

# **Основы информационной безопасности**

**Лабораторная работа № 2. Дискреционное разграничение прав в Linux.  
Основные атрибуты**

Демидова Екатерина Алексеевна

# Содержание

1	Цель работы	4
2	Теоретические сведения	5
3	Выполнение лабораторной работы	6
4	Выводы	13
	Список литературы	14

## Список иллюстраций

3.1	Создание нового пользователя guest . . . . .	6
3.2	Просмотр информации о пользователе . . . . .	7
3.3	Просмотр существующих в системе директорий . . . . .	7
3.4	Изменение прав доступа к директории . . . . .	8

# 1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

## 2 Теоретические сведения

При работе с командой `chmod` важно понимать основные права доступа, которые назначают файлам или каталогам. В Linux используется три основных типа прав доступа[1]:

- Чтение (Read) — обозначается буквой «r». Предоставляет возможность просматривать содержимое файла или каталога.
- Запись (Write) — обозначается буквой «w». Позволяет создавать, изменять и удалять файлы внутри каталога, а также изменять содержимое файла.
- Выполнение (Execute) — обозначается буквой «x». Дает разрешение на выполнение файла или на вход в каталог.

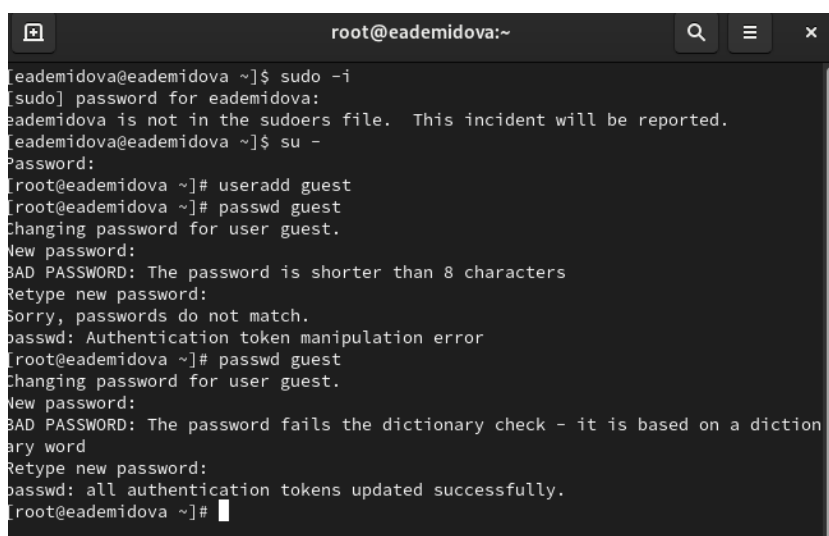
Каждый из указанных выше типов прав доступа может быть назначен трем группам пользователей:

- Владелец (Owner) — пользователь, который является владельцем файла или каталога.
- Группа (Group) — группа пользователей, к которой принадлежит файл или каталог.
- Остальные пользователи (Others) — все остальные пользователи системы.

Комбинация этих базовых прав доступа для каждой из групп пользователей определяет полный набор прав доступа для файла или каталога.

### 3 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы ОС создадим учетную запись пользователя guest(рис. 3.1)

A terminal window titled 'root@eademidova:~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

```
[eademidova@eademidova ~]$ sudo -i
[sudo] password for eademidova:
eademidova is not in the sudoers file. This incident will be reported.
[eademidova@eademidova ~]$ su -
Password:
[root@eademidova ~]# useradd guest
[root@eademidova ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@eademidova ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@eademidova ~]#
```

Рис. 3.1: Создание нового пользователя guest

Войдем в систему от имени пользователя guest. Определим директорию, в которой мы находимся, командой `pwd`. Сравнив её с приглашением командной строки, увидим, что она называется как наш пользователь. Она является домашней директорией. Также уточним имя нашего пользователя командой `whoami`. С помощью команды `id` также увидим имя пользователя и его `id 1001`, а кроме того, что он входит в группу `guest` с `id 1001`. Сравнивая вывод `id` с выводом команды `groups`, можно увидеть, что действительно наш пользователь входит только в одну группу(в этом случае указывается только ее название). Посмотрим файл

/etc/passwd командой `cat /etc/passwd` и увидим, что `uid` и `gid` пользователя равен 1001, что также было видно из предыдущих выводов команд(рис. 3.2).

```
[guest@eademidova ~]$ pwd
/home/guest
[guest@eademidova ~]$ cd
[guest@eademidova ~]$ pwd
/home/guest
[guest@eademidova ~]$ whoami
guest
[guest@eademidova ~]$ ud
bash: ud: command not found...
Similar command is: 'du'
[guest@eademidova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023
[guest@eademidova ~]$ groups
guest
[guest@eademidova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@eademidova ~]$
```

Рис. 3.2: Просмотр информации о пользователе

Определим существующие в системе директории командой `ls -l /home/` – это `guest` и `eademidova`, правами на чтение, запись и изменение директорий владеет только их владелец. Также с помощью команды `lsattr` увидим, что для нашей домашней директории не установлены расширенные атрибуты, а для других пользователей мы не можем это увидеть(рис. 3.3)

```
[guest@eademidova ~]$ ls -l /home/
total 8
drwx----- 14 eademidova eademidova 4096 Jun 28 16:51 eademidova
drwx----- 14 guest      guest      4096 Jun 30 18:25 guest
[guest@eademidova ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/eademidova
----- /home/guest
[guest@eademidova ~]$
```

Рис. 3.3: Просмотр существующих в системе директорий

Создадим в домашней директории поддиректорию `dir1` командой `mkdir dir1`, с помощью команд `ls -l` и `lsattr` увидим, что для владельца этой директории есть все права, а для группы и остальных доступно только чтение и вход(не доступно внесение изменений), также видно, что никаких расширенных атрибутов не установлено. Затем снимем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверим выполнение с помощью команды `ls -l`. Также попытаемся создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`, но так как мы забрали право на запись в эту директорию, то получим отказ в создании. А введя команду `ls -l /home/guest/dir1` увидим, что просмотр директории также запрещен(рис. 3.4).

```

[guest@eademidova ~]$ mkdir dir1
[guest@eademidova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Desktop
drwxr-xr-x. 2 guest guest 6 Jun 30 18:43 dir1
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Documents
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Downloads
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Music
drwxr-xr-x. 2 guest guest 53 Jun 30 18:41 Pictures
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Public
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Templates
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Videos
[guest@eademidova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@eademidova ~]$ chmod 000 dir1
[guest@eademidova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Desktop
d------. 2 guest guest 6 Jun 30 18:43 dir1
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Documents
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Downloads
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Music
drwxr-xr-x. 2 guest guest 53 Jun 30 18:41 Pictures
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Public
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Templates
drwxr-xr-x. 2 guest guest 6 Jun 30 18:25 Videos
[guest@eademidova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@eademidova ~]$ ls -l /home/guest/dir1/
ls: cannot open directory '/home/guest/dir1/': Permission denied

```

Рис. 3.4: Изменение прав доступа к директории

В табл. [3.1] приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Таблица 3.1: Установленные права и разрешённые действия

Права директории	Права файла	Права и действия							
		Сме- на	Про- смот	Пе- ре-	Сме- на	Уда- ле-	За- пись	Чте- ние	Сме- на
		фай-	фай-	фай-	фай-	фай-	фай-	фай-	фай-
		ла	ла	ла	ла	ла	ла	ла	ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+



Права директории	Права файла	<div> <div>Про- Пе- Сме-</div> <div>смотр ре- на</div> <div>Сме- фай- име- ат-</div> <div>на лов в но- ри-</div> <div>ди- ди- ва- бу-</div> <div>рек- рек- ние тов</div> </div>							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	ди- рек- то- рии	фай- ла	фай- ла
d(400)	(000)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(000)	(100)	-	-	-	-	-	-	-	-
d(100)	(100)	-	-	-	-	+	-	-	+
d(200)	(100)	-	-	-	-	-	-	-	-
d(300)	(100)	+	+	-	-	+	-	+	+
d(400)	(100)	-	-	-	-	-	+	-	-
d(500)	(100)	-	-	-	-	+	+	-	+
d(600)	(100)	-	-	-	-	-	+	-	-
d(700)	(100)	+	+	-	-	+	+	+	+
d(000)	(200)	-	-	-	-	-	-	-	-
d(100)	(200)	-	-	+	-	+	-	-	+
d(200)	(200)	-	-	-	-	-	-	-	-
d(300)	(200)	+	+	+	-	+	-	+	+
d(400)	(200)	-	-	-	-	-	+	-	-
d(500)	(200)	-	-	+	-	+	+	-	+
d(600)	(200)	-	-	-	-	-	+	-	-
d(700)	(200)	+	+	+	-	+	+	+	+
d(000)	(300)	-	-	-	-	-	-	-	-

Права директории	Права файла	Про- Пе- Сме- смотр ре- на Сме- фай- име- ат- на лов в но- ри- зда- ле- За- Чте- ди- ди- ва- бу- ние ние пись ние рек- рек- ние тов фай- фай- в фай- то- то- фай- фай- ла ла файл ла рии рии ла ла							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Пе- ре- име- но- ва- ние фай- ла	Сме- на ри- бу- тов фай- ла
d(100)	(300)	-	-	+	-	+	-	-	+
d(200)	(300)	-	-	-	-	-	-	-	-
d(300)	(300)	+	+	+	-	+	-	+	+
d(400)	(300)	-	-	-	-	-	+	-	-
d(500)	(300)	-	-	+	-	+	+	-	+
d(600)	(300)	-	-	-	-	-	+	-	-
d(700)	(300)	+	+	+	-	+	+	+	+
d(000)	(400)	-	-	-	-	-	-	-	-
d(100)	(400)	-	-	-	+	+	-	-	+
d(200)	(400)	-	-	-	-	-	-	-	-
d(300)	(400)	+	+	-	+	+	-	+	+
d(400)	(400)	-	-	-	-	-	+	-	-
d(500)	(400)	-	-	-	+	+	+	-	+
d(600)	(400)	-	-	-	-	-	+	-	-
d(700)	(400)	+	+	-	+	+	+	+	+
d(000)	(500)	-	-	-	-	-	-	-	-
d(100)	(500)	-	-	-	+	+	-	-	+
d(200)	(500)	-	-	-	-	-	-	-	-
d(300)	(500)	+	+	-	+	+	-	+	+
d(400)	(500)	-	-	-	-	-	+	-	-
d(500)	(500)	-	-	-	+	+	+	-	+

Права директории	Права файла	<div> <div>Про- Пе- Сме-</div> <div>смотр ре- на</div> <div>Сме- фай- име- ат-</div> <div>на лов в но- ри-</div> <div>ди- ди- ва- бу-</div> <div>рек- рек- ние тов</div> </div>							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	ди- рек- то- рии	фай- ла	фай- ла
d(600)	(500)	-	-	-	-	-	+	-	-
d(700)	(500)	+	+	-	+	+	+	+	+
d(000)	(600)	-	-	-	-	-	-	-	-
d(100)	(600)	-	-	+	+	+	-	-	+
d(200)	(600)	-	-	-	-	-	-	-	-
d(300)	(600)	+	+	+	+	+	-	+	+
d(400)	(600)	-	-	-	-	-	+	-	-
d(500)	(600)	-	-	+	+	+	+	-	+
d(600)	(600)	-	-	-	-	-	+	-	-
d(700)	(600)	+	+	+	+	+	+	+	+
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(700)	+	+	+	+	+	+	+	+

В табл. [3.2] приведены данные о том, какие минимальные права должны быть для совершения различных действий.

Таблица 3.2: Минимальные права для совершения операций

Операция	Минимальные права на	
	директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

## 4 Выводы

В результате выполнения работы были приобретены практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Список литературы

1. Граннеман С. Linux. Карманный справочник. 2-е изд. Вильямс, 2019. 464 с.