических (форматы gif, bmp) и звуковых (формат wav) файлах является программа Э.Брауна S-Tools. Программа позволяет не только скрыть сообщение, но и зашифровать его с помощью стойкого криптоалгоритма, что обеспечивает как высокую скрытность факта передачи сообщения, так и стойкость секретного сообщения

С помощью данной программы в графический файл внедрен целый куплет одной песни вместе с припевом (формат MP3, объем 46,4 кб). Полученный стегоконтейнер можно рассмотреть на рисунке.

Визуально невозможно определить, что рисунок содержит в себе еще какую-то информацию. Более того, даже имея упомянутую программу S-Tools, невозможно обнаружить, что файл содержит вложенное сообщение. Необходимо еще ввести правильный пароль и установить правильный алгоритм шифрования. Только после этого можно обнаружить, что в графическом файле спрятан звуковой файл, извлечь его из стегоконтейнера и прослушать запрятанную песню.