

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ  
УНИВЕРСИТЕТ им. Н.Э. БАУМАНА

Факультет «Информатика и системы управления»

Кафедра «Автоматизированные системы обработки информации и управления»



**Сёмкин П.С., Сёмкин А.П.**

Методические материалы к лабораторным работам  
по дисциплине  
«Операционные системы»

Лабораторная работа № 4  
«ОС Ubuntu. Расширенные права доступа  
к файлам и каталогам»

**Москва**

**2022 г.**

## ОГЛАВЛЕНИЕ

<b>1 ЦЕЛЬ РАБОТЫ .....</b>	<b>4</b>
<b>2 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ.....</b>	<b>4</b>
<b>2.1 Использования расширенных разрешений.....</b>	<b>4</b>
2.1.1 Разрешение для файла на установку идентификатора пользователя (setuid) .....	4
2.1.2 Разрешение на установку идентификатора группы(setgid) .....	4
2.1.3 Разрешение на защиту файла от случайного удаления (sticky bit) .....	5
2.1.4 Установка битов расширенных разрешений.....	5
<b>2.2 Использование списков контроля доступа ACL .....</b>	<b>7</b>
2.2.1 Понятие ACL .....	7
2.2.2 Изменение и просмотр настроек ACL .....	7
2.2.3 Работа с ACL по умолчанию.....	8
<b>3 ВЫПОЛНЕНИЕ РАБОТЫ.....</b>	<b>9</b>
<b>3.1 Задание.....</b>	<b>9</b>
<b>3.2 Порядок выполнения работы .....</b>	<b>9</b>
3.2.1 Создание каталога с общим доступом(shared).....	9
3.2.2 Управление расширенными правами доступа к файлам и каталогам с использованием ACL .....	10
<b>3.3 Ответить на контрольные вопросы.....</b>	<b>11</b>
<b>4 КОНТРОЛЬНЫЕ ВОПРОСЫ .....</b>	<b>11</b>
<b>5 ЛИТЕРАТУРА.....</b>	<b>11</b>
<b>6 ПРИЛОЖЕНИЕ.....</b>	<b>12</b>
<b>6.1 Команды Ubuntu для работы с пользователями .....</b>	<b>12</b>
6.1.1 Создание нового пользователя .....	12
<b>6.2 Команды Ubuntu для работы с группами пользователей .....</b>	<b>12</b>
6.2.1 Создание группы пользователей .....	12
6.2.2 Добавление учётной записи пользователя в группу .....	12
<b>6.3 Команды Ubuntu для работы с файлами и каталогами .....</b>	<b>12</b>
6.3.1 Создание каталога .....	12
6.3.2 Смена владельца каталога .....	12
6.3.3 Смена группы владельцев каталога со всеми вложенными каталогами и файлами .....	12
6.3.4 Установка возможности создавать файлы в каталоге для членов группы	13
6.3.5 Установка принадлежности файлов группе пользователей .....	13
6.3.6 Установка возможности для пользователей удалять из каталога только принадлежащие им файлы.....	13

6.3.7	Создание файлов .....	13
6.4	<b>Управление расширенными правами доступа к файлам и каталогам с использованием ACL .....</b>	<b>13</b>
6.4.1	Проверка текущих прав доступа к каталогу .....	13
6.4.2	Установка прав доступа к каталогу.....	14

## 1 Цель работы

Целью работы является знакомство с расширенными правами доступа к файлам и каталогам ОС Ubuntu

## 2 Теоретическая часть

### 2.1 *Использования расширенных разрешений*

Помимо основных разрешений (рассмотренных в лабораторной работе №3), в файловых системах ОС Ubuntu есть набор расширенных разрешений. Биты таких разрешения устанавливаются по умолчанию и могут быть при необходимости настроены пользователем.

#### 2.1.1 **Разрешение для файла на установку идентификатора пользователя (setuid)**

**set user ID upon execution** - «установка ID пользователя во время выполнения»

Когда для файла установлен атрибут **setuid**, то пользователь, запускающий этот файл на исполнение, получает повышение прав до пользователя-владельца файла (обычно **root**) в рамках запущенного процесса. После получения повышенных прав процесс может выполнять задачи, выполнение которых обычному пользователю недоступно.

Использование **setuid** может быть потенциально опасно, т.к. может предоставлять права доступа **root**.

*В некоторых файлах операционная система устанавливает данный бит по умолчанию.*

#### 2.1.2 **Разрешение на установку идентификатора группы(setgid)**

**set group ID upon execution** — «установка ID группы во время выполнения».

При применении к исполняемому файлу, данный бит дает пользователю, который исполняет файл, разрешения владельца группы этого файла. Таким образом, **setgid** в этом случае выполняет то же самое, что и **setuid**.

*Как и в случае с разрешением **setuid**, **setgid** применяется к некоторым системным файлам в качестве настройки по умолчанию.*

Когда **setgid** применяется к каталогу, его можно использовать для установки владельца группы по умолчанию для файлов и подкаталогов, созданных в этом каталоге. *По умолчанию, когда пользователь создает файл, его эффективная первичная группа устанавливается как владелец группы для этого файла.*

Разрешение **setgid** является очень полезным разрешением для установки в каталогах общих групп.

### 2.1.3 Разрешение на защиту файла от случайного удаления (**sticky bit**)

Это разрешение полезно для защиты файлов от случайного удаления, если несколько пользователей имеют права на запись в один и тот же каталог. Если применяется закрепленный **sticky bit**, пользователь может удалить файл, только если он является пользователем-владельцем файла или каталога, в котором содержится файл. По этой причине он применяется в качестве разрешения по умолчанию для каталога **/tmp** и может быть полезен также для каталогов общих групп.

При использовании **sticky bit**, пользователь может удалять файлы, только если выполняется одно из следующих условий:

- Пользователь является владельцем файла;
- Пользователь является владельцем каталога, в котором находится файл.

### 2.1.4 Установка битов расширенных разрешений

Чтобы установить биты разрешений **setuid**, **setgid** и **sticky bit**, можно использовать команду **chmod**.

При этом

**setuid** имеет числовое значение **4**,

**setgid** имеет числовое значение **2**,

**sticky bit** имеет числовое значение **1**.

Для задания расширенных разрешений могут быть использованы **абсолютный и относительный режимы**.

В первом случае команде **chmod** необходимо задание всех устанавливаемых прав, причём первая цифра относится к расширенным разрешениям.

Следующая команда, добавит разрешение **setgid** на каталог и установит **gwx** для пользователя и **gx** для группы и других:

**chmod 2755 /userdir**

В **относительном режиме** можно применить только какое-либо из расширенных разрешений:

1. Для **setuid** **chmod u+s**
2. Для **setgid** **chmod g+s**
3. Для **sticky bit** **chmod +t**

Права доступа	Восьмеричное представление	Символьное представление	Действие
<b>setuid</b>	<b>4</b>	<b>u+s</b>	Пользователь выполняет файл с разрешениями владельца файла
<b>setgid</b>	<b>2</b>	<b>g+s</b>	Пользователь выполняет файл с разрешениями владельца группы
<b>sticky bit</b>	<b>1</b>	<b>+t</b>	

**Таблица. Способы представления расширенных прав доступа**

Найти все файлы, у которых установлены биты **setuid** и **setgid** можно с помощью команд:

**find / -perm -u+s**

**find / -perm -g+s**

## 2.2 Использование списков контроля доступа ACL

### 2.2.1 Понятие ACL

Списки контроля доступа к файловой системе (ACL Access Control List) предоставляет расширенный и более гибкий механизм распределения прав файловых систем. Они предназначены для расширения прав доступа к файлам и позволяют устанавливать разрешения любым пользователям или группам пользователей для различных файлов и каталогов

Кроме того, списки ACL позволяют администраторам устанавливать разрешения по умолчанию сложным способом, при котором установленные разрешения могут различаться в разных каталогах.

### 2.2.2 Изменение и просмотр настроек ACL

Если нужно, чтобы создаваемые в некотором каталоге файлы принадлежали к какой-то группе и имели определенные права доступа, то для этого следует определить параметры ACL для каталога.

Чтобы увидеть текущие настройки ACL, необходима команда **getfacl**.

Команда **ls -l** не показывает никаких существующих ACL; он просто показывает + после списка разрешений, который указывает, что списки ACL применяются и к файлу.

Перед настройкой списков ACL всегда полезно показать текущие настройки ACL с помощью **getfacl**.

В результате выполнения команды **getfacl** разрешения показаны для трех разных объектов: пользователя, группы и других.

Для установки ACL используется команда **setfacl**.

#### Примеры использования

- **setfacl -m g:test:rx /dir.**
  - m -указывает, что текущие настройки ACL необходимо изменить.
  - g:test:rx -установить ACL для каталога /dir для чтения и выполнения (rx) для группы (g) test
- **setfacl -m u:student:rwx /dir**
  - m -указывает, что текущие настройки ACL необходимо изменить.

**u:student:rwX** -дает разрешения пользователю student в каталоге **/dir**, не делая его владельцем и не изменяя назначение текущего владельца.

Команда **setfacl** имеет много возможностей и опций.

Если используется параметр **-R**, то происходит настройка ACL для всех файлов и подкаталогов, которые в настоящее время существуют в каталоге, где устанавливается ACL. **Рекомендуется всегда использовать эту опцию при изменении списков ACL для существующих каталогов.**

### 2.2.3 Работа с ACL по умолчанию

Одним из преимуществ использования списков ACL является то, что можно давать разрешения нескольким пользователям или группам в каталоге. Еще одним преимуществом является то, что можно включить наследование, работая с ACL по умолчанию.

Установив ACL по умолчанию, определяют разрешения, которые будут установлены для всех новых элементов, создаваемых в каталоге. ACL по умолчанию не меняет разрешения для существующих файлов и подкаталогов. Чтобы изменить их, нужно добавить и обычный ACL.

Чтобы установить ACL по умолчанию, просто нужно добавить опцию **d** после опции **-m** (порядок имеет значение!). Надо использовать **setfacl -m d:g:test:rx /data**, чтобы группа **test** имела доступ на чтение и выполнение всего, что когда-либо будет создано в каталоге **/data**.

Чтобы использовать ACL для настройки доступа нескольких пользователей или групп к одному и тому же каталогу, необходимо установить ACL дважды. Сначала необходимо выполнить **setfacl -R -m**, чтобы изменить ACL для текущих файлов. Затем выполнить **setfacl -m d:**, чтобы позаботиться обо всех новых элементах, которые также будут созданы.

ACL и обычные разрешения не всегда хорошо интегрированы. Проблемы могут возникнуть, если применили ACL по умолчанию к каталогу, после чего элементы были добавлены в этот каталог, и затем попытались изменить обычные разрешения.



Изменения, которые применяются к обычным разрешениям, не будут хорошо отражены в обзоре ACL. Чтобы избежать проблем, сначала надо установить обычные разрешения, после чего установить ACL по умолчанию.

### 3 Выполнение работы

#### 3.1 Задание.

1. Создать каталог с общим доступом(shared) **ДЕКАНАТ** и обеспечить доступ к данному каталогу группы пользователей, используя расширенные разрешения (биты `setgid` и `sticky`).

2. Обеспечить разграничение доступа пользователей группы **group\_dek** к подкаталогам каталога **ДЕКАНАТ**, используя **ACL**.

#### 3.2 Порядок выполнения работы

1. Войти в систему под учётной записью **stud\_XX** (XX –индекс группы).
2. Запустить программу виртуализации **Oracle VM VirtualBox**.
3. Запустить виртуальную машину **Ubuntu**.
4. Войти под учётной записью **admin\_kaf**

##### 3.2.1 Создание каталога с общим доступом(shared).

1. Создать с использованием утилиты **adduser** учётные записи пользователей **dekan**, **sotrudnik**, **admin\_dek** (пароль **dekanat**)

2. Создать группу пользователей **group\_dek** и включить в неё пользователей **dekan**, **sotrudnik**, **admin\_dek** (включить пользователей также в группу **sudo**)

3. Войти в систему под учётной записью **admin\_dek**

4. Создать в корневом каталоге / файловой системы каталог **ДЕКАНАТ**, который будет принадлежать группе пользователей **group\_dek**.

5. Сменить владельца каталога **ДЕКАНАТ** на **admin\_dek**

6. Сменить группу владельцев каталога **ДЕКАНАТ** на группу **group\_dek** (со всеми вложенными каталогами и файлами)

7. Установить, что члены группы пользователей **group\_dek** должны иметь возможность создавать файлы в каталоге **ДЕКАНАТ**.

8. Установить, что все файлы, созданные в каталоге **ДЕКАНАТ**, должны принадлежать группе пользователей **group\_dek**.

9. Установить, что пользователи должны иметь возможность удалять из каталога **ДЕКАНАТ** только принадлежащие им файлы.

10. Создать в каталоге **ДЕКАНАТ** каталоги

## **ПРИКАЗЫ и ИНФОРМАЦИЯ**

11. Проверить корректность созданных каталогов.

12. Войти в систему с использованием учетных записей пользователей, состоящих в группе **group\_dek**, создать файлы и получить информацию о правах доступа к ним:

- Для пользователя **dekan**:

создать файл / **ДЕКАНАТ** / **ПРИКАЗЫ** / **Приказ061121.txt**

- Для Пользователя **sotrudnik**

создать файл / **ДЕКАНАТ** / **ИНФОРМАЦИЯ** / **Новости.txt**

### **3.2.2 Управление расширенными правами доступа к файлам и каталогам с использованием ACL**

Необходимо обеспечить разграничение доступа пользователей группы **group\_dek** к подкаталогам каталога **ДЕКАНАТ**.

1. Войти в систему под учётной записью **admin\_dek**

2. Проверить, используя команду **getfacl**, текущие права доступа к каталогу

## **ПРИКАЗЫ**

3. Установить, используя команду **setfacl**, права доступа к каталогу **ПРИКАЗЫ** для пользователей **dekan** (полный доступ) , и **sotrudnik** (только чтение)
4. Проверить текущие права доступа к каталогу **ПРИКАЗЫ**
5. Проверить текущие права доступа к каталогу **ИНФОРМАЦИЯ**
6. Установить права доступа к каталогу **ИНФОРМАЦИЯ** для пользователей **sotrudnik** (полный доступ) , и **dekan** (только чтение)
7. Проверить текущие права доступа к каталогу **ИНФОРМАЦИЯ**

### 3.3 Ответить на контрольные вопросы.

## 4 Контрольные вопросы

1. Каково назначение расширенных разрешений **setuid**, **setgid** и **sticky bit**?
2. В чём отличие задания расширенных разрешений в абсолютном и относительном режимах?
3. Как назначаются права при использовании **ACL**?

## 5 ЛИТЕРАТУРА

1. Сёмкин П.С., Аксёнов А.Н. Файловые системы. Логическая организация и физическая реализация. Сборник учебно-методических работ кафедры «Системы обработки информации и управления» (бакалавры). Учебное пособие. Вып. 1./Под ред: В.М. Черненко. –М: «АртКом», 2013. – стр. 95-120
2. Сёмкин П.С., Семкин А.П. Файловые системы операционных систем **Windows** и **Unix**. Сборник учебно-методических работ кафедры «Системы обработки информации и управления» (бакалавры). Учебное пособие. Вып. 2./Под ред. В.М. Чёрненко. –М: «АртКом», 2014. – стр. 160-189
3. Негус К. **Ubuntu** и **Debian Linux** для продвинутых. 2-е изд. – СПб.: Питер, 2014. -384 с.: ил.

## 6 Приложение

### 6.1 Команды Ubuntu для работы с пользователями

#### 6.1.1 Создание нового пользователя

- Утилита **adduser**
  - **sudo adduser dekan**
  - **sudo adduser sotrudnik**
  - **sudo adduser admin\_dek**

### 6.2 Команды Ubuntu для работы с группами пользователей

#### 6.2.1 Создание группы пользователей

**\$ sudo groupadd dekanat**

#### 6.2.2 Добавление учётной записи пользователя в группу

**\$sudo usermod** опции **имя\_группы** **имя\_пользователя**

**-a** – добавить пользователя в новую группу (используется с опцией **G**)

**-g** – назначить главной группой

**G** – назначить вторичной группой

**sudo usermod -a -G dekanat,sudo dekan**

**sudo usermod -a -G dekanat,sudo sotrudnik**

**sudo usermod -a -G dekanat,sudo admin\_dek**

### 6.3 Команды Ubuntu для работы с файлами и каталогами

#### 6.3.1 Создание каталога

**\$ sudo mkdir** <имя каталога> - создание каталога

**\$sudo mkdir -p / ДЕКАНАТ**

#### 6.3.2 Смена владельца каталога

**sudo chown admin\_dek:group\_dek / ДЕКАНАТ**

#### 6.3.3 Смена группы владельцев каталога со всеми вложенными каталогами и файлами

**sudo chgrp -R group\_dek / ДЕКАНАТ**

### 6.3.4 Установка возможности создавать файлы в каталоге для членов группы

Установить, что члены группы пользователей **group\_dek** должны иметь возможность создавать файлы в каталоге **ДЕКАНАТ**.

```
sudo chmod -R 770 / ДЕКАНАТ
```

### 6.3.5 Установка принадлежности файлов группе пользователей

Установить, что все файлы, созданные в каталоге **ДЕКАНАТ**, должны принадлежать группе пользователей **group\_dek**.

```
sudo chmod -R 2770 /ДЕКАНАТ
```

*2 –означает, что включён бит **setgid** и создаваемые файлы наследуют ту же группу, что и каталог, а вновь создаваемые вложенные каталоги будут наследовать **setgid** родительского*

*В листинге **ls -la** в разрешениях групп будет **rws***

### 6.3.6 Установка возможности для пользователей удалять из каталога только принадлежащие им файлы

Установить, что пользователи должны иметь возможность удалять из каталога **ДЕКАНАТ** только принадлежащие им файлы.

```
chmod +t / ДЕКАНАТ
```

В листинге **ls -la** в разрешениях прочих будет **--T**

### 6.3.7 Создание файлов

```
touch / ДЕКАНАТ / ПРИКАЗЫ /Приказ061121.txt
```

## 6.4 Управление расширенными правами доступа к файлам и каталогам с использованием **ACL**

### 6.4.1 Проверка текущих прав доступа к каталогу

```
getfacl / ДЕКАНАТ / ПРИКАЗЫ
```

## 6.4.2 Установка прав доступа к каталогу

**setfacl -m u:dekan:rwx, u:sotrudnik:r-- / ДЕКАНАТ / ПРИКАЗЫ**

**setfacl -m u:sotrudnik:rwx, u:dekan:r-- / ДЕКАНАТ / ИНФОРМАЦИЯ**