ЛЕКЦИЯ 14
УДАЛЁННЫЙ ДОСТУП И ЗАЩИТА ДАННЫХ

Лектор

Ст. преподаватель Купо А.Н.

Файловая система и программные средства уплотнения носителей

Удалённый доступ и программные средства ограничения доступа

Файловая система – это часть операционной системы, обеспечивающей организацию хранения и доступа к информации на различных носителях, пользовательский интерфейс при работе с данными, и обеспечения совместного использования файлов несколькими пользователями и процессами.

В отличие от этого файловая система позволяет пользователю оперировать с более удобным для него понятием – **файл**. Файловая система берет на себя **организацию взаимодействия** программ с файлами, расположенными на дисках. Для идентификации файлов используются **имена**.

Различают: обычные файлы, специальные файлы, файлы-каталоги

Общая модель файловой системы

Сравнительные характеристики существующих файловых систем

	FAT	FAT32	NTFS
ОС, её поддерживающие	DOS, Windows 95/98/Me, Windows NT/2000/XP/Vista	Windows 98/Me, Windows 2000/XP/Vista	Windows NT/2000/XP/Vista
Максимальный размер тома	2 Гбайт	практически неограничен	практически неограничен
Макс. число файлов на томе	примерно 65 тысяч	практически не ограничено	практически не ограничено
Имя файла	с поддержкой длинных имен - 255 символов, системный набор символов	с поддержкой длинных имен - 255 символов, системный набор символов	255 символов, любые символы любых алфавитов (65 тысяч разных начертаний)
Возможные атрибуты файла	Базовый набор	Базовый набор	всё, что придет в голову производителям программного обеспечения
Безопасность	нет	нет	да (начиная с Windows 2000 встроена возможность физически шифровать данные)

Сравнительные характеристики существующих файловых систем

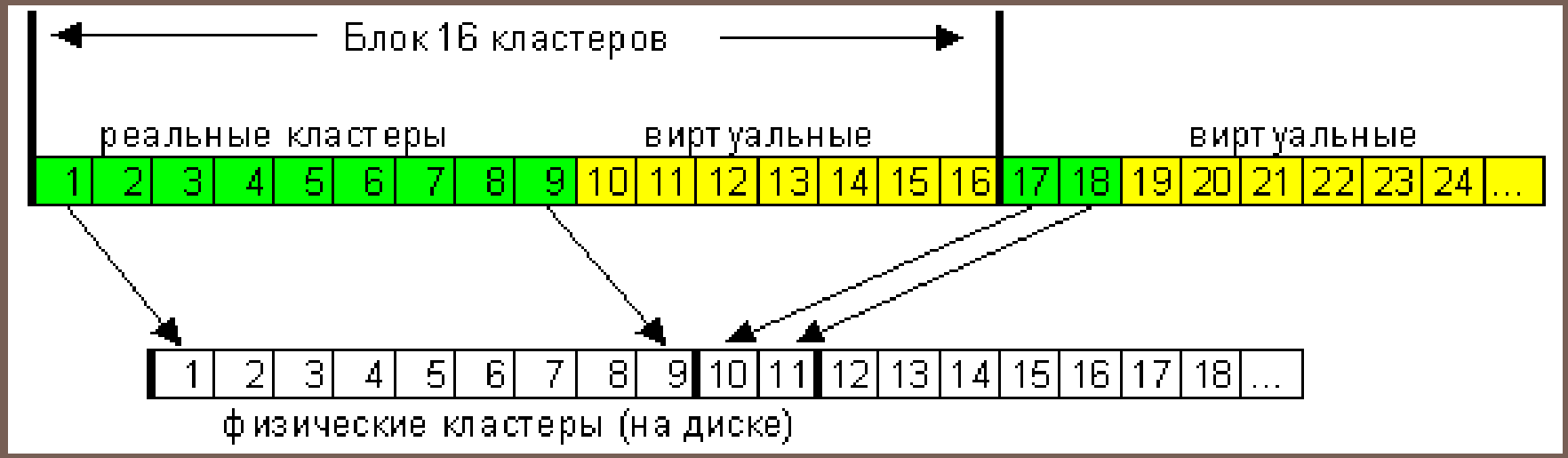
Сжатие	да (только программные средства MSDOS - DoubleSpace, DriveSpace, Stacker)	нет	да
Устойчивость к сбоям	средняя (система слишком проста и поэтому ломаться особо нечему :))	плохая (средства оптимизации по скорости привели к появлению слабых по надежности мест)	полная - автоматическое восстановление системы при любых сбоях (не считая физические ошибки записи, когда пишется одно, а на самом деле записывается другое)
Экономичность	минимальная (огромные размеры кластеров на больших дисках)	улучшена за счет уменьшения размеров кластеров	максимальна. Очень эффективная и разнообразная система хранения данных
Быстродействие	высокое для малого числа файлов, но быстро уменьшается с появлением большого количества файлов в каталогах. результат - для слабо заполненных дисков - максимальное, для заполненных - плохое	полностью аналогично FAT, но на дисках большого размера (десятки гигабайт) начинаются серьезные проблемы с общей организацией данных	система не очень эффективна для малых и простых разделов (до 1 Гбайт), но работа с огромными массивами данных и внушительными каталогами организована как нельзя более эффективно и очень сильно превосходит по скорости другие системы

Сжатие NTFS

Сжатие файлов имеет очень высокую скорость и только одно большое отрицательное свойство – огромная виртуальная фрагментация сжатых файлов.

Сжатие осуществляется блоками по 16 кластеров и использует так называемые "виртуальные кластеры"

Видно, что сжатый файл имеет "виртуальные" кластеры, реальной информации в которых нет. Как только система видит такие виртуальные кластеры, она тут же понимает, что данные предыдущего блока, кратного 16-ти, должны быть разжаты, а получившиеся данные как раз заполнят виртуальные кластеры.



Безопасность информации

Безопасная информационная система — это система, которая:

1. защищает данные от несанкционированного доступа,
2. всегда готова предоставить их своим пользователям
3. надежно хранит информацию
4. гарантирует неизменность данных.

Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

Безопасность информации

- **Конфиденциальность** (confidentiality) — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).
- **Доступность** (availability) — гарантия того, что авторизованные пользователи всегда получат доступ к данным.
- **Целостность** (integrity) — гарантия сохранности данными правильных значений, кото-рая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Безопасность информации

- Любое действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети, называется **угрозой**.

- Реализованная угроза называется **атакой**.

- **Риск** — это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.

Безопасность информации

Неумышленные угрозы вызываются ошибочными действиями лояльных сотрудников, становятся следствием их низкой квалификации или безответственности и(или) последствия ненадежной работы программных и аппаратных средств системы.

Можно выделить следующие типы умышленных угроз:

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- «подслушивание» внутрисетевого трафика.

Безопасность информации

Незаконное проникновение может быть реализовано через уязвимые места в системе безопасности с использованием недокументированных возможностей операционной системы.

Другим способом незаконного проникновения в сеть является использование «чужих» паролей, полученных путем подглядывания, расшифровки файла паролей, подбора паролей или получения пароля путем анализа сетевого трафика.

Нелегальные действия легального пользователя — этот тип угроз исходит от легальных пользователей сети, которые, используя свои полномочия, пытаются выполнять действия, выходящие за рамки их должностных обязанностей.

Безопасность информации

аутентификация, авторизация, аудит и технология защищенного канала.

Аутентификация (authentication) предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей. Термин «аутентификация» в переводе с латинского означает «установление подлинности». Аутентификацию следует отличать от идентификации. Идентификаторы пользователей используются в системе с теми же целями, что и идентификаторы любых других объектов, файлов, процессов, структур данных, но они не связаны непосредственно с обеспечением безопасности. Идентификация заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация — это процедура доказательства пользователем того, что он есть тот, за кого себя выдает, в частности, доказательство того, что именно ему принадлежит введенный им идентификатор.

Безопасность информации

аутентификация, авторизация, аудит и технология защищенного канала.

Средства **авторизации (authorization)** контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые ему были определены администратором. Кроме предоставления прав доступа пользователям к каталогам, файлам и принтерам система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т. п.

Безопасность информации

аутентификация, авторизация, аудит и технология защищенного канала.

Система авторизации наделяет пользователя сети правами выполнять определенные действия над определенными ресурсами. Для этого могут быть использованы различные формы предоставления правил доступа, которые часто делят на два класса:

1. избирательный доступ;

2. мандатный доступ.

Безопасность информации

аутентификация, авторизация, аудит и технология защищенного канала.

Избирательные права доступа реализуются в операционных системах универсального назначения.

Мандатный подход к определению прав доступа заключается в том, что вся информация делится на уровни в зависимости от степени секретности, а все пользователи сети также делятся на группы, образующие иерархию в соответствии с уровнем допуска к этой информации.

Безопасность информации

аутентификация, авторизация, аудит и технология защищенного канала.

Аудит (auditing) — фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Подсистема аудита современных ОС позволяет дифференцирование задавать перечень интересующих администратора событий с помощью удобного графического интерфейса. Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью, или любые попытки создать, получить доступ или удалить системные ресурсы. Аудит используется для того, чтобы засекать даже неудачные попытки «взлома» системы. .

Безопасность информации

аутентификация, авторизация, аудит и технология защищенного канала.

Технология защищенного канала призвана обеспечивать безопасность передачи данных по открытой транспортной сети, например по Интернету.

Защищенный канал подразумевает выполнение трех основных функций:

1. взаимную аутентификацию абонентов при установлении соединения, которая может быть выполнена, например, путем обмена паролями;
2. защиту передаваемых по каналу сообщений от несанкционированного доступа, напри-мер, путем шифрования;
3. подтверждение целостности поступающих по каналу сообщений, например, путем передачи одновременно с сообщением его дайджеста.

Шифрование данных

Любая процедура **шифрования**, превращающая информацию из обычного «понятного» вида в «нечитабельный» зашифрованный вид, естественно, должна быть дополнена процедурой **дешифрирования**, которая, будучи примененной к зашифрованному тексту, снова приводит его в понятный вид. Пара процедур — шифрование и дешифрирование — называется **криптосистемой**.

В современных алгоритмах шифрования предусматривается наличие параметра — секретного ключа. В криптографии принято правило Керкхоффа: «Стойкость шифра должна определяться только секретностью ключа».

ОС Microsoft Windows

- Команда **Всегда просматривать состояние безопасности компьютера**: в центре обеспечения безопасности отображаются основные параметры безопасности и оповещения при возникновении риска.

Команда **Защитить компьютер от атак из Интернета**: брандмауэр Windows включен по умолчанию.

Команда **Проверить наличие последних важных обновлений программ для борьбы с «червями» и вирусами**: упрощенное включение и использование автоматического обновления.

ОС Microsoft Windows

- Команда **Обеспечить повышенную защиту при использовании беспроводных соединений в общественных местах**: использование специальных возможностей для защиты компьютера от других компьютеров в беспроводной сети.

- Команда **Уменьшить доступность компьютера для опасных программ и вирусов**: появление нескольких новых средств безопасности в обозревателе Internet Explorer.

- Команда **Увеличить безопасность чтения сообщений электронной почты**: программа Outlook Express автоматически блокирует рисунки и использует расширенные параметры безопасности обозревателя Internet Explorer.

ОС Microsoft Windows

1. **блокировка компьютера;**
2. **защита файлов с помощью пароля экранной заставки;**
3. **использование паролей для защиты компьютера.**

При создании пароля следует также создать дискету сброса паролей. Если пароль забыт, можно будет с помощью этой дискеты сбросить пароль и получить доступ к своим файлам и программам.

ОС Microsoft Windows

Учётные записи пользователей

Учетная запись пользователя определяет, какие действия пользователь может производить в Windows. На автономном компьютере или на компьютере, входящем в рабочую группу, учетная запись пользователя устанавливает полномочия каждого пользователя. На компьютере, являющимся частью сетевого домена пользователь должен входить по крайней мере в одну группу. Разрешения и права, предоставленные группе, распространяются и на ее членов.

ОС Microsoft Windows

- Учетная запись **администратора** компьютера предназначена для тех, кто может вносить изменения на уровне системы, устанавливать программы и иметь доступ ко всем файлам на компьютере. Пользователь с учетной записью администратора компьютера имеет полный доступ к другим учетным записям пользователей на компьютере.

ОС Microsoft Windows

Администратор

- может создавать и удалять учетные записи пользователей на компьютере
- может создавать пароли для других пользователей на компьютере;
- может изменять в учетной записи имена пользователей, рисунки, пароли и типы учетных записей;
- не может изменить тип своей учетной записи на ограниченную в случае, когда на компьютере больше нет пользователей с учетной записью администратора компьютера.

Таким образом обеспечивается наличие на компьютере по крайней мере одного пользователя с учетной записью администратора.

ОС Microsoft Windows

- Учетная запись с ограниченными правами предназначается для пользователей, которым должно запрещено изменять большинство настроек компьютера и удалять важные файлы. Пользователь с учетной записью с ограниченными правами:
  - не может устанавливать программы и оборудование, но имеет доступ к уже установленным на компьютере программам;
  - может изменять собственный рисунок, назначенный учетной записи, а также создавать, изменять или удалять собственный пароль;
  - не может изменять имя или тип собственной учетной записи.

ОС Microsoft Windows

Учетная запись **гостя** предназначается для пользователей, не имеющих собственных учетных записей на компьютере. У учетной записи гостя нет пароля. Это позволяет быстро входить на компьютер для проверки электронной почты или просмотра Интернета. Пользователь, вошедший с учетной записью гостя:

- не может устанавливать программы и оборудование, но имеет доступ к уже установленным на компьютере программам;
- не может изменить тип учетной записи гостя;
- может изменить рисунок учетной записи гостя.