Система защиты информации

Защитить информацию – это значит:

1. Обеспечить физическую целостность информации, т.е. не допустить искажений или уничтожения элементов информации;

2. Не допустить подмены (модификации) элементов информации при сохранении ее целостности;

3. Не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;

4. Быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использованы только в соответствии с обговоренными сторонами условиями.

Процессы по нарушению надежности можно классифицировать на:

1. Случайные (непреднамеренные).
2. Злоумышленные (преднамеренные).

Объект защиты – структурный компонент системы, в котором находится или может находится подлежащая защите информация

Объекты защиты:

1. ПК, серверы, рабочие станции в сети.
2. Узел связи.
3. Средства отображения информации.
4. Средства документирования информации.
5. Компьютерный или дисплейный зал и хранилище информации.
6. Внешние каналы связи и сетевое оборудование.
7. Накопители и носители информации.

Элемент защиты – это блоки (документы, массивы, потоки и др.) информации в объектах защиты.

Элементы защиты:

1. Данные и программы в основной памяти компьютера, на внешних носителях.
2. Данные, отображаемые на мониторе, выводимые на принтер.
3. Данные, размножаемые на копировально-множительном оборудовании.
4. Отходы обработки информации в виде бумажных и магнитных носителей.
5. Журналы назначения паролей зарегистрированным пользователям.
6. Служебные инструкции по работе с комплексными задачами.
7. Архивы данных и программного обеспечения.

Система защиты информации – комплекс мер и мероприятий:

1. Организационно-административного характера;
2. Технического характера;
3. Программно-аппаратного характера;
4. Технологического характера;
5. Правового характера;
6. Морально-этического характера.

Организационно-административные меры

Сводятся к регламентации доступа к информационными и вычислительным ресурсам, функциональным процессам систем обработки данных, регламентации деятельности персонала.

Типичные организационно-административные средства:

1. Создание контрольно-пропускного режима на территории, где располагаются средства обработки информации.
2. Тщательный подбор персонала работающего с информацией.
3. Хранение информации в сейфах.
4. Защита от установки прослушивающей аппаратуры;
5. Разграничение доступа в соответствии с функциональным обязанностями работников.

Технические средства защиты

Сводятся к созданию некоторой физически замкнутой среды вокруг объектов и элементов защиты.

Мероприятия технической защиты

1. Установка средств физической преграды защитного контура помещений (кодовые замки, охранная сигнализация, видеонаблюдение).
2. Ограничение электромагнитного излучения путем экранирования помещений.
3. Использование автономных средств защиты аппаратуры в виде кожухов, крышек, дверец с установкой контроля вскрытия аппаратуры.

Программные средства и методы защиты

Сводятся защите информации в ПК и компьютерных сетях.

Программные средства и методы защиты

1. разграничение и пароль доступа к ресурсам;
2. регистрация и анализ протекающих процессов, событий, пользователей;
3. предотвращение возможных разрушительных воздействий на ресурсы (скрытие папок и файлов, антивирусная проверка);
4. криптографическая защита (преобразование информации с помощью алгоритмов, кодов, ключей …);
5. идентификация и аутентификация пользователей и процессов.

Технологические средства защиты информации

Сводятся к комплексу мероприятий, органично встраиваемых в технологические процессы преобразования данных.

Технологические средства защиты информации

1. Создание архивных копий носителей.
2. Ручное или автоматическое сохранение обрабатываемых документов во внешней памяти компьютера.
3. Регистрация пользователей компьютерных средств в журналах.
4. Автоматическая регистрация доступа пользователей к тем или иным ресурсам.

Правовые и морально-этические меры и средства защиты

Сводятся к использованию действующих в стране:

1.Нормативно-правовых актов, регламентирующих правила обращения с информацией и ответственность за их нарушение.

2.Норм поведения, соблюдение которых способствует защите информации.

Компьютерные вирусы

Компьютерные вирусы – это программы, которые могут «размножаться» создавать свои копии) и скрытно внедрять свои копии в файлы, загрузочные сектора дисков и документы. При этом копии могут сохранять способность дальнейшего распространения. Вирус может дописывать себя везде, где он имеет шанс выполниться.

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») заражал дискеты персональных компьютеров.

В настоящее время известно более 50 тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

Активизация вируса может быть связана с различными событиями:

- Наступлением определённой даты или дня недели
- Запуском программы
- Открытием документа и т.д.

Классификация компьютерных вирусов

Компьютерные вирусы

По среде обитания: файловые, загрузочные, сетевые, макровирусы

По способу заражения: резидентные, нерезидентные

По особенностям алгоритма: простейшие, репликаторы, невидимки, мутанты, квазивирусы

Рассмотрим подробнее одну из классификаций По среде обитания

Файловые вирусы.

- *Файловые вирусы внедряются в исполняемые файлы (программы) и активизируются при их запуске.*

После запуска зараженной программы вирус находится в оперативной памяти компьютера и может заражать другие файлы вплоть до момента выключения компьютера или перезагрузки операционной системы.

При этом могут быть заражены даже файлы данных (например, звуковые или графические). Поэтому не рекомендуется запускать на выполнение файлы, полученные из сомнительного источника и не проверенные предварительно антивирусными программами.

Загрузочные

- *Загрузочные вирусы записывают себя в загрузочный сектор диска.*

При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведет себя как файловый. Чтобы обезопасить себя от подобных вирусов, не загружайте операционную систему с гибких дисков и установите на BIOS вашего компьютера защиту от изменений загрузочного сектора.

Макровирусы

- *Макровирусы заражают файлы документов Word, электронных таблиц Excel.*

Макровирусы фактически являются **макрокомандами (макросами**), которые встраиваются в документ. **После загрузки зараженного документа в соответствующее приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы**. Угроза заражения прекращается только после закрытия приложения. Профилактика заражения такими вирусами состоит в отказе от загрузки макросов, однако таким образом вы отключите и полезные макросы, содержащиеся в документе.

Сетевые вирусы.

- *Сетевые вирусы – вирусы, распространяющиеся и заражающие компьютеры по компьютерной сети.*

Заражение может произойти и, например, **при получении зараженных файлов с серверов файловых архивов.** Существуют и специфические вирусы, которые распространяются через электронную почту и WWW. К ним относятся, например, так называемые **Интернет – черви (Worm). Эти вирусы распространяются во вложенных в почтовое сообщение файлах.** Такие вирусы, как правило, активизируются по определенным датам и уничтожают файлы на дисках зараженного компьютера.

Профилактика заражения компьютерным вирусом

Основные признаки появления в системе вируса

- Замедления работы некоторых программ;
- Увеличение размеров файлов (особенно выполняемых);
- Появление не существовавших ранее «странных» файлов, особенно в каталоге Windows или корневом;
- Уменьшение объема доступной оперативной памяти;
- Внезапно возникающие разнообразные видео и звуковые эффекты;
- Заметное снижение скорости работы в Интернете (вирус или троянец могут передавать информацию по сети);
- Жалобы от друзей (или провайдера) о том, что к ним приходят непонятные письма (вирусы любят рассылать себя по почте);
- Исчезновение файлов и каталогов или искажение их содержимого;
- Невозможность загрузки операционной системы;
- Изменение размеров, даты и времени модификации файлов;
- Частые зависания и сбои в работе компьютера.

Общие рекомендации по профилактике заражения вирусом

- Проверяйте на наличие вирусов все поступающие извне данные, в том числе через гибкие и компакт – диски, а также по любым сетям.
- Периодически проверяйте все жесткие диски вашего компьютера на наличие вирусов.
- Старайтесь использовать лицензионные программные продукты.
- Не пускайте за свой компьютер друзей с неизвестно откуда взявшимися «игрушками».
- Всегда защищайте свои гибкие диски от записи при работе на других компьютерах, если на них не будет производиться запись информации.
- Не оставляйте в кармане дисковода для гибких магнитных дисков дискету при включении или перезагрузке компьютера, чтобы исключить заражение компьютера загрузочными вирусами.
- Регулярно обновляйте вирусную базу своих антивирусных программ

ПОМНИТЕ!

При борьбе с вирусами не стоит стирать все файлы вашего компьютера подряд. При этом можно удалить важные системные файлы, что приведет к невозможности работы на компьютере.

На этом построено действие «психологических» вирусов, рассчитанных именно на то, что пользователь своими руками разрушит систему.

Антивирусные программы

- Детекторы – обнаруживают вирусы по совпадению с известной комбинацией байтов
- Доктора (фаги и полифаги) – аналогичны детекторам, но дополнительно производят лечение
- Ревизоры – обнаруживают вирусы по сравнению состояния загрузочного сектора и FATтаблицы
- Ревизоры-доктора – аналогичны ревизорам, но дополнительно производят лечение
- Фильтры – располагаются резидентно в ОП и перехватывают обращение к ОС, которые используются вирусом
- Вакцины (иммунизаторы) – модифицируют программы так, что вирус считает их уже зараженными

Для защиты компьютеров от вирусов создаются специальные *антивирусные программы.* Они способны либо обнаружить вирус, либо обнаружить и обезвредить его.

К наиболее популярным антивирусным программам относятся российские программы **DrWeb, ADinf, AVP** и зарубежные **Norton Antivirus, Dr/Solomon.**