Контрольные вопросы

https://learn.microsoft.com/ru-RU/troubleshoot/windows-client/backup-and-storage/fat-hpfs-and-ntfs-file-systems

https://xakep.ru/2016/10/28/file-system-secrets/

http://citforum.ru/operating_systems/sos/glava_10

https://docs.microsoft.com/ru-ru/windows/security/identity-protection/access-control/access-control

https://intuit.ru/studies/professional_retraining/962/courses/217/lecture/5609?page=3

https://lektsii.org/9-63798.html

https://windowsnotes.ru/other/nastrojka-razreshenij-fajlovoj-sistemy-ntfs/

https://intuit.ru/studies/courses/631/487/lecture/11059?page=9

Что такое файловая система?

Файловая система - это часть операционной системы, назначение которой состоит в том, чтобы обеспечить пользователю удобный интерфейс при работе с данными, хранящимися на диске, и обеспечить совместное использование файлов несколькими пользователями и процессами.

В широком смысле понятие "файловая система" включает:

- совокупность всех файлов на диске,
- наборы структур данных, используемых для управления файлами, такие, например, как каталоги файлов, дескрипторы файлов, таблицы распределения свободного и занятого пространства на диске,
- комплекс системных программных средств, реализующих управление файлами, в частности: создание, уничтожение, чтение, запись, именование, поиск и другие операции над файлами.

Файлы бывают разных типов: обычные файлы, специальные файлы, файлы-каталоги.

Специальные файлы - это файлы, ассоциированные с устройствами ввода-вывода, которые позволяют пользователю выполнять операции ввода-вывода, используя обычные команды записи в файл или чтения из файла. Эти команды обрабатываются вначале программами файловой системы, а затем на некотором этапе выполнения запроса преобразуются ОС в команды управления соответствующим устройством. Специальные файлы, так же как и устройства ввода-вывода, делятся на блок-ориентированные и байт-ориентированные.

Каталог - это, с одной стороны, группа файлов, объединенных пользователем исходя из некоторых соображений (например, файлы, содержащие программы игр, или файлы, составляющие один программный пакет), а с другой стороны - это файл, содержащий системную информацию о группе файлов, его составляющих. В каталоге содержится список файлов, входящих в него, и устанавливается соответствие между файлами и их характеристиками (атрибутами).

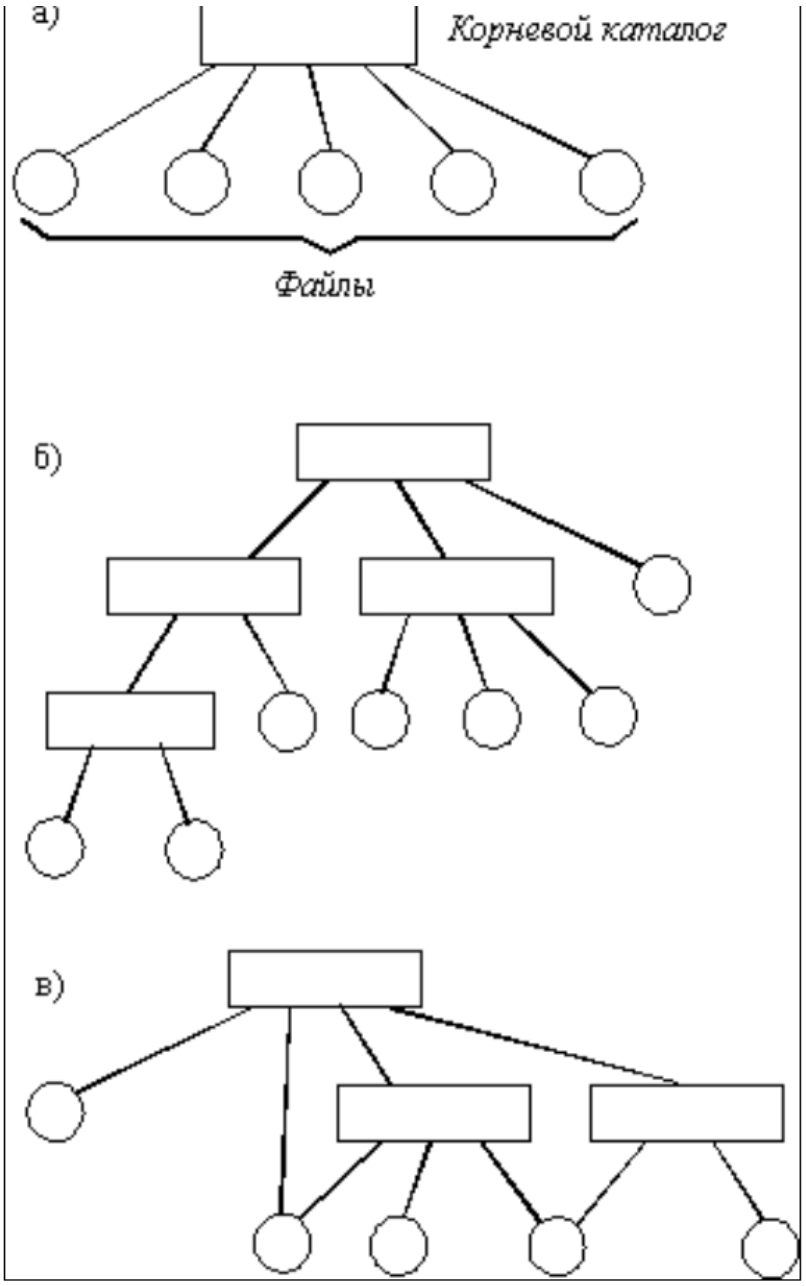


Рис. 2.32. Логическая организация файловой системы
а - одноуровневая; б - иерархическая (дерево); в - иерархическая (сеть)

Основными функциями файловой системы являются:

- размещение и упорядочивание на носителе данных в виде файлов;
- определение максимально поддерживаемого объема данных на носителе информации;
- создание, чтение и удаление файлов;
- назначение и изменение атрибутов файлов (размер, время создания и изменения, владелец и создатель файла, доступен только для чтения,

скрытый файл, временный файл, архивный, исполняемый, максимальная длина имени файла и т.п.);

- определение структуры файла;
- поиск файлов;
- организация каталогов для логической организации файлов;
- защита файлов при системном сбое;
- защита файлов от несанкционированного доступа и изменения их содержимого.

Перечислите существующие файловые системы.

ФАЙЛОВАЯ СИСТЕМА	МАКСИМАЛЬНЫЙ РАЗМЕР ТОМА	ПРЕДЕЛЬНЫЙ РАЗМЕР ОДНОГО ФАЙЛА	ДЛИНА СОБСТВЕННОГО ИМЕНИ ФАЙЛА	ДЛИНА ПОЛНОГО ИМЕНИ ФАЙЛА (ВКЛЮЧАЯ ПУТЬ ОТ КОРНЯ)	ПРЕДЕЛЬНОЕ ЧИСЛО ФАЙЛОВ И/ИЛИ КАТАЛОГОВ
FAT16	2 ГБ секторами по 512 байт или 4 ГБ кластерами по 64 КБ	2 ГБ	255 байт с LFN	-	-
FAT32	8 ТБ секторами по 2 КБ	4 ГБ (2^32 - 1 байт)	255 байт с LFN	до 32 подкаталогов с CDS	65460
EXFAT	≈ 128 ПБ (2^32-1 кластеров по 2^25-1 байт) теоретически / 512 ТБ из-за сторонних ограничений	16 ЭБ (2^64 - 1 байт)	255 символов Unicode (UTF-16)	32760 символов Unicode, но не более 255 символов в каждом элементе	2796202 в каталоге
NTFS	256 ТБ кластерами по 64 КБ или 16 ТБ кластерами по 4 КБ	16 ТБ (Win 7) / 256 ТБ (Win 8)	255 символов Unicode (UTF-16)	32760 символов Unicode, но не более 255 символов в каждом элементе	2^32-1
HFS+	8 ЭБ (2^63 байт)	8 ЭБ	255 символов Unicode (UTF-16)	отдельно не ограничивается	2^32-1
APFS	8 ЭБ (2^63 байт)	8 ЭБ	255 символов Unicode (UTF-16)	отдельно не ограничивается	2^63
EXT3	32 ТБ (теоретически) / 16 ТБ кластерами по 4 КБ (из-за ограничений утилит e2fs programs)	2 ТБ (теоретически) / 16 ГБ у старых программ	255 символов Unicode (UTF-16)	отдельно не ограничивается	-
EXT4	1 ЭБ (теоретически) / 16 ТБ кластерами по 4 КБ (из-за ограничений утилит e2fs programs)	16 ТБ	255 символов Unicode (UTF-16)	отдельно не ограничивается	4 млрд.
F2FS	16 ТБ	3,94 ТБ	255 байт	отдельно не ограничивается	-
BTRFS	16 ЭБ (2^64 - 1 байт)	16 ЭБ	255 символов ASCII	2^17 байт	-

https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D1%84%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D1%8B%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC

Типы файлоывх систем:

https://timeweb.com/ru/community/articles/tipy-faylovyh-sistem-ih-prednaznachenie-i-otlichiya

Какова модель разграничения доступа в ОС Windows?

Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретного субъекта. Правом редактирования дискреционного списка контроля доступа обычно обладают владелец объекта и администратор безопасности. Эта модель отличается простотой реализации, но возможна утечка конфиденциальной информации даже в результате санкционированных действий пользователей.

Мандатная модель разграничения доступа предполагает назначение объекту метки (грифа) секретности, а субъекту – уровня допуска. Доступ субъектов к объектам в мандатной модели определяется на основании правил «не читать выше» и «не записывать ниже». Использование мандатной модели, в отличие от дискреционного управления доступом, предотвращает утечку конфиденциальной информации, но снижает производительность компьютерной системы.

Ролевая модель разграничения доступа основана на конструировании ролей и назначении их пользователям на основании выполняемых ими конкретных должностных обязанностей. При назначении и использовании ролей возможно наложение динамических и статических ограничений на совмещение разных ролей одним субъектом, одновременное использование одной роли разными субъектами и т.п. Подобный подход к разграничению доступа к объектам позволяет разделить обязанности между конструктором ролей и диспетчером ролей, а также более точно связать права доступа пользователей к объектам компьютерной системы с их обязанностями в организации, исключить избыточность полномочий.

В операционных системах Microsoft Windows и операционных системах клона Unix обычно применяется дискреционное управление доступом к объектам. Объекты разграничения доступа в Windows имеют дескриптор безопасности, содержащий информацию о владельце объекта (его идентификаторе безопасности SID, Security Identifier) и дискреционном списке управления доступом к объекту (Discretionary Access Control List, DACL), правом

редактирования которого обладают владелец объекта и администратор. Владелец файла может лишить администратора права изменения разрешений на доступ к объекту. Администратор обладает специальной привилегией смены владельца на другого пользователя, обладающего такой же специальной привилегией (например, на самого себя).

Разграничение доступа к файлам и папкам возможно с помощью Проводника Windows (вкладки Безопасность функций Свойства контекстного меню выделенного объекта), принтеру – с помощью функции Принтеры и факсы Панели управления (вкладки Безопасность функции Свойства выделенного принтера), реестру Windows – с помощью Редактора реестра regedit.exe (функции Разрешения контекстного меню выделенного раздела).

https://learn.microsoft.com/ru-ru/windows/security/identity-protection/access-control/access-control

Что такое DACL?

access control list (ACL) is a list of access control entries (ACE). Каждый ACE в ACL идентифицирует доверенного лица и указывает права доступа , разрешенные, запрещенные или проверенные для этого доверенного лица. Дескриптор безопасности для защищаемого объекта может содержать два типа списков управления доступом: *DACL* и *SACL*.

Список управления доступом на уровне пользователей (DACL) определяет доверенных лиц, которым разрешен или запрещен доступ к защищаемому объекту. Когда процесс пытается получить доступ к защищаемому объекту, система проверяет ACE в DACL объекта, чтобы определить, следует ли предоставить доступ к нему. Если у объекта нет DACL, система предоставляет полный доступ всем пользователям. Если dacl объекта не имеет ACE, система отклоняет все попытки доступа к объекту, так как DACL не разрешает какие-либо права доступа. Система проверяет ACE в последовательности, пока не найдет один или несколько ACE, которые разрешают все запрошенные права

доступа, или пока не будет отказано в любом из запрошенных прав доступа. Дополнительные сведения см. в разделе Управление доступом к объекту DACLs. Сведения о том, как правильно создать DACL, см. в разделе Создание DACL.

Системный список управления доступом (SACL) позволяет администраторам регистрировать попытки доступа к защищенному объекту. Каждый ACE указывает типы попыток доступа со стороны указанного доверенного лица, которые приводят к созданию системой записи в журнале событий безопасности. ACE в SACL может создавать записи аудита при сбое попытки доступа, при успешном выполнении или и в том, Дополнительные сведения о списках SACL см. в разделе Аудит создания и права доступа к saCL.

Перечислите существующие разрешения для пользователей.

ОС Windows предоставляет различные уровни разрешений для пользователей, определяющие их доступ к разным ресурсам и функциональности системы. Вот некоторые основные разрешения и группы пользователей:

1. Администратор (Administrator):

- Полный доступ ко всем ресурсам и функциям системы.

- Возможность изменять системные настройки, устанавливать и удалять программы.

2. Пользователь (User):

- Обычные пользователи с ограниченными правами.

- Могут использовать приложения, создавать и изменять свои файлы в своей учетной записи.

3. Гость (Guest):

- Ограниченные права доступа.

- Обычно используется для временного доступа к системе без создания учетной записи.

4. Группы пользователей:

- Различные группы, такие как "Администраторы", "Пользователи", "Гости" и др.

- Присвоение пользователя к определенной группе предоставляет ему соответствующие права.

5. Права доступа к файлам и папкам:

- Чтение (Read), Запись (Write), Исполнение (Execute), Полный доступ (Full Control), и т.д.

- Разрешения можно устанавливать для отдельных файлов и папок.

6. Права на выполнение задач (Task Execution Rights):

- Определяют, какие задачи могут быть выполнены пользователями (например, установка программ).

7. Права на реестр (Registry Rights):

- Разрешения для изменения данных в реестре системы.

8. Права на сетевые ресурсы (Network Rights):

- Определяют доступ к сетевым ресурсам, таким как общие папки и принтеры.

9. Права на удаленный доступ (Remote Rights):

- Определяют возможность удаленного управления и доступа к компьютеру.

Это общие категории разрешений, и конкретные права могут варьироваться в зависимости от конфигурации системы и версии ОС Windows.
Пользовательские права можно управлять с помощью "Панели управления" и инструментов безопасности.

http://www.oszone.net/4024/File_and_Folder_Permissions

Существуют следующие базовые разрешения на доступ к файлам: Полный доступ (Full Control), Изменить (Modify), Чтение и Выполнение (Read & Execute), Чтение (Read) и Запись (Write).
Для папок применимы такие базовые разрешения: Полный доступ (Full Control), Изменить (Modify), Чтение и Выполнение (Read & Execute), Список содержимого папки (List Folder Contents), Чтение (Read) и Запись (Write).

Базовое разрешение	Значение для папок	Значение для файлов
Чтение (Read)	Разрешает обзор папок и просмотр списка файлов и подпапок	Разрешает просмотр и доступ к содержимому файла
Запись (Write)	Разрешает добавление файлов и подпапок	Разрешает запись данных в файл
Чтение и Выполнение (Read & Execute)	Разрешает обзор папок и просмотр списка файлов и подпапок; наследуется файлами и папками	Разрешает просмотр и доступ к содержимому файла, а также запуск исполняемого файла
Список содержимого папки (List Folder Contents)	Разрешает обзор папок и просмотр списка файлов и подпапок; наследуется только папками	Не применимо
Изменить (Modify)	Разрешает просмотр содержимого и создание файлов и подпапок; допускает удаление папки	Разрешает чтение и запись данных в файл; допускает удаление файла
Полный доступ (Full Control)	Разрешает просмотр содержимого, а также создание, изменение и удаление файлов и подпапок	Разрешает чтение и запись данных, а также изменение и удаление файла

Особые разрешения	Полный доступ (Full Control)	Изменить (Modify)	Чтение и выполнение (Read & Execute)	Чтение (Read)	Запись (Write)
Выполнение файлов (Execute File)	X	X	X		
Чтение данных (Read Data)	X	X	X	X	
Чтение атрибутов (Read Attributes)	X	X	X	X	
Чтение дополнительных атрибутов (Read Extended Attributes)	X	X	X	X	
Запись данных (Write Data)	X	X			X
Дозапись данных (Append Data)	X	X			X
Запись атрибутов (Write Attributes)	X	X			X
Запись дополнительных атрибутов (Write Extended Attributes)	X	X			X
Удаление (Delete)	X	X			
Чтение разрешений (Read Permissions)	X	X	X	X	X
Смена разрешений (Change Permissions)	X				
Смена владельца (Take Ownership)	X				

Особые разрешения	Полный доступ (Full Control)	Изменить (Modify)	Чтение и выполнение (Read & Execute)	Список содержимого папки (List Folder Contents)	Чтение (Read)	Запись (Write)
Обзор папок (Traverse Folder)	X	X	X	X		
Содержание папки (List Folder)	X	X	X	X	X	
Чтение атрибутов (Read Attributes)	X	X	X	X	X	
Чтение дополнительных атрибутов (Read Extended Attributes)	X	X	X	X	X	
Создание файлов (Create Files)	X	X				X
Создание папок (Create Folders)	X	X				X
Запись атрибутов (Write Attributes)	X	X				X
Запись дополнительных атрибутов (Write Extended Attributes)	X	X				X
Удаление подпапок и файлов (Delete Subfolders and Files)	X					
Удаление (Delete)	X	X				
Чтение разрешений (Read Permissions)	X	X	X	X	X	X
Смена разрешений (Change Permissions)	X					
Смена владельца (Take Ownership)	X					

https://www.dell.com/support/kbdoc/ru-rs/000137238/%D0%BE%D0%B1%D1%89%D0%B8%D0%B5-%D1%81%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F-%D0%BE-%D1%80%D0%B0%D0%B7%D1%80%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D1%8F%D1%85-%D0%B4%D0%BB%D1%8F-%D1%84%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2-%D0%B8-%D0%BF%D0%B0%D0%BF%D0%BE%D0%BA-%D0%B2-windows

Расскажите про наследование разрешений.

В операционной системе Windows 10 наследование разрешений является важной концепцией для управления доступом к файлам и папкам. Наследование позволяет применять разрешения, установленные для родительского объекта (например, папки), к его дочерним объектам (например, файлам внутри этой папки). Это облегчает управление разрешениями и обеспечивает более эффективное и последовательное управление доступом.

Вот основные моменты, касающиеся наследования разрешений в Windows 10:

1. **Родительский объект (папка):** Когда вы устанавливаете разрешения для папки, эти разрешения могут быть унаследованы всеми файлами и подпапками внутри нее.
2. **Унаследованные разрешения:** По умолчанию, новые файлы и подпапки, создаваемые внутри папки, автоматически наследуют разрешения этой папки. Таким образом, управление разрешениями для родительской папки автоматически распространяется на все ее содержимое.
3. **Изменение наследуемых разрешений:** Вы можете изменять или отменять наследование разрешений для конкретного файла или подпапки. Это позволяет создавать специфические настройки доступа для определенных объектов внутри родительской папки.
4. **Продвинутое управление:** В дополнение к базовым разрешениям (чтение, запись, выполнение), вы можете использовать дополнительные возможности, такие как наследование, отказ в доступе, аудит и т. д.
5. **Наследование ACL (Access Control List):** Наследование разрешений осуществляется через список управления доступом (ACL). ACL содержит записи (ACE), определяющие разрешения для конкретных пользователей или групп.
6. **Процесс изменения разрешений:** При изменении разрешений для родительской папки вы можете выбрать опцию "Применить только к этому объекту" или "Применить ко всем подпапкам и файлам". Это позволяет настроить, как изменения должны распространяться по иерархии.

Для изменения разрешений и управления наследованием разрешений в Windows 10, вы можете использовать свойства файла или папки, перейдя во

вкладку "Безопасность". Здесь вы найдете информацию о текущих разрешениях и сможете внести необходимые изменения.

Эти возможности позволяют более гибко управлять безопасностью данных в операционной системе Windows 10 и обеспечивают эффективное управление доступом пользователей к файлам и папкам.

В операционной системе Windows 10 разрешения могут быть установлены на различные ресурсы, такие как файлы, папки и разделы реестра. Когда вы устанавливаете разрешения для родительского объекта (например, папки), эти разрешения могут наследоваться всеми дочерними объектами (например, файлами и подпапками внутри этой папки). Вот типичные разрешения, которые могут наследоваться:

1. **Чтение (Read):** Позволяет просматривать содержимое файла или папки.
2. **Запись (Write):** Позволяет создавать, изменять и удалять файлы внутри папки, а также изменять содержимое файлов.
3. **Выполнение (Execute):** Для папок это разрешение позволяет входить в папку и выполнять в ней операции. Для файлов оно обозначает возможность запуска исполняемого файла.
4. **Полный доступ (Full Control):** Предоставляет полный контроль над файлом или папкой, включая возможность изменения разрешений.
5. **Специальные разрешения (Special Permissions):** Это более детальные разрешения, которые могут включать в себя такие возможности, как изменение разрешений, владение объектом, аудит и другие.

Когда устанавливаются разрешения для родительской папки, эти разрешения по умолчанию наследуются всеми новыми файлами и подпапками внутри этой папки. Однако, важно отметить, что можно изменить или отменить наследование разрешений для конкретных объектов в структуре файловой системы.

При необходимости можно также использовать продвинутые настройки разрешений, такие как отдельные настройки для конкретных пользователей или групп пользователей, а также настройки аудита для отслеживания событий доступа к файлам и папкам.

Где изменять наследование разрешений:

Свойство папки - Безопасность - Дополнительно - Изменить разрешения - Отключить наследование - преобразовать унаследованные разрешения в явные… Дальше делай нужные права (добавляй / удаляй)

Перечислите способы для разграничения доступа.

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

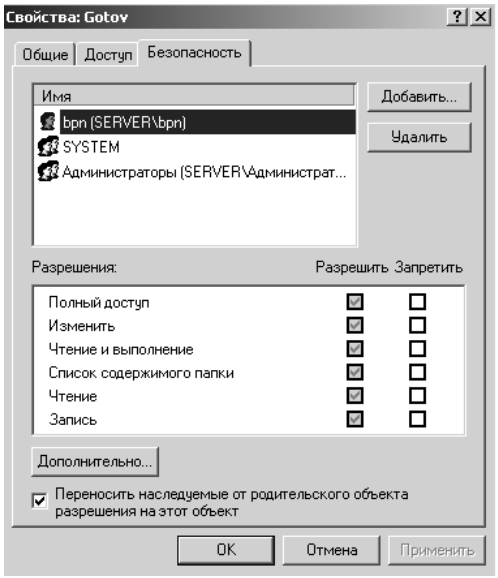
Существуют следующие методы разграничения доступа:

1. разграничение доступа по спискам;
2. использование матрицы установления полномочий;
3. разграничение доступа по уровням секретности и категориям;
4. парольное разграничение доступа.

При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Пример (операционная система Windows 2000) разграничения доступа по спискам для одного объекта показан на рисунке 1.



Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами — объекты (ресурсы) информационной системы. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, т.к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток — пустые).

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы по уровням секретности и категориям.

При разграничении по уровню секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен, например, пользователь имеющий доступ к данным «секретно» также имеет доступ к данным «конфиденциально» и «общий доступ».

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы информационной системы разделяются по уровням важности, причем определенному уровню соответствует категория пользователей. В качестве примера, где используются категории пользователей, приведем операционную систему Windows 2000, подсистема безопасности которой по умолчанию поддерживает следующие категории (группы) пользователей: «администратор», «опытный пользователь», «пользователь» и «гость». Каждая из категорий имеет определенный набор прав. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности.

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

Разграничение прав доступа является обязательным элементом защищенной информационной системы. Напомним, что еще в «Оранжевой книге США» были введены понятия:

— произвольное управление доступом;

— принудительное управление доступом.

4.3.2 Мандатное и дискретное управление доступом

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа:

- дискретное управление доступом;
- мандатное управление доступом.

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом — основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

При внимательном рассмотрении можно заметить, что дискретное управление доступом есть ничто иное, как произвольное управление доступом (по «Оранжевой книге США»), а мандатное управление реализует принудительное управление доступом.

В чем отличие между пользовательскими и системными переменными окружения?

В операционной системе Windows существуют два типа переменных окружения: пользовательские и системные. Вот их основные отличия:

1. **Область действия:**
    - **Пользовательские переменные окружения (User Environment Variables):** Привязаны к конкретному пользователю. Они действуют только для того пользователя, который их создал, и не влияют на других пользователей системы.
    - **Системные переменные окружения (System Environment Variables):** Применяются ко всей системе. Они действуют для всех пользователей, включая системные службы.
2. **Уровень приоритета:**

Приоритет между пользовательскими и системными переменными окружения зависит от того, какая из них имеет более высокий уровень. В общем, если есть конфликт между пользовательской и системной переменной с одинаковым именем, то переменная с более высоким уровнем имеет приоритет.
Если пользовательская и системная переменные с именем `MY_VARIABLE` существуют одновременно, то при использовании переменной в контексте

данного пользователя будет использовано значение пользовательской переменной (`User Value`). Если бы пользователь удалил свою пользовательскую переменную, тогда бы использовалось значение системной переменной (`System Value`).

Таким образом, пользовательские переменные имеют приоритет над системными переменными в том случае, если у них одинаковые имена.

3. **Изменение:**

    - **Пользовательские переменные окружения:** Могут быть изменены и настроены конкретным пользователем. Обычно устанавливаются через интерфейс управления системой.
    - **Системные переменные окружения:** Обычно устанавливаются при установке операционной системы или при установке дополнительного программного обеспечения. Их изменение требует административных прав.

4. **Безопасность:**

    - **Пользовательские переменные окружения:** Ограничены правами пользователя, который их создал. Не могут повлиять на других пользователей.
    - **Системные переменные окружения:** Требуют административных прав для изменения. Изменение системных переменных может повлиять на все пользователи и системные службы.

Примеры использования переменных окружения включают указание путей к исполняемым файлам, установку опций конфигурации и другие параметры, которые могут влиять на поведение программ и системы в целом.

Перечислите три достоинства FAT.

Файловая система FAT (File Allocation Table) имеет несколько преимуществ, которые в определенных сценариях делают ее предпочтительной. Вот некоторые из них:

1.1) Поддержка широкого спектра устройств:

- FAT поддерживается многими операционными системами, что делает ее универсальной и совместимой с различными устройствами, такими как флеш-накопители, карты памяти, старые жесткие диски и т. д.

1.2) Поддержка множественных операционных систем:

- FAT является стандартной файловой системой для различных платформ, включая Windows, macOS и многие встраиваемые системы. Это делает устройства, форматированные в FAT, легко доступными для обмена данными между разными операционными системами.

2) Простота и эффективность:

- FAT - простая файловая система, что облегчает ее реализацию и использование. Она не требует сложных механизмов управления и обеспечивает достаточно быстрый доступ к файлам.

3) Восстановление данных и отмена удаления:

- FAT имеет механизм восстановления данных после сбоев, что может быть полезно для устройств с ограниченным доступом к электропитанию или подверженных неожиданным отключениям.
- Невозможно выполнить отмену удаления в разделе Windows NT в любой из поддерживаемых файловых систем. При отмене удаления служебные программы пытаются получить прямой доступ к оборудованию, что невозможно сделать в Windows NT. Однако если файл был расположен в секции FAT и система перезапущена в MS-DOS, файл можно отменить.

4?) Поддержка огромных объемов данных:

- В зависимости от версии (FAT12, FAT16, FAT32), FAT поддерживает различные объемы данных, вплоть до терабайтов (в случае FAT32). Это может быть полезно для устройств с большим объемом хранения данных.

Несмотря на эти преимущества, стоит отметить, что у FAT есть и недостатки, такие как ограничение на размер файла и объем файловой системы, относительно более новых файловых систем, таких как NTFS (New Technology File System) и exFAT (Extended File Allocation Table). Решение о выборе файловой системы зависит от конкретных требований проекта и сценариев использования.

Перечислите три недостатка NTFS.

Несмотря на то, что файловая система NTFS (New Technology File System) является одной из наиболее распространенных и функциональных файловых систем для операционных систем Windows, у нее есть некоторые недостатки:

1) Несовместимость с некоторыми другими операционными системами: NTFS является проприетарной файловой системой, созданной Microsoft, и ее поддержка может быть ограничена в некоторых других операционных системах, таких как Linux или macOS. Хотя существуют некоторые сторонние драйверы для поддержки NTFS на этих платформах, они могут не обеспечивать полную совместимость.

2.1) Большой объем метаданных: NTFS имеет больший объем метаданных по сравнению с некоторыми другими файловыми системами. Это может привести к незначительному увеличению использования дискового пространства на маленьких разделах.

2.2) Относительная сложность: NTFS обладает богатым набором функций и возможностей, но это может сделать его более сложным в сравнении с более простыми файловыми системами, особенно для неопытных пользователей.

3.1) Ограниченная поддержка аттрибутов файлов в стандартных приложениях: Некоторые атрибуты файлов, поддерживаемые NTFS, могут не использоваться или не поддерживаться стандартными приложениями, что может снизить полезность этих функций.

3.2) Отсутствие нативной поддержки архитектуры журналирования для всех операционных систем: NTFS использует журналирование для обеспечения целостности данных в случае сбоев или сбоев системы. Однако не все операционные системы, которые могут читать NTFS, полностью поддерживают эту функцию, что может привести к потере данных при критических событиях.

The main difference between the two, in my opinion, is how they handle permissions. Linux uses POSIX permissions for managing files in a file system. Unfortunately, NTFS is not compatible with this permission system, and that's why you really shouldn't use it as a system (or even /home) partition, for that matter. That basically means that any user would be able to modify any file in the FS - which is usually a bad idea.

4) Невозможность отмены удаления.

Несмотря на эти недостатки, NTFS остается широко используемой файловой системой в среде Windows благодаря своей высокой надежности, поддержке разрешения конфликтов и расширенным функциональным возможностям.