Методы защиты информации

Селиверстов А.М. мастер п/о

Утечка информации

Цифровая информация – это информация, хранение, передача и обработка которой осуществляются средствами ИКТ.

Защищаемая информация – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Угроза утечки:

- Преднамеренная кража, копирование, прослушивание и пр.;
- Проникновение в память компьютера, в базы данных и информационных систем;
- Перехват в каналах передачи данных, искажение, подлог данных

Меры защиты информации

Существует множество способов защиты информации:

- Физическая защита каналов;
- Криптографические шифры;
- Цифровая подпись и сертификаты;
- Антивирусные программы;
- Брандмауэры;
- Межсетевые экраны;
- Резервное копирование;
- Контроль и профилактика оборудования;
- Разграничение доступа;
- Использование блоков бесперебойного питания.

Компьютерный вирус

Компьютерный вирус **—** это фрагмент исполняемого кода, который копирует себя в другую программу, модифицируя ее при этом.

Существует несколько разновидностей компьютерных вирусов:

- Файловые - внедряются в исполняемые файлы (программы) и активизируются пи их запуске. Находятся в ОЗУ до завершения работы компьютера.
- Загрузочные - записывают себя в загрузочный сектор диска (в программу – загрузчик ОС). При загрузке ОС с зараженного диска внедряется в ОЗУ и ведет себя как файловый вирус.
- Макровирусы - являются макрокомандами, которые заражают файлы документов Word, Excel. Находятся в ОЗУ до закрытия приложения.
- Драйверные - заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.
- Сетевые - заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение. Похищают пароли пользователей. Рассылают себя по электронным адресам.

Резервное копирование

Резервное копирование данных – процесс создания копии данных, необходимый для быстрого и недорогого восстановления информации в случае утери рабочей копии.

Восстановление данных – процесс восстановления данных в оригинальном месте.

Преимущества: надежность хранения информации, простота в эксплуатации – автоматизация, быстрое внедрение.

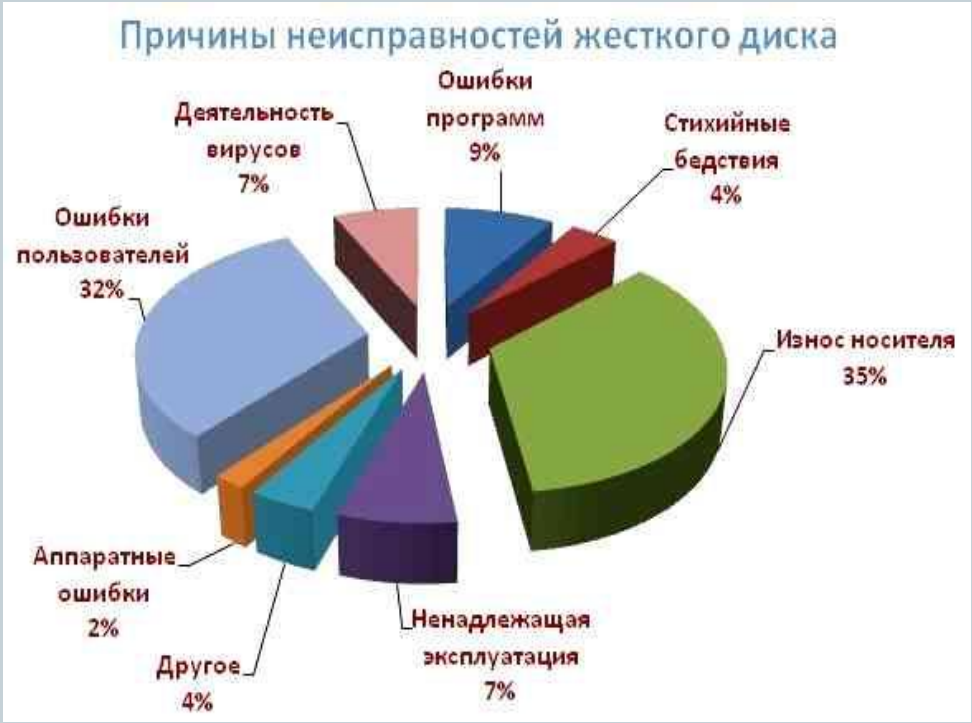
Виды резервного копирования

- ***Полное резервное*** - создание полной копии всех данных;
- ***Дифференциальное –*** Каждый файл, который был изменен после полного резервного копирования, копируется каждый раз заново;
- ***Инкрементное (добавочное) –*** Добавляет только те файлы, которые были изменены
- с момента предыдущего резервного копирования;
- ***Клонирование -*** Позволяет скопировать данные в другой раздел или на другой носитель.

Причины неисправности жесткого магнитного диска

Существует множество причин неисправности жесткого диска:

- Ошибки программ;
- Стихийные бедствия;
- Износ носителя;
- Ненадлежащая эксплуатация;
- Аппаратные ошибки;
- Ошибки пользователей;
- Деятельность вирусов;
- Другое.



Устройства хранения данных

Запоминающее устройство — носитель информации, предназначенный для записи и хранения данных. В основе работы запоминающего устройства может лежать любой физический эффект, обеспечивающий приведение системы к двум или более устойчивым состояниям.

Устройства хранения данных (внешние устройства)

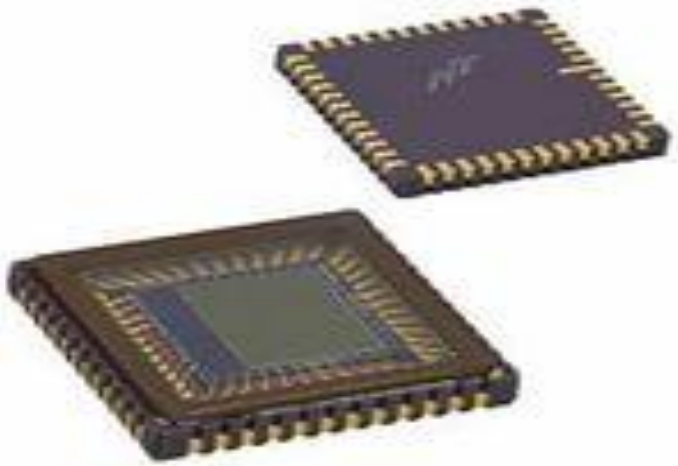
Устройства хранения информации делятся на 2 вида:

- внешние (периферийные) устройства
- внутренние устройства

К **внешним устройствам** относятся магнитные диски, CD, DVD, BD, стримеры, жесткий диск (винчестер) , а также флэш-карта. Главный их недостаток в том, что они работают медленнее устройств внутренней памяти.

Устройства хранения данных (внутренние устройства)

К **внутренним устройствам** относятся оперативная память, кэш-память, CMOS-память, BIOS. Главным достоинством является скорость обработки информации. Но в то же время устройства внутренней памяти довольно дорогостоящи.



Заключение

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

Вирусы успешно внедрились в повседневную компьютерную жизнь, и покидать ее в обозримом будущем не собираются.