МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ П. О. СУХОГО

Факультет автоматизированных и информационных систем

Кафедра «Информационные технологии»

Реферат

на тему: **Управление файловой системой. Управление доступом**

Выполнила студентка гр. ИТП-11
Леоненко В.Ю.
Принял преподаватель
Точко В.Н.

Гомель 2021

ОГЛАВЛЕНИЕ

1. Общие понятия 3
2. Управление доступом в *Windows* 4
2.1 Учётная запись пользователей 4
2.2 Управление доступом к файловой системе 6
2.3 Управление доступом к реестру 9
2.4 Управление доступом к общим (сетевым) ресурсам 10
2.5 Особые папки общего доступа 12
3. Управление доступом в *Linux* 13
3.1 Управление доступом к файловой системе 13
3.2 *Suid* и *Sgid* 14
4. Инструменты управления доступом к объектам в *Windows* 15
Список использованных источников 16

1. ОБЩИЕ ПОНЯТИЯ

Системы линейки *Windows 9x* не являются многопользовательскими в том понимании, что не позволяют разграничить доступ к ресурсам, а лишь позволяют выбрать профиль - способ отображения данных в соответствии с настройками того или иного пользователя. В системах линейки *Linux* и *Windows NT* доступ к объектам управляется операционной системой. Перечень объектов, к которым может разграничиваться доступ зависит от конкретного типа ОС. Например, в *Windows* защищаемыми объектами могут быть файлы, устройства, каналы, задания, процессы, потоки, объекты синхронизации, порты ввода-вывода, разделы общей памяти, сетевые ресурсы, разделы реестра и др.

Управление доступом заключается в предоставлении пользователям, группам и компьютерам определенных разрешений на доступ к объектам ОС.

Разрешение представляет собой правило, связанное с объектом ОС, которое определяет, каким пользователям и какого типа доступ к объекту разрешен.

Назначаемые разрешения зависят от вида объекта. Например, в *Windows* разрешения, которые могут быть назначены для файла, отличаются от разрешений, допустимых для раздела реестра.

Владение объектами.

При создании объекта ему назначается владелец. По умолчанию владельцем объекта становится его создатель. Какие разрешения ни были бы установлены для объекта, владелец объекта всегда может изменить эти разрешения.

Наследование разрешений.

Механизм наследования облегчает администраторам задачи назначения разрешений и управления ими. Благодаря этому механизму разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера. Например, файлы, создаваемые в папке, наследуют разрешения этой папки.

2. УПРАВЛЕНИЕ ДОСТУПОМ В *WINDOWS*

2.1 Учётная запись пользователей

Для каждого зарегистрированного пользователя система создает свою учетную запись. Учетные записи всех пользователей хранятся в некой системной базе данных. Упрощенно она представляет собой таблицу, схематически показанную на рисунке 1.

Рисунок 1 – База данных учетных записей

Для каждой учетной записи система хранит имена, пароли и уникальные идентификаторы – *SID (Security Identifier)*. Последний используется системой в дальнейшем везде, где нужно однозначно сослаться на ту или иную учетную запись. База данных учетных записей содержит сведения не только о пользователях, но и группах пользователей (например, администраторы), которые также имеют *SID*. Группы позволяют нескольким пользователям задать общие права доступа. Управление учетными записями с помощью групп позволяет упростить работу администратора по контролю доступа пользователей к ресурсам.

Для каждого объекта или ресурса ОС, поддерживается контрольный список доступа (*Access Control List – ACL*). Он определяет перечень пользователей, которым разрешен доступ к данному объекту, а также тех, кому запрещен.

Каждый список контроля доступа (*ACL*) представляет собой набор элементов контроля доступа (*Access Control Entries*, или *ACE*).

Рисунок 2 – *ACL* и *ACE*

ACE бывает двух типов (разрешающий и запрещающий доступ) и обязательно содержит три поля:

– *SID* пользователя или группы;

– вид доступа, на которое распространяется данное правило;

– тип *ACE* – разрешающий или запрещающий.

Таким образом, *ACL*, изображенный на рис.2, устанавливает следующие правила: пользователю *SID1* разрешить доступ на чтение объекта, но запретить доступ на запись, а пользователю *SID2* – разрешить полный доступ к объекту.

Кроме того, к дескриптору безопасности применимы следующие правила:

– если *ACL* отсутствует, то объект считается незащищенным, т. е. все имеют к нему неограниченный доступ;

– если *ACL* существует, но не содержит ни одного *ACE*, то доступ к объекту закрыт для всех.

Теоретически может сложиться такая ситуация, когда два *ACE* противоречат друг другу. Например, один *ACE* дает полный доступ членам определенной группы, а другой – запрещает доступ определенному пользователю из этой группы. Получит ли этот пользователь доступ к объекту зависит от того, в каком порядке *ACE* расположены.

Когда процесс запрашивает определенный вид доступа к защищенному объекту, система действует по следующему алгоритму:

– просматриваются все *ACE* в *ACL* от первого к последнему;

– если хотя бы один из видов запрошенного доступа не предоставлен (запрещен или достигнут конец *ACL*), система принимает решение отказать в доступе к объекту.

Определяющую роль играет первый встреченный элемент, дающий возможность пользователю воспользоваться запрошенной услугой или отказывающий в этом.

Из этого можно сделать вывод, что запрещающие элементы не имеет смысла размещать внизу *ACL*, так как если перед ними нет соответствующих разрешающих, доступ все равно будет закрыт. Запрещающие элементы обычно размещают вверху списка, особенно если нужно запретить доступ конкретному пользователю, который может его получить, воспользовавшись членством в группе. В *Windows XP* запрещающие элементы автоматически помещаются вверху *ACL*.

2.2 Управление доступом к файловой системе

Базовые разрешения объектов файловой системы *Windows* приведены в таблице 1.

Таблица 1 - Базовые разрешения для файлов и папок

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

При вычислении действующих разрешений пользователя принимаются во внимание все разрешения назначенные пользователю, а также группам, членом которых он является.

Помимо базовых разрешений существуют также особые разрешения объектов. В отличие от базовых они более конкретны и используются для более точной настройки разрешений к файловым объектам.

Взаимосвязь между базовыми и особыми разрешениями приведены в таблице 2.

Таблица 2 - Особые разрешения для файловых объектов

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

2.3 Управление доступом к реестру

Реестр *Windows* представляет собой реляционную базу данных, в которой аккумулируется вся необходимая для нормального функционирования компьютера информация о настройках операционной системы, а также об используемом совместно с *Windows* программном обеспечении и оборудовании. Все хранящиеся в реестре данные представлены в стандартизированной форме и четко структурированы согласно предложенной разработчиками *Windows* иерархии.

Ветвь *HKEY_CLASSES_ROOT*, обычно обозначаемая в технической документации аббревиатурой *HKCR*, включает в себя ряд подразделов, в которых содержатся сведения о расширениях всех зарегистрированных в системе типов файлов и данные о *COM*-серверах, зарегистрированных на компьютере. Фактически, данную ветвь с функциональной точки зрения можно считать аналогом ключа *HKEY_LOCAL_MACHINE\Software*, поскольку здесь собраны все необходимые операционной системе данные о файловых ассоциациях.

В ветви *HKEY_CURRENT_USER*, обозначаемой в документации аббревиатурой *HKCU*, содержится информация о пользователе, ведущем на компьютере текущий сеанс работы, который обслуживается реестром. В ее подразделах находится информация о переменных окружения, группах программ данного пользователя, настройках Рабочего стола, цветах экрана, сетевых соединениях, принтерах и дополнительных настройках приложений (переменные окружения используются в *Windows* в сценариях, записях реестра и других приложениях в качестве подстановочных параметров). Эта информация берется из подраздела *Security ID (SID)* ветви *HKEY_USERS* для текущего пользователя. Фактически, в данной ветви собраны все сведения, относящиеся к профилю пользователя, работающего с *Windows* в настоящий момент.

HKEY_LOCAL_MACHINE (HKLM) – это ветвь, в которой содержится информация, относящаяся к операционной системе и оборудованию, например, тип шины компьютера, общий объем доступной памяти, список загруженных в данный момент времени драйверов устройств, а также сведения о загрузке *Windows*. Данная ветвь включает наибольшее количество информации в системном реестре *Windows* и нередко используется для тонкой настройки аппаратной конфигурации компьютера. Следует понимать, что хранящиеся в этой ветви данные справедливы для всех профилей, зарегистрированных в системе пользователей.

Ветвь *HKEY_USERS (HKU)* содержит подразделы с информацией обо всех профилях пользователей данного компьютера. Один из ее подразделов всегда соотносится с подразделом *HKEY_CURRENT_USER* (через параметр

Security ID (SID) пользователя). Другой подраздел, *HKEY_USERS\DEFAULT*, содержит информацию о настройках системы в момент времени, предшествующий началу сеанса текущего пользователя.

Ветвь *HKEY_CURRENT_CONFIG (HKCC)* содержит подразделы с информацией обо всех профилях оборудования, используемого в данном сеансе работы. Профили оборудования позволяют выбрать драйверы поддерживаемых устройств для заданного сеанса работы (например, не использовать активацию порта док-станции переносного компьютера, когда он не подключен к станции). Эта информация берется из подразделов *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*.

Вполне очевидно также, что некорректное изменение хранящейся в реестре информации вполне способно нарушить работоспособность *Windows*. Достаточно допустить ошибку в записи значения какого-либо ключа или параметра, и пользователь больше не сможет загрузить компьютер. Именно по этой причине разработчики *Windows* заметно ограничили доступ к реестру, и редактировать параметры реестра, касающиеся безопасности, могут только пользователи *Windows*, имеющие в системе учетную запись Администратора. Для редактирования и управления доступом к реестру предназначена стандартная утилита *Regedit*. Управление доступом осуществляется аналогично управлению доступом к файловой системе, с тем отличием, что *ACL* устанавливаются не для папок и файлов, а для разделов и ключей реестра. [2, с.131]

2.4 Управление доступом к общим (сетевым) ресурсам

Файлы и папки, хранящиеся на локальном компьютере, в сети или в Интернете, можно передавать в общий доступ. Файлы и папки, находящиеся в общем доступе, менее защищены, чем при отсутствии общего доступа к ним. Пользователи, имеющие доступ к компьютеру по сети, в зависимости от установленных разрешений, могут просматривать, копировать, изменять, создавать или удалять файлы, содержащиеся в общей папке.

В общем случае, лучше всего задавать разрешения с помощью файловой системы *NTFS* – в этом случае применяются более строгие разрешения. Однако имеется возможность задавать собственные разрешения для общих (сетевых) ресурсов. Эти разрешения применяются только к пользователям, доступ которых к ресурсу осуществляется по сети. Они не применяются к пользователям, которые получают доступ к ресурсу на компьютере, на котором сохранен ресурс.

Разрешения применяются ко всем файлам и папкам общего ресурса. По этим причинам разрешения для общих ресурсов обеспечивают меньший уровень безопасности, чем разрешения *NTFS*. Однако эти разрешения являются единственным способом защиты сетевых ресурсов для томов с файловыми системами *FAT* и *FAT32*, поскольку разрешения *NTFS* не доступны для томов с файловыми системами *FAT* и *FAT32*.

Разрешениями определяются максимальные права доступа пользователя к общему ресурсу при работе в сети. Все эти свойства являются дополнением безопасности, предоставляемой файловой системой *NTFS* (т. е. разрешения файловой системы и собственные разрешения общего ресурса при доступе к нему по сети действуют в совокупности!).

Имеется возможность применять следующие типы разрешений доступа к общим папкам или дискам:

1. чтение;
2. изменить;
3. полный доступ.

Разрешение «Чтение» позволяет:

- просматривать имена файлов и подкаталогов;
- просматривать подпапки;
- просматривать данные в файлах;
- выполнять программные файлы.

Разрешение «Изменить» включает разрешение «Чтение», а также позволяет:

- добавлять файлы и подпапки;
- изменять данные в файлах;
- удалять подпапки и файлы.

Разрешение «Полный доступ» используется по умолчанию для всех новых общих ресурсов. При общем использовании ресурса это разрешение назначается группе «Все». Разрешение «Полный доступ» включает разрешения «Изменить» и «Чтение», а также позволяет:

- изменять разрешения (только для файлов и папок *NTFS*);
- стать владельцем (только для файлов и каталогов *NTFS*).

2.5 Особые папки общего доступа

Помимо папок общего доступа, которые создает пользователь в процессе своей работы, существуют особые общие ресурсы, которые называются административными или системными. Ниже приведен полный список такого рода ресурсов.

Таблица 3 – Список ресурсов

Ресурс	Описание
Имя диска	Представляет собой общий ресурс, который позволяет администраторам подключаться к корневому каталогу диска.
ADMIN	Это ресурс, который используется при удаленном администрировании компьютера. Путь к этому общему ресурсу всегда совпадает с путем к системному каталогу (т. е. каталогу, в котором установлена система, например *C:\Windows*).
IPC	Представляет собой ресурс совместного доступа к именованным каналам, которые обеспечивают связь между программами. Используется для удаленного администрирования компьютера и для просмотра общих ресурсов компьютера. Этот ресурс нельзя удалить.
PRINT	Общий ресурс, используемый для удаленного администрирования принтеров.

3. УПРАВЛЕНИЕ ДОСТУПОМ В *LINUX*

3.1 Управление доступом к файловой системе

Классическая система управления доступом в *Linux* несколько отличается от рассмотренной выше системы в *Windows*, хотя присутствуют и общие черты.

В отличие от *Windows* большинство объектов разграничения доступа представлено в *Linux* в виде файлов. Т. о. разграничение доступа к файловой системе является в данной ОС важнейшей задачей системы управления доступом.

Каждый пользователь в системе имеет свой уникальный идентификационный номер (*user ID*, или *UID*). Группы также имеют такой идентификатор, который называется *group ID*, или *GID*.

В свою очередь файлы имеют двух владельцев: пользователя (*user owner*) и группу пользователей (*group owner*). Для каждого файла есть индивидуальные права доступа, которые разбиты на три группы:

1. доступ для пользователя-владельца файла (*owner*);
2. доступ для группы-владельца файла (group);
3. доступ для остальных пользователей (*others*).

Для каждой категории устанавливаются три вида доступа: (*x*) – право на запуск файла, (*r*) – право на чтение файла, (*w*) – право на изменение (редактирование) файла. Т. е. права доступа можно представить в виде битовой строки, в которой каждые 3 бита определяют права доступа для соответствующей категории пользователей. Эти биты отвечают за право на чтение, запись и исполнение файла или каталога. Если бит установлен в 1 – операция разрешена, если в 0 – запрещена. Т. о. права доступа к файлу или каталогу описываются тремя восьмеричными цифрами, самая левая из которых – права доступа владельца, средняя – права группы, правая – права доступа для всех остальных.

Право на чтение файла позволяет пользователю читать содержимое файла. Для каталога установка права на чтение позволяет читать файлы, находящиеся в этом каталоге.

Право на запись файла позволяет пользователю изменять его содержимое. Для каталога – создавать файлы внутри каталога.

Право на выполнение для файла позволяет запускать файл на выполнение в качестве программы. Для каталога установка этого права дает возможность пользователю входить в каталог и просматривать его содержимое.

Помимо прав доступа существуют так называемые модификаторы доступа. К наиболее используемым модификаторам доступа относятся *SUID* и *SGID*.

3.2 *Suid* и *Sgid*

Если файлу установлен модификатор доступа *SUID* и файл исполняемый, то файл при запуске на выполнение получает не права пользователя, запустившего его, а права владельца файла. Такие приемы используются для того, чтобы пользователь мог работать с некоторыми системными файлами, владельцем которых является привилегированный пользователь. К примеру, для того, чтобы пользователь мог самостоятельно изменить свой пароль при помощи программы *passwd*, у этой программы, владельцем которой является пользователь *root*, должен быть установлен бит *SUID*, поскольку она работает с файлом *shadow*, модификацию которого имеет право производить только пользователь *root*.

Если файл имеет модификатор доступа *SGID*, то это аналогично установке бита *SUID*, только вместо владельца файла используется группа, которой принадлежит файл. В случае установки *SGID* для каталога файлы, содержащиеся в этом каталоге, будут иметь установки группы такие же, как у каталога.

Модификаторы доступа при правильном использовании представляют очень мощное и гибкое средство. С другой стороны, неправильная настройка системы с использованием этих модификаторов может свести все действия по обеспечению безопасности к нулю. Особенно опасной представляется ситуация, когда тот же *SUID* установлен на исполняемый файл, принадлежащий привилегированному пользователю. При выполнении файла запустивший его пользователь получает право выполнять операции, доступные только пользователю *root*. Если даже файл не выполняет никаких системных операций и не работает с системными файлами, неправильное его использование может привести к очень неприятным последствиям.

Управление доступом к файловой системе возможно также с использованием *ACL*, подобно управлению в *Windows*. Однако для этого придется смонтировать файловую систему с определенными параметрами и установить дополнительные компоненты ОС.

4. ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ДОСТУПОМ К ОБЪЕКТАМ В *WINDOWS*

Управление доступом пользователей к локальной файловой системе можно осуществлять следующими способами:

1. закладка «Безопасность» в диалоговом окне свойств папки или файла;
2. командная строка (*CACLS*).

Управление доступом пользователей к реестру можно осуществлять через стандартную утилиту *Regedit*.

Управление доступом пользователей к общим (сетевым) ресурсам можно осуществлять следующими способами:

1. оснастка Общие папки (*fsmgmt.msc*);
2. оснастка Управление компьютером (*compmgmt.msc*);
3. закладка «Доступ» в диалоговом окне свойств файла или папки;
4. командная строка (*NET FILE, NET SHARE, NET SESSION*).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Национальный открытый университет «Интуит» [Электронный ресурс] – Режим доступа: https://intuit.ru/studies/courses/1089/217/lecture/5609 – Дата доступа: 18.04.2021.

2. Разработка системы управления доступом для ОС семейства *Windows* / Д.М. Бречка, А.А. Литвиненко / Омский государственный университет им. Ф.М. Достоевского, 2017 – с. 131-140.