Содержание:

Введение

В тот самый момент, когда первый компьютер впервые обработал несколько байт данных моментально встал вопрос: где и как хранить полученные результаты ? Как сохранять результаты вычислений, текстовые и графические образы, произвольные наборы данных ?

Вопрос этот корнями своими уходит в глубокую древность. Информация была всегда, независимо от того воспринималась она человеком или нет. И человек, едва выделившись из животного мира, стал активно использовать информацию в своих собственных целях. Более того, он сам стал источником информации для других. Уже тогда ее умели получать, обрабатывать, передавать, накапливать и что особенно важно – хранить.

Поначалу, для хранения и накопления информации, человек использовал свою память – он попросту запоминал полученную информацию и помнил ее какое то время. Тогдашние потоки информации не сравнить с нынешними, поэтому человеческой памяти пока хватало. Дело ограничивалось именами соплеменников, двумя заклинаниями злых духов, да десятком мифов и легенд.

Постепенно, люди пришли к выводу, что такой способ хранения информации имеет ряд недостатков:

– человек мог спутать различные данные;

– неправильно понять другого человека;

– элементарно забыть что-то важное;

– в конце концов его могли просто убить на охоте.

Понимая всю ненадежность такого способа хранения и накопления информации, человек придумал записывать информацию в виде рисунков на стенах пещер в которых жил. Это был огромный шаг вперед на пути хранения информации:

человек сопоставил фактам и событиям реальной жизни схематические рисунки и значки на стене пещеры – закодировал информацию. В таком виде информацию было гораздо легче хранить и накапливать, пещеры тогда были большие и места на стене было много.

С изобретением письменности дела пошли еще веселей: люди стали записывать полученную информацию на дощечках, табличках, папирусах, а позднее и в книгах, которые они к тому времени изобрели. Поток информации резко возрос, к тому же, люди открыли массу способов добывания или получения информации, и добывали ее вовсю.

Очень скоро накопилось огромное количество информации – сотни лет достижения человеческой мысли тщательно записывались, документировались и хранились в несчетных архивах и хранилищах.

К середине XX века поток информации достиг громадных размеров и продолжал стремительно расти в геометрической прогрессии. Человечество стало тонуть в захлестывающем его океане всевозможной информации. В этот критический момент и был изобретен компьютер – устройство для получения, накопления, хранения, обработки, передачи и распространения информации.

А как только он был изобретен, сразу встал вопрос, заданный в самом начале, как компьютер будет хранить эту информацию. Очевидно, что ни один из выше перечисленных способов не годился. Пришлось изобретать что-то новое.

Виды носителей информации

Прежде всего должно быть устройство с помощью которого компьютер будет запоминать информацию, затем требуется носитель информации, на котором ее можно будет переносить с места на место, причем другой компьютер должен также легко прочитать эту информацию. Рассмотрим некоторые из этих устройств:

1. Устройство чтения перфокарт: предназначено для хранения программ и наборов данных с помощью перфокарт – картонных карточек с пробитыми в определенной последовательности отверстиями. Перфокарты были изобретены задолго до появления компьютера, с их помощью на ткацких станках получали очень сложные и красивые ткани, потому что они управляли работой механизма. Изменишь набор перфокарт и рисунок ткани будет совсем другим – это зависит от расположения

отверстий на карте. Применительно к компьютерам был использован тот же принцип, только вместо рисунка ткани отверстия задавали команды компьютеру или наборы данных. Такой способ хранения информации не лишен недостатков: – очень низкая скорость доступа к информации;

– большой объем перфокарт для хранения небольшого количества информации;

– низкая надежность хранения информации;

– к тому же от перфоратора постоянно летели маленькие кружочки картона, которые попадали на руки, в карманы, застревали в волосах и уборщицы были страшно недовольны.

Перфокартами люди были вынуждены пользоваться не потому что этот способ как-то особенно нравился им, или он имел какие-то неоспоримые достоинства, вовсе нет, он вообще не имел достоинств, просто в то время ничего другого еще не было, выбирать было не из чего, приходилось выкручиваться.

2. Накопитель на магнитной ленте (стриммер): основан на использовании устройства магнитофонного типа, и кассет с магнитной пленкой. Этот способ накопления информации известен давно и успешно применяется и сегодня. Это объясняется тем, что на небольшой кассете помещается довольно большой объем информации, информация может храниться продолжительное время и скорость доступа к ней гораздо выше, чем у устройства чтения перфокарт.

С другой стороны стриммер пригоден только для накопления, хранения больших массивов информации, резервирования данных. Обрабатывать информацию с помощью стриммера практически невозможно – стриммер устройство последовательного доступа к данным: чтобы получить 5-й файл мы должны промотать четыре. А если нужен 7529-й ?

3. Накопитель на гибких магнитных дисках (НГМД – дисковод): сравнительное новое устройство хранения информации. Это устройство использует в качестве носителя информации гибкие магнитные диски – дискеты, которые могут быть 5-ти или 3-х дюймовыми. Дискета – это магнитный диск вроде пластинки, помещенный в картонный конверт. В зависимости от размера дискеты изменяется ее емкость в байтах. Если на стандартную дискету размером 5’25 дюйма помещается до 720 Кбайт информации, то на дискету 3’5 дюйма уже 1,44 Мбайта. Дискеты универсальны, подходят на любой компьютер того же класса оснащенный дисководом, могут служить для хранения, накопления, распространения и

обработки информации. Дисковод – устройство параллельного доступа, поэтому все файлы одинаково легко доступны. Сейчас дискеты применяются в основном для резервирования небольших объемов данных и для распространения информации. Дискеты размером 5’25 дюйма морально устарели и используются редко.

К недостаткам относятся маленькая емкость, что делает практически невозможным долгосрочное хранение больших объемов информации, и не очень высокая надежность самих дискет.

4. Накопитель на жестком магнитном диске (НЖМД – винчестер): является логическим продолжением развития технологии магнитного хранения информации. Появились несколько лет назад и уже завоевали огромную популярность благодаря своим многочисленным достоинствам:

– чрезвычайно большая емкость;

– простота и надежность использования;

– возможность обращаться к тысячам файлов одновременно;

– высокая скорость доступа к данным.

Из недостатков можно выделить лишь отсутствие съемных носителей информации, все данные записаны внутри винчестера на жестких магнитных дисках. (В настоящее время используются внешние винчестеры и системы резервного копирования с дисками по типу дискет). Емкости современных винчестеров поистине устрашающи: еще пять лет назад винчестер емкостью 100 Мбайт казался недостижимым идеалом, пределом заветных мечтаний – казалось, что и половины его пространства хватит на много лет работы. Но прошло пять лет, и такие винчестеры уже даже не выпускаются как морально устаревшие. Им на смену пришли новые, более быстрые, более вместительные аппараты. Винчестеры емкостью 850 Мб, 1.6, 2.1, 3.5, 4.3 Гигабайт давно ни кого не удивляют. А ведь существуют винчестеры в 1000 раз более емкие – речь идет о Терабайтах информации. Одного такого винчестера хватило бы чтобы записать всю историю Древнего Мира.

Пока они используются только в очень солидных организациях, но давайте подождем лет пять...

5. Устройство чтения компакт-дисков (CD-ROM): появились несколько лет назад и уже широко распространились. В этих устройствах используется принцип считывания сфокусированным лазерным лучом бороздок на металлизированном несущем слое компакт-диска. Этот принцип позволяет достичь высокой плотности записи информации, а следовательно и большой емкости при минимальных размерах. Компакт-диск является идеальным средством хранения информации – дешев до смешного, практически не подвержен каким-либо влияниям среды, информация записанная на нем не исказится и не сотрется, пока диск не будет уничтожен физически, имеет емкость 650 Мбайт, сравнимую с неплохим винчестером при этом его производство несравнимо дешевле и проще, при размерах с 5-ти дюймовую дискету вмещает информации в 900 раз больше, чем дискета.

Имеет только один недостаток – на компакт-диск нельзя записывать информацию. Данные на него записываются либо в процессе производства, либо потом, пользователем (устройство CD-R), но только единожды.

6. Другие устройства накопления и хранения информации: кроме вышеперечисленных основных устройств накопления и хранения информации существуют некоторые другие, по разным причинам менее популярные. К таким устройствам относятся:

– магнитооптические диски;

– бернулли-диски;

– устройства резервирования данных;

– некоторые другие устройства.

Все эти устройства имеют разные емкости, скорости доступа к информации, свои минусы и плюсы, а также разную цену. У них есть свои ограничения, но есть и несомненные достоинства. Одно у них всех есть общее – эти устройства были созданы для хранения, накопления и резервирования данных.

Понятие каналов утечки информации

Современные информационные технологии разделили судьбу всех прогрессивных технологий XX в. Бесспорно, что широкое внедрение средств компьютерной

техники (СКТ) и телекоммуникаций в производственную, хозяйственную, финансовую деятельность предприятий, учреждений, организаций значительно повышает эффективность их работы. Рубеж тысячелетий знаменуется все большим проникновением СКТ в повседневную жизнь людей, вовлечением их в глобальную сеть Internet . Так, например, по оценкам зарубежных специалистов, темп роста пользователей Internet составляет порядка 15 % в месяц. Обратной стороной глобальной информатизации явилось появление компьютерной преступности.

На локальном уровне угроз компьютерной безопасности (например, для помещений, занимаемых учреждением, организацией, предприятием, и размещенных в них СКТ) выделяют каналы утечки информации, под которыми понимают совокупность источников информации, материальных носителей или среды распространения несущих эту информацию сигналов и средств выделения информации из сигналов или носителей.

Факторы информационных угроз следует рассматривать как потенциальную возможность использования каналов утечки информации. Объективное существование данных каналов утечки предполагает их возможное использование злоумышленниками для несанкционированного доступа к информации, ее модификации, блокированию и иных неправомерных манипуляций, т. е. наличие каналов утечки информации влияет на избрание способа совершения преступления.

В рамках данного учебного пособия каналы утечки информации целесообразно условно классифицировать на традиционные каналы утечки информации (каналы утечки информации в широком смысле) и каналы утечки информации непосредственно из СКТ (каналы утечки в узком смысле). Наличие первых предопределяет широкое использование их с применением специальных технических средств для проведения различных разведывательных мероприятий. Они известны задолго до появления современных средств вычислительной техники (см. рис.1).

Локальные факторы угроз информационной безопасности

Каналы утечки информации и технические устройства несанкционированного доступа

Каналы утечки информации в широком смысле

Каналы утечки информации в узком смысле

Рис.1

Каналы утечки информации непосредственного из СКТ и технические устройства съема такой информации стали использоваться злоумышленниками сравнительно недавно.

Для получения информации из обозначенных выше традиционных каналов утечки применяются специализированные технические средства ведения разведки (ТСВР), среди которых выделяют следующие основные группы:

- радиомикрофоны и микрофоны;
- оптические системы;

■устройства перехвата телефонных сообщений;

- видеосистемы записи и наблюдения;
- системы определения местоположения контролируемого объекта;
- системы контроля и воздействия на компьютеры и их сети.
- устройства приема, записи, управления.

Традиционные каналы утечки информации

Традиционные каналы утечки информации приведены на рисунке 2.

Традиционные каналы утечки аудио- и видеоинформации	Контактное или бесконтактное подключение к электронным устройствам. Встроенные микрофоны, видео- и радиозакладки в стенах, мебели предметах.
	Съем акустической информации при помощи лазерных устройств с отражающих поверхностей.
	Оптический дистанционный съем видеоинформации.

Применение узконаправленных микрофонов и диктофонов.

Утечки информации по цепям заземления, сетям громкоговорящей связи, охранно-пожарной сигнализации, линиям коммуникаций и сетям электропитания.

Высокочастотные каналы утечки информации бытовой и иной технике.

Утечка за счет плохой звукоизоляции стен и перекрытий.

Исследование злоумышленником производственных и технологических отходов.

Утечка информации через телефонные и факсимильные аппараты.

Оборудование виброканалов утечки информации на сетях отопления газо -и водоснабжения.

Утечка информации через персонал.

Утечка акустических сигналов (речевая информация)

Утечка электромагнитных сигналов (в т.ч. оптического диапазона)

Утечка информации с носителей (либо с носителями)

Рис.2

Контактное подключение к электронным устройствам является простейшим способом съема информации. Чаще всего реализуется непосредственным подключением к линии связи.

Бесконтактное подключение может осуществляться за счет электромагнитных наводок или с помощью сосредоточенной индуктивности.

Встроенные микрофоны, видео- и радиозакладки в стенах, мебели, предметах. Могут быть установлены в элементы интерьера, строительные конструкции, СКТ, теле- и радиоприемники, розетки, телефонные аппараты, калькуляторы, замаскированы под канцелярские принадлежности, элементы одежды и т. д. Обладают дальностью действия от 50 до 1000 м при сравнительно небольшой стоимости. Ниже приведены примеры таких устройств.

Съем акустической информации при помощи лазерных устройств с отражающих поверхностей. Принцип действия основан на моделировании по амплитуде и фазе отраженного лазерного луча от окон, зеркал и т. д. Отраженный сигнал

принимается специальным приемником. Дальность действия — до нескольких сотен метров. На эффективность применения подобных устройств сильное влияние оказывают условия внешней среды (погодные условия).

Оптический дистанционный съем видеоинформации. Может осуществляться через окна помещений с использованием длиннофокусного оптического оборудования в автоматическом или в ручном режиме работы.

Применение узконаправленных микрофонов и диктофонов. Применяются высокочувствительные микрофоны с очень узкой диаграммой направленности. Узкая диаграмма направленности позволяет указанным устройствам избежать влияния посторонних шумов. Узконаправленные микрофоны могут быть использованы совместно с магнитофонами и диктофонами.

Утечки информации по цепям заземления, сетям громкоговорящей связи, охранно-пожарной сигнализации, линиям коммуникаций и сетям электропитания. Утечка информации по цепям заземления возможна за счет существования гальванической связи проводников электрического тока с землей.

При организации каналов утечки информации через сигнализации различного назначения злоумышленники используют «микрофонный эффект» датчиков. Подобные каналы утечки получили название параметрических каналов. Они формируются путем «высокочастотной накачки» (ВЧ - облучения, ВЧ -навязывания) электронных устройств с последующим переизлучением электромагнитного поля, промодулированного информационным сигналом. Промодулированные ВЧ-колебания могут быть перехвачены и демодулированы соответствующими техническими средствами.

Аналогичным образом могут быть созданы высокочастотные каналы утечки информации в бытовой и иной технике.

Утечка за счет плохой звукоизоляции стен и перекрытий. Съем информации может происходить с применением как простейших приспособлений (фонендоскоп), так и достаточно сложных технических устройств, например специализированных микрофонов.

Оборудование виброканалов утечки информации на сетях отопления, газо- и водоснабжения. Средой распространения акустических волн являются трубы газо- и водоснабжения, конструкции зданий. Акустическая информация может, например, восприниматься при помощи пьезоэлектрических датчиков, затем

усиливаться и фиксироваться при помощи магнитофонов либо передаваться в эфир.

Утечки информации через персонал. Многие исследователи, в том числе зарубежные, отмечают, что люди представляют наибольшую угрозу для информационной, и в частности компьютерной, безопасности. Наибольшую же угрозу представляют собственные сотрудники, которые могут уничтожать или искажать информацию, писать компьютерные вирусы, похищать информацию в целях шпионажа.

По Г. Н. Мухину обстоятельствами, влекущими совершение подобных действий, могут быть:

- вербовка сотрудника криминальными структурами;
- внедрение этими же структурами или конкурирующими субъектами хозяйствования своего агента в штат предприятия или банка с целью выполнения разведывательных и иных функций;
- имеющиеся у сотрудника проблемы социально-психологического либо морально-этического порядка, обусловленные неудовлетворенностью им заработной платой или занимаемой должностью, пренебрежительным отношением к нему либо оскорбительным поведением со стороны руководства и др.

Проведенный анализ позволяет сделать вывод, что в основном работа злоумышленников по съему информации с каналов утечки сводится к получению речевой информации.

Под речевой информацией понимают некоторый объем сведений, обработанный человеческим сознанием и выданный в виде речевых сигналов акустическим речевым аппаратом человека. Речевая информация может быть записана на носитель, позволяющий считывать ее зрительным аппаратом человека или воспроизводить акустически.

В настоящее время в связи с бурным развитием электронной техники речевая информация, передаваемая по каналам связи, становится все более уязвимой. Простейшие технические средства связи позволяют прослушивать телефонные переговоры, передаваемые по линиям связи, находясь на больших расстояниях от линии и объекта.

Любые средства передачи речевой информации могут быть одновременно и каналами ее утечки. По мнению Г. В. Давыдова и Ю. В. Шамгина, наиболее вероятными средствами передачи речевой информации являются следующие акустические каналы:

человек - человек (слушатели);

человек - микрофон - усилитель - громкоговоритель - человек (слушатели);

человек - микрофон — магнитофон (запись речи на автоответчик);

магнитофон (считывание речи) — усилитель — громкоговоритель - человек (слушатели);

человек — тракт электросвязи (радиосвязи) - человек (слушатели);

автоответчик (считывание речи) - речевой сигнал - автоответчик (запись речи);

человек - устройство, управляющее голосом;

синтезатор искусственной речи - человек.

Наиболее распространенными средствами приема и регистрации сигналов речевой информации, распространяемой по акустическому каналу, являются:

микрофон и устройства, выполняющие его функцию;

пассивные отражатели светового луча, играющие роль мембраны для акустических волн (оконные стекла, иные тонкостенные отражатели);

волноводные тракты акустических волн различного типа (вентиляционные каналы, стеновые панели);

лазерный луч, реагирующий на локальные изменения плотности воздуха в поле распространения акустической волны.

Наиболее очевидными каналами утечки речевой информации являются следующие:

1.На открытом пространстве (или в незащищенном помещении):

прямое подслушивание (скрытое или случайное);

узконаправленный микрофон

«жучки» в одежде, автомобиле, местных предметах и т. д.;

артикулярное считывание по мимике говорящих;

случайная или преднамеренная беседа, инициированная слушателем.

2. В помещении:

прослушивание через ограждающие конструкции из-за недостаточной звукоизоляции последних;

считывание со стекол окон;

прослушивание сигналов речи за счет передачи их по трубопроводам и вентиляционным системам;

прослушивание сигналов речи за счет акустоэлектрического преобразования в системах телефонии, радиовещания и сигнализации;

визуальное считывание с носителей информации и дисплеев компьютеров.

Каналы утечки информации из СКТ

Эти каналы схематично представлены на рис. 3

Каналы утечки информации из СКТ	Утечка информации за счет введения программно-аппаратных закладок в СКТ
	Утечки за счет побочного электромагнитного излучения и наводок (ПЭМИН)
	Утечки за счет съема информации с принтера и клавиатуры по акустическому каналу
	Утечка, модификации, уничтожение или блокирование информации с использованием компьютерных вирусов
	Утеря носителей информации

Инициализация злоумышленником каналов утечки, вызванных несовершенством программного либо аппаратного обеспечения, а также систем защиты

Рис. 3

Утечка информации за счет введения программно-аппаратных закладок в СКТ. Весьма правильной представляется точка зрения авторов, отмечающих, что в настоящее время в основе производства технических средств и программного обеспечения вычислительных систем лежат комплектующие изделия зарубежного производства, что обеспечивает конкурентоспособность выпускаемых изделий. Однако при этом появляется угроза утечки информации, а также управляемого выведения из строя средств вычислительной техники, заложенная в них либо на этапе производства, либо на этапе сборки. Подобные устройства могут быть установлены негласным образом и впоследствии при эксплуатации СКТ. Использование закладных элементов (ЗЭ) представляется реальной и опасной угрозой при использовании вычислительной техники.

Аппаратные ЗЭ могут быть реализованы в аппаратуре персональных компьютеров и периферийных устройств. При этом возможны утечки информации, искажение вычислительного процесса, а также управляемый выход из строя вычислительной системы.

Программные ЗЭ могут быть представлены в виде модификации компьютерной программы, в результате которой данная программа способна выполняться несколькими способами в зависимости от определенных обстоятельств. При работе программные ЗЭ могут никак не проявляться, однако при определенных условиях программа работает по алгоритму, отличному от заданного (подобно компьютерным вирусам). В литературе описан пример внесения программистом в программу начисления заработной платы предприятия нежелательных изменений,

работа которых началась после его увольнения, т. е. когда фамилия программиста исчезла из базы данных персонала.

Существует классификация ЗЭ по следующим критериям:

способ у размещения ЗЭ;

способу активизации ЗЭ;

пути внедрения ЗЭ в систему;

разрушающему действию ЗЭ.

Утечки за счет перехвата побочного электромагнитного излучении и наводок (ПЭМИН). При функционировании СКТ возникают побочные электромагнитные излучения и наводки, несущие обрабатываемую информацию. ПЭМИН излучаются в пространство клавиатурой, принтером, монитором, накопителями на магнитных дисках, кабелями. Утечка данных обусловлена лишь излучением сигналов при перемене данных. Все прочие излучения сигналов от разных блоков СКТ являются взаимными помехами.

Перехват ПЭМИН осуществляется радиоприемными устройствами, средствами анализа и регистрации информации. При благоприятных условиях с помощью направленной антенны можно осуществлять перехват на расстоянии до 1-1,5 км. В. И. Ярочкин отмечает, что перехват информации за счет ПЭМИН обладает рядом особенностей:

информация добывается без непосредственного контакта с источником;

на прием сигналов не влияет ни время года, ни время суток;

информация получается в реальном масштабе времени, в момент ее передачи или излучения;

реализуется скрытно;

дальность перехвата ограничивается только особенностями распространения радиоволн соответствующих диапазонов.

Утечки за счет съема информации с принтера и клавиатуры по акустическому каналу. Наличие указанного канала утечки позволяет перехватывать и декодировать акустические колебания, средой распространения которых является

воздушная среда. Источником данных колебаний являются соответствующие устройства СКТ. Технически возможен перехват и декодирование кодов клавиш клавиатуры. Дальность действия подобных перехватов ограничена мощностью источника акустических и электромагнитных колебаний.

Утечка, модификация, уничтожение или блокирование информации с использованием компьютерных вирусов. Существует множество типов! вирусов, каждый из которых обладает собственными отличительными при-1 знаками. Анализ специальной научной литературы дает нам основание утверждать, что все вирусы изменяют либо файлы с данными, либо програм-1 мы внутри компьютера, либо разрушают сами компьютеры[1]. Большинство! из них представляют собой опасность только для IBM-совместимых компьютеров, однако именно этот тип компьютеров распространен в наибольшей! степени.

Последствия вирусной модификации могут быть различными - от нее значительных помех до полного уничтожения данных и программ. Вирусы, использующиеся правонарушителями для программного уничтожения, разрушают информацию в зависимости от определенных логических или временных условий.

Попадание вирусов в компьютерную систему может быть спровоцировано различными способами от высокотехнологичного несанкционированного подключения до основанного на личном доверии обмана оператора

системы путем переписывания заранее зараженных игр и сервисных программ с умыслом на вывод компьютерной системы из строя. Вирус может попасть в систему и при неумышленных действиях операторов ЭВМ — при обмене дискетами, CD-ROM-дисками, файлами.

В настоящее время «рассадником» компьютерных вирусов стала глобальная сеть Internet. Особенно активно распространяются в этой сети так называемые макровирусы, которые передаются вместе с файлами документов MS-Word и файлами рабочих книг MS-Excel. Целесообразно привести краткий анализ традиционных воздействий компьютерных вирусов на СКТ, которые известны из специальной научной литературы. На рис. 5 приведена примерная видовая классификация компьютерных вирусов.

«Троянский конь» — специальная программа, которая разрешает действия, отличные от определенных в спецификации программы.

«Червь» - программа, которая создается для распространения своих копий в другие компьютерные системы по компьютерным сетям путем поиска уязвимых мест в операционных системах.

«Логическая бомба» - программа, выполняемая периодически или в определенный момент с целью исказить, уничтожить или модифицировать данные. Наступление р ую к

Р

ис.5

Файл-инфекторы изменяют содержимое управляющих программ путем добавления нового кода в существующие файлы. Такой тип вируса поражает файлы, которые обозначены как COM, EXE, SYS, DLL. Файл-инфекторы распространяются через любой носитель данных, используемый для хранения и передачи управляемого кода. Вирус может храниться на хранения информации либо передаваться по сетям и через модемы.

Вирусы сектора начальной загрузки заражают основную загрузочную область на жестких дисках или загрузочный сектор на дискетах. Оригинальная версия обычно, но не всегда, хранится где-нибудь на диске. В результате вирус запустится перед загрузкой компьютера. Вирусы такого типа обычно остаются в секторе памяти до тех пор, пока пользователь не выйдет из системы.

Вирусы, результаты воздействия которых на компьютерные системы) их сети могут проявляться как применение нескольких отдельных вирусов, называются комбинированными (составными) вирусами. Вирус, который проникает как в сектор

начальной загрузки, так и в файлы, имеет больше возможностей для размножения. В результате способности вируса проникать как в сектор начальной загрузки, так и в файлы, компьютерная система заражается вирусом независимо от того, была ли она загружена с зараженного диска или в результате запуска зараженной программы.

Парные вирусы поражают операционную систему таким образом, что нарушается последовательность выполнения файлов COM и EXE с одним именем. Этот тип вируса создает копию файла COM, но в размере файла EXE. Имя файла остается прежним. При запуске пользователем программы операционная система выполнит вновь созданный файл COM, в котором содержится код вируса, после чего загружает и выполняет файл EXE.

Цепными называются вирусы, модифицирующие таблицы расположения файлов и директорий таким образом, что вирус загружается и запускается до того, как запускается желаемая программа. Они связывают элементы таблицы расположения директорий с отдельным кластером, содержащим код вируса. Оригинальный номер первого кластера сохраняется в неиспользуемой части элемента таблицы директорий. Сама по себе программа физически не изменяется, изменяется только элемент таблицы расположения директорий. Подобные вирусы также известны как вирусы системных файлов, секторные вирусы или вирусы таблиц расположения файлов.

Полиморфные вирусы производят копии самих себя. Эти копии различны для каждого из незараженных файлов. Код вируса меняется после каждого нового заражения, но принцип его действия всякий раз остается неизменным. Известны, например, две так называемые утилиты мутации вируса: Mutation Engine и Polymorphic Trident Engine. При использовании этих утилит любой вирус становится полиморфным, так как утилиты добавляют в его код определенные команды в произвольной последовательности.

По деструктивным возможностям компьютерные вирусы можно разделить на следующие 4 группы (рис. 6):

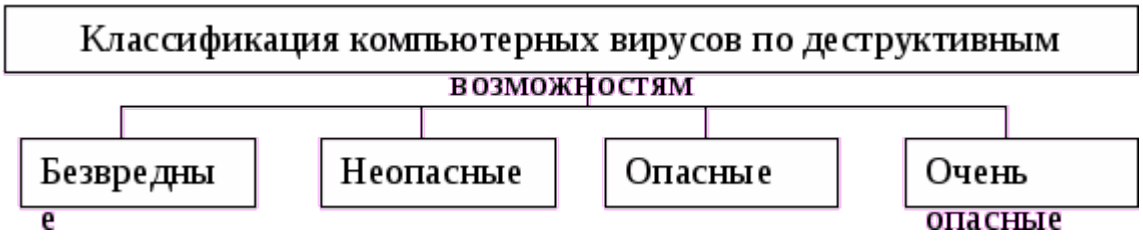

Рис. 6

1. Безвредные - никак не влияющие на работу компьютерной системы, кроме уменьшения количества свободной памяти, указанной в результате своего распространения.
2. Неопасные - влияние которых ограничивается уменьшением свобод ной памяти, а также графическими, звуковыми и прочими эффектами.
3. Опасные - которые могут привести к серьезным сбоям в работе компьютерных систем.
4. Очень опасные — в алгоритм их работы введены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, способствовать быстрому износу движущихся частей механизмов (например, вводить в резонанс и разрушать головки некоторых типов жестких дисков) и т. д.

Необходимо отметить, что существуют и другие классификации компьютерных вирусов, например по способу их воздействия на СКТ и обслуживающий их персонал.

1.Компьютерные вирусы, не повреждающие файловую структуру:

размножающиеся в оперативных запоминающих устройствах (ОЗУ);

раздражающие оператора (имитирующие неисправность аппаратуры; формирующие сообщения на терминале; формирующие звуковые эффекты; переключающие режимы настройки и др.);

сетевые.

2. Компьютерные вирусы, повреждающие файловую структуру:

повреждающие программы и данные пользователя;

повреждающие системную информацию (области диска, форматирующие носители, файлы операционной системы).

3. Компьютерные вирусы, воздействующие на аппаратуру и оператора:

повреждающие аппаратуру (микросхемы, диски, принтеры; выжигающие люминофор);

воздействующие на оператора (в том числе на зрение, психику и др.).

Утеря носителей информации. Может произойти в результате:

хищения с полным или частичным разрушением места хранения;

физического уничтожения из-за умышленных несанкционированны действий персонала;

пожара либо воздействия на носитель высокой температуры, ионизирующего излучения, химических веществ, сильного электромагнитного поля;

стихийных бедствий (землетрясение, наводнение, ураган и др.);

иных форс-мажорных обстоятельств.

Инициализация злоумышленником каналов утечки, вызванных несовершенством программного либо аппаратного обеспечения, а такою систем защиты, как правило, производится на этапе подготовки к совершению информационного компьютерного преступления, реже - непосредственно при его совершении. Речь идет о так называемых атаках на информационные системы. Под атакой подразумевается любая попытка преодоления систем защиты

Заключение

Главной целью злоумышленника является получение информации о составе, состоянии и деятельности объекта конфиденциальных интересов (фирмы, изделия, проекта, рецепта, технологии и т.д.) в целях удовлетворения своих информационных потребностей. Возможно в корыстных целях и внесение определенных изменений в состав информации, циркулирующей на объекте конфиденциальных интересов. Такое действие может привести к дезинформации по определенным сферам деятельности, учетным данным, результатам решения некоторых задач. Более опасной целью является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов. Полный объем сведений о деятельности конкурента не может быть получен только каким-нибудь одним из возможных способов доступа к информации. Чем большими информационными возможностями обладает злоумышленник, тем больших успехов он может добиться в конкурентной борьбе.

На успех может рассчитывать тот, кто быстрее и полнее соберет необходимую информацию, переработает ее и примет правильное решение. От целей зависит как выбор способов действий, так и количественный и качественный состав привлекаемых сил и средств посягательства.

Точно также, способы защиты информационных ресурсов должны представлять собой целостный комплекс защитных мероприятий, планирование которых рассмотрено в четвертом и пятом разделах. Разумеется, это не полный перечень, поскольку каждый руководитель решает какие методы и средства защиты необходимо использовать применительно к данному объекту, что зависит от функций, выполняемых объектом, а также от его экономических соображений.

Таким образом, главной целью данной курсовой работы была разработка комплексной системы защиты информации