Защита съемных носителей

Съемные носители информации

- **Носитель информации**– физическая среда, непосредственно хранящая информацию.
- **Носитель информации**— строго определённая часть конкретной информационной системы, служащая для промежуточного хранения или передачи информации.
- **Носитель информации** — внешние запоминающие устройства (внешняя память). Эти носители информации можно классифицировать по различным признакам, например, по типу исполнения, материалу, из которого изготовлен носитель и т.п.

Классификация носителей информации

Ленточные носители информации

Дисковые носители информации

Устройства на основе flash-памяти

Ленточные носители информации

- **Магнитная лента** — носитель магнитной записи, представляющий собой тонкую гибкую ленту, состоящую из основы и магнитного рабочего слоя. Рабочие свойства магнитной ленты характеризуются её чувствительностью при записи и искажениями сигнала в процессе записи и воспроизведения.
- Наиболее широко применяется многослойная магнитная лента с рабочим слоем из игольчатых частиц магнитно-твёрдых порошков гамма-окиси железа (γ-Fe2O3), двуокиси хрома (CrO2) и гамма-окиси железа, модифицированной кобальтом, ориентированных обычно в направлении намагничивания при записи.

Дисковые носители информации

Накопители на гибких магнитных дисках (НГМД), они же флоппи-диски, они же дискеты

Накопители на жестких магнитных дисках (НЖМД), они же винчестеры (в народе просто «винты»)

Накопители на оптических компакт-дисках:

- CD-ROM (Compact Disk ROM)
- DVD-ROM

Гибкие магнитные диски

- **Гибкие магнитные диски** помещаются в пластмассовый корпус. Такой носитель информации называется дискетой. Дискета вставляется в дисковод, вращающий диск с постоянной угловой скоростью. Магнитная головка дисковода устанавливается на определенную концентрическую дорожку диска, на которую и записывается (или считывается) информация.
- Информационная ёмкость дискеты невелика и составляет всего 1.44 Мбайт. Скорость записи и считывания информации также мала (около 50 Кбайт/с) из-за медленного вращения диска (360 об./мин).

Жесткие магнитные диски

- Жесткий диск (HDD — Hard Disk Drive) относится к несменным дисковым магнитным накопителям. Первый жесткий диск был разработан фирмой IBM в 1973 г. и имел емкость 16 Кбайт. Жесткие магнитные диски представляют собой несколько десятков дисков, размещенных на одной оси, заключенных в металлический корпус и вращающихся с высокой угловой скоростью. Скорость записи и считывания информации с жестких дисков достаточно велика (около 133 Мбайт/с) за счет быстрого вращения дисков (7200 об./мин).
- В жестких дисках используются достаточно хрупкие и миниатюрные элементы. Чтобы сохранить информацию и работоспособность жестких дисков, необходимо оберегать их от ударов и резких изменений пространственной ориентации в процессе работы.

Лазерные дисководы и диски

- **Лазерные** дисководы используют оптический принцип чтения информации. На лазерных дисках CD (CD — Compact Disk, компакт диск) и DVD (DVD — Digital Video Disk, цифровой видеодиск) информация записана на одну спиралевидную дорожку (как на грампластинке), содержащую чередующиеся участки с различной отражающей способностью. Лазерный луч падает на поверхность вращающегося диска, а интенсивность отраженного луча зависит от отражающей способности участка дорожки и приобретает значения 0 или 1. Для сохранности информации лазерные диски надо предохранять от механических повреждений (царапин), а также от загрязнения.
- Существуют CD-R и DVD-R диски информация на которые может быть записана только один раз. На дисках CD-RW и DVD-RW информация может быть записана/перезаписана многократно.

Устройства на основе flash-памяти

- Flash-память - это энергонезависимый тип памяти, позволяющий записывать и хранить данные в микросхемах. Устройства на основе flash-памяти не имеют в своём составе движущихся частей, что обеспечивает высокую сохранность данных при их использовании в мобильных устройствах.
- Flash-память представляет собой микросхему, помещенную в миниатюрный корпус. Для записи или считывания информации накопители подключаются к компьютеру через USB-порт. Информационная емкость карт памяти достигает 1024 Мбайт.

Безопасность съемных носителей

Угрозы:

- **Кража или находка.**
- **Отъем.**
- **Завладение оставленным без присмотра устройством.**
- **Завладение путем мошенничества и социальной инженерии.**

Проблема обеспечения санкционированности использования данных является неоднозначной, но в основном охватывает вопросы защиты данных от нежелательной модификации или уничтожения, а также от несанкционированного их чтения.

Можно выделить три обобщенных механизма управления доступа к данным:

- идентификация пользователя
- непосредственная (физическая) защита данных
- поддержка прав доступа пользователя к данным с возможностью их передачи.

Также проблема сохранения целостности данных имеет организационный аспект

Организационный аспект включает следующие правила:

- носители информации должны храниться в местах, не доступных для посторонних лиц;
- важная информация должна иметь несколько копий на разных носителях;
- защита данных на жестком магнитном диске должна поддерживаться периодическим копированием на гибкие магнитные носители. Частота копирования должна выбираться из соображений минимизации среднего времени на копирование и времени на восстановление информации после последнего копирования в случае возникновении дефектов в модифицированной версии;
- данные, относящиеся к различным задачам, целесообразно хранить отдельно;
- необходимо строго руководствоваться правилами обращения с магнитными носителями

Методы защиты съемных носителей

- **Метод защиты при помощи паролей.**
- **Метод шифрования данных:**
  - **Шифрование всего носителя**
  - **Создание зашифрованного раздела**
  - **Шифрование файлов**
- **Биометрия**
- **Методы защиты от копирования файлов**

Метод защиты при помощи паролей

- Согласно методу защиты при помощи программных паролей, реализуемому программными средствами, процедура общения пользователя с ПЭВМ построена так, что запрещается доступ до тех пор, пока не будет введен пароль. Пароль держится пользователем в тайне и периодически меняется, чтобы предотвратить несанкционированное его использование.
- Метод паролей является самым простым и дешевым, однако не обеспечивает надежной защиты, так как с помощью ПК становится возможным за небольшое время раскрыть действующий пароль и получить доступ к данным. Более того, основная уязвимость метода паролей заключается в том, что пользователи зачастую выбирают очень простые и легкие для запоминания (и тем самым для разгадывания) пароли, которые не меняются длительное время, а нередко остаются прежними и при смене пользователя.

Метод шифрования данных

- Метод шифрования данных – это один из наиболее эффективных методов защиты. Он может быть особенно полезен для усложнения процедуры несанкционированного доступа, даже если обычные средства защиты удалось обойти. Для этого источник информации кодирует ее при помощи некоторого алгоритма шифрования и ключа шифрования. Получаемые зашифрованные выходные данные не может понять никто, кроме владельца ключа.

Применимо к флешкам сегодня существует два типа защиты данных: аппаратный и программный.

- Аппаратное шифрование реализуется за счёт внедрение в конструкцию накопителя дополнительных устройств, которые блокируют возможность его подключения к компьютеру. При этом такие устройства могут иметь различный принцип действия: от физического блокирования доступа к флешке вообще, до использования современных сканеров отпечатков пальца.
- Флешки с аппаратным шифрованием, а значит, с накопителем дополнительных устройств, стоят немало, поэтому покупать их имеет смысл лишь в том случае, когда планируется передавать на них что-то очень секретное. Для остальных же целей достаточно использовать специальное ПО

Можно выделить три основных типа программного шифрования:

- Первый тип подразумевает шифрование всего носителя и доступ к нему по паролю.
- Второй – создание дополнительного зашифрованного раздела на носителе (нечто вроде, скрытой папки) с парольной защитой.
- Третий же вариант – "точечное" шифрование отдельных важных файлов

Биометрия

- Биометрические технологии сегодня активно применяются не только в системах контроля доступа и в смартфонах, но и для защиты данных на носителях информации. Данные хранятся на носителе в зашифрованном виде, а для того, чтобы получить к ним доступ предстоит подтвердить личность, например, приложив палец к площадке датчика.