

Лабораторная работа №2

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	21
	Список литературы	22

Список иллюстраций

4.1	Создание пользователя	9
4.2	Переход в домашнюю директорию	9
4.3	Информация о пользователе	10
4.4	uid и gid пользователя	10
4.5	Директории в системе	10
4.6	Расширенные атрибуты на поддиректориях	11
4.7	Права доступа	11
4.8	Расширенные атрибуты	11
4.9	Изменение атрибутов	12
4.10	Создание файла	12
4.11	Переход в директорию	12
4.12	Проверка разрешения операций для директории с правами 100 .	13
4.13	Проверка разрешения операций для директории с правами 200 .	13
4.14	Проверка разрешения операций для директории с правами 300 .	14
4.15	Проверка разрешения операций для директории с правами 400 .	14
4.16	Проверка разрешения операций для директории с правами 500 .	15
4.17	Проверка разрешения операций для директории с правами 600 .	15
4.18	Проверка разрешения операций для директории с правами 700 .	16
4.19	Минимально необходимые права для создания и удаления поддиректория	19

Список таблиц

4.1	Установленные права и разрешённые действия	16
4.2	Минимальные права для совершения операций	20

1 Цель работы

Целью данной лабораторной работы является 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 Задание

- Выполнить лабораторную работу по порядку
- Заполнить таблицу “Установленные права и разрешённые действия”
- Заполнить таблицу “Минимальные права для совершения операций”

3 Теоретическое введение

Дискреционное разграничение прав в Linux: основные атрибуты

В современных операционных системах критически важно обеспечить надежную защиту данных и контроль доступа к ресурсам. Одним из базовых механизмов безопасности в Linux является дискреционное управление доступом (Discretionary Access Control, DAC). Эта модель основана на том, что права доступа к файлам и каталогам определяются их владельцем, который может передавать или ограничивать доступ другим пользователям.

Основным инструментом DAC в Linux является система разрешений файловой системы (file permissions), которая управляет правами на чтение (read), запись (write) и выполнение (execute) для владельца файла, группы пользователей и всех остальных. Помимо классической схемы прав (rwx), Linux поддерживает специальные атрибуты, такие как SUID, SGID и sticky bit, а также списки расширенных прав доступа (ACLs), которые позволяют более гибко управлять доступом.

Хотя дискреционная модель удобна и широко применяется, она имеет уязвимости, связанные с человеческим фактором. Например, владелец файла может случайно предоставить доступ нежелательным пользователям, что создает риск утечки данных. Поэтому в современных системах безопасности Linux дополнительно используются механизмы обязательного контроля доступа (Mandatory Access Control, MAC), такие как SELinux и AppArmor, которые обеспечивают более строгие ограничения на уровне системы.

Таким образом, дискреционное разграничение прав в Linux является фундаментальным механизмом контроля доступа, который обеспечивает гибкость в

управлении ресурсами, но требует внимательной настройки и дополнения более строгими методами защиты.

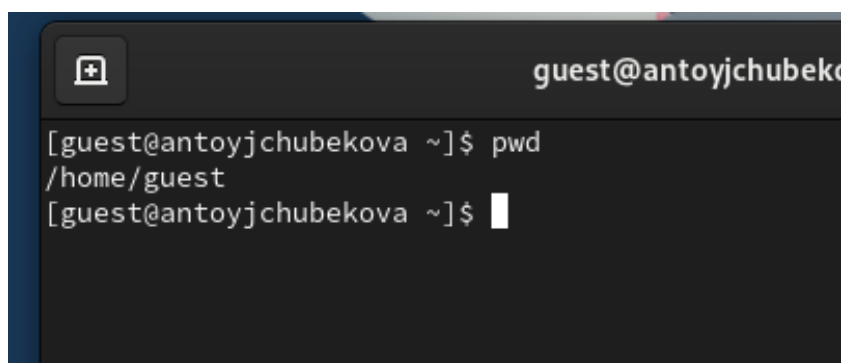
4 Выполнение лабораторной работы

Создаю учетную запись пользователя guest с помощью команды `useradd guest`.
Затем задаю пароль для пользователя guest с командой `passwd guest`. (рис. 4.1).

```
[antoyjchubekova@antoyjchubekova ~]$ sudo -i
[sudo] password for antoyjchubekova:
[root@antoyjchubekova ~]# useradd guest
[root@antoyjchubekova ~]# passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@antoyjchubekova ~]#
```

Рис. 4.1: Создание пользователя

Войдем в систему от имени пользователя guest. С помощью команды `pwd` определим директорию, в которой мы находимся. Мы видим, что мы находимся в домашней директории. (рис. 4.2).



```
guest@antoyjchubekova
[guest@antoyjchubekova ~]$ pwd
/home/guest
[guest@antoyjchubekova ~]$
```

Рис. 4.2: Переход в домашнюю директорию

С помощью команды `whoami` удостоверимся, что наш пользователь guest. Уточним имя пользователя, его группу, а также группы, куда входит пользователь,

командой `id`. Используя команду `groups`, узнаем в какие группы входит пользователь. Мы видим, что пользователь `guest`, входит только в группу `guest`. Полученная информация совпадает с данными, выводимыми в приглашении командной строки. (рис. 4.3).

```
[guest@antoyjchubekova ~]$ whoami
guest
[guest@antoyjchubekova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@antoyjchubekova ~]$ groups
guest
[guest@antoyjchubekova ~]$
```

Рис. 4.3: Информация о пользователе

С помощью команды `cat /etc/passwd | grep guest` выведем информацию об `uid` пользователя и `gid` пользователя. Мы видим, что значения `uid-1001` и `gid-1001` совпадают со значениями вывода команды `id`. (рис. 4.4).

```
[guest@antoyjchubekova ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@antoyjchubekova ~]$
```

Рис. 4.4: `uid` и `gid` пользователя

Определим существующие в системе директории командой `ls -l /home/`. Мы видим, что у нас две директории наших пользователей. (рис. 4.5).

```
[guest@antoyjchubekova ~]$ ls -l /home/
total 8
drwx-----, 14 antoyjchubekova antoyjchubekova 4096 Feb 27 07:35 antoyjchubekova
drwx-----, 14 guest          guest          4096 Feb 27 07:45 guest
[guest@antoyjchubekova ~]$
```

Рис. 4.5: Директории в системе

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Мы видим, что расширенные атрибуты не установлены у нашего пользователя. Для просмотра расширенных атрибутов директории других пользователей, нам было отказано в доступе. (рис. 4.6).

```
[guest@antoyjchubekova ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/antoyjchubekova
----- /home/guest
[guest@antoyjchubekova ~]$
```

Рис. 4.6: Расширенные атрибуты на поддиректориях

Создадим в домашней директории поддиректорий dir1. С помощью команды `ls -l` определим какие права доступа были выставлены на директорию dir1. Мы видим, что установлены полные права для владельца и нулевые права для остальных. (рис. 4.7).

```
[guest@antoyjchubekova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Desktop
drwxr-xr-x. 2 guest guest 6 Feb 27 08:06 dir1
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Documents
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Music
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Public
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Templates
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Videos
[guest@antoyjchubekova ~]$
```

Рис. 4.7: Права доступа

С помощью команды `lsattr` посмотрим расширенные атрибуты директории dir1. (рис. 4.8).

```
[guest@antoyjchubekova ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@antoyjchubekova ~]$
```

Рис. 4.8: Расширенные атрибуты

Снимем с директории dir1 все атрибуты командой `chmod 000 dir1` и проверим

правильность выполнения команды командой `ls -l`. Мы видим, что все выполнилось правильно и теперь владелец, группа, остальные не имеют никаких прав. (рис. 4.9).

```
[guest@antoyjchubekova ~]$ chmod 000 dir1
[guest@antoyjchubekova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Desktop
d----- . 2 guest guest 6 Feb 27 08:06 dir1
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Documents
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Downloads
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Music
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Pictures
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Public
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Templates
drwxr-xr-x. 2 guest guest 6 Feb 27 07:45 Videos
[guest@antoyjchubekova ~]$
```

Рис. 4.9: Изменение атрибутов

Попытаемся создать в директории файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Мы получили отказ в выполнении операции по созданию файла, так как у владельца нет никаких прав, ни на чтение, ни на выполнение, ни на запись. (рис. 4.10). Если мы попытаемся перейти в директорию `dir1` командой `ls -l /home/guest/dir1`, там также будет отказано в доступе, так как у владельца нет права на выполнение. (рис. 4.11).

```
[guest@antoyjchubekova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova ~]$
```

Рис. 4.10: Создание файла

```
[guest@antoyjchubekova ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@antoyjchubekova ~]$
```

Рис. 4.11: Переход в директорию

Теперь заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории, определив опытным путем, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Мы проверим все права gwx владельца для директории и для файла.

Для начала проверим разрешенные операции для директория с правами 100 и файла с правами - 000. Аналогично дальше проверяем для файла с правами - 100,200,300,400,500,600,700. (рис. 4.12).

```
[guest@antoyjchubekova ~]$ cd dir1
[guest@antoyjchubekova dir1]$ chmod 100 file1
[guest@antoyjchubekova dir1]$ touch file2
touch: cannot touch 'file2': Permission denied
[guest@antoyjchubekova dir1]$ rm file1
rm: remove write-protected regular file 'file1'? y
rm: cannot remove 'file1': Permission denied
[guest@antoyjchubekova dir1]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova dir1]$ cat file1
cat: file1: Permission denied
[guest@antoyjchubekova dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest@antoyjchubekova dir1]$ mv file1 file2
mv: cannot move 'file1' to 'file2': Permission denied
[guest@antoyjchubekova dir1]$ sudo chattr +a file1
```

Рис. 4.12: Проверка разрешения операций для директории с правами 100

Проверяем разрешенные операции для директории с правами 200 и файла с правами- 000. Аналогично дальше проверяем для файла с правами - 100,200,300,400,500,600,700. (рис. 4.13).

```
[guest@antoyjchubekova ~]$ chmod 200 dir1
[guest@antoyjchubekova ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@antoyjchubekova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova ~]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest@antoyjchubekova ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest@antoyjchubekova ~]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest@antoyjchubekova ~]$ mv dir1/file1 dir2/fill
mv: cannot stat 'dir1/file1': Permission denied
```

Рис. 4.13: Проверка разрешения операций для директории с правами 200

Проверяем разрешенные операции для директории с правами 300 и файла с правами- 000. Аналогично дальше проверяем для файла с правами - 100,200,300,400,500,600,700. (рис. 4.14).

```

[guest@antoyjchubekova ~]$ chmod 300 dir1
[guest@antoyjchubekova ~]$ cd dir1
[guest@antoyjchubekova dir1]$ chmod 000 file1
[guest@antoyjchubekova dir1]$ touch file2
[guest@antoyjchubekova dir1]$ rm file2
[guest@antoyjchubekova dir1]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova dir1]$ cat file1
cat: file1: Permission denied
[guest@antoyjchubekova dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest@antoyjchubekova dir1]$ mv file1 file2
[guest@antoyjchubekova dir1]$ mv file2 file1

```

Рис. 4.14: Проверка разрешения операций для директории с правами 300

Проверяем разрешенные операции для директории с правами 400 и файла с правами- 000. Аналогично дальше проверяем для файла с правами - 100,200,300,400,500,600,700. (рис. 4.15).

```

[guest@antoyjchubekova ~]$ chmod 400 dir1
[guest@antoyjchubekova ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@antoyjchubekova ~]$ ls dir1
ls: cannot access 'dir1/file1': Permission denied
file1
[guest@antoyjchubekova ~]$ ls dir1
ls: cannot access 'dir1/file1': Permission denied
file1
[guest@antoyjchubekova ~]$ chmod 000 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ chmod 000 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ █

```

Рис. 4.15: Проверка разрешения операций для директории с правами 400

Проверяем разрешенные операции для директории с правами 500 и файла с правами- 000. Аналогично дальше проверяем для файла с правами - 100,200,300,400,500,600,700. (рис. 4.16).

```

[guest@antoyjchubekova ~]$ chmod 500 dir1
[guest@antoyjchubekova ~]$ cd dir1
[guest@antoyjchubekova dir1]$ chmod 000 file1
chmod: cannot access 'file1': No such file or directory
[guest@antoyjchubekova dir1]$ chmod 000 file1
[guest@antoyjchubekova dir1]$ touch file2
touch: cannot touch 'file2': Permission denied
[guest@antoyjchubekova dir1]$ rm file1
rm: remove write-protected regular file 'file1'? y
rm: cannot remove 'file1': Permission denied
[guest@antoyjchubekova dir1]$
[guest@antoyjchubekova dir1]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova dir1]$ cat file1
cat: file1: Permission denied
[guest@antoyjchubekova dir1]$ ls
file1
[guest@antoyjchubekova dir1]$ mv file1 file2
mv: cannot move 'file1' to 'file2': Permission denied
[guest@antoyjchubekova dir1]$

```

Рис. 4.16: Проверка разрешения операций для директории с правами 500

Проверяем разрешенные операции для директории с правами 600 и файла с правами- 000. Аналогично дальше проверяем для файла с правами - 100,200,300,400,500,600,700. (рис. 4.17).

```

[guest@antoyjchubekova ~]$ chmod 600 dir1
[guest@antoyjchubekova ~]$ chmod 000 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest@antoyjchubekova ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova ~]$ cat /home/guest/dir1/file1
cat: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova ~]$ cd dir1
bash: cd: dir1: Permission denied
[guest@antoyjchubekova ~]$ ls ^C
[guest@antoyjchubekova ~]$ ls /home/guest/dir1/
ls: cannot access '/home/guest/dir1/file1': Permission denied
file1
[guest@antoyjchubekova ~]$ mv /home/guest/dir1/file1 home/guest/dir1/file2
mv: cannot stat '/home/guest/dir1/file1': Permission denied
[guest@antoyjchubekova ~]$ ~

```

Рис. 4.17: Проверка разрешения операций для директории с правами 600

Проверяем разрешенные операции для директории с правами 700 и файла с правами- 000. Аналогично дальше проверяем для файла с правами - 100,200,300,400,500,600,700. (рис. 4.18).

```

[guest@antoyjchubekova ~]$ chmod 700 dir1
[guest@antoyjchubekova ~]$ cd dir1
[guest@antoyjchubekova dir1]$ chmod 000 file1
[guest@antoyjchubekova dir1]$ touch file2
[guest@antoyjchubekova dir1]$ rm file2
[guest@antoyjchubekova dir1]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@antoyjchubekova dir1]$ cat file1
cat: file1: Permission denied
[guest@antoyjchubekova dir1]$ ls
file1
[guest@antoyjchubekova dir1]$ mv file1 file2
[guest@antoyjchubekova dir1]$ mv file2 file1

```

Рис. 4.18: Проверка разрешения операций для директории с правами 700

Исходя из этих результатов заполним таблицу “Установленные права и разрешённые действия” 4.1

Таблица 4.1: Установленные права и разрешённые действия

	Права	Со-зда-ние	Уда-ле-ние	За-пись	Чте-ние	Сме-на	Про-смотр	Пере-име-нова-ние	Смена атрибу-тов
Правы дирек-тории	фай-ла	фай-ла	фай-ла	файл	фай-ла	рек-тории	в дирек-тории	файла	файла
000	000	-	-	-	-	-	-	-	-
000	100	-	-	-	-	-	-	-	-
000	200	-	-	-	-	-	-	-	-
000	300	-	-	-	-	-	-	-	-
000	400	-	-	-	-	-	-	-	-
000	500	-	-	-	-	-	-	-	-
000	600	-	-	-	-	-	-	-	-
000	700	-	-	-	-	-	-	-	-
100	000	-	-	-	-	+	-	-	+
100	100	-	-	-	-	+	-	-	+
100	200	-	-	+	-	+	-	-	+
100	300	-	-	+	-	+	-	-	+

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- тории	Про- смотр файлов в дирек- тории	Пере- име- нова- ние файла	Смена атрибу- тов файла
100	400	-	-	-	+	+	-	-	+
100	500	-	-	-	+	+	-	-	+
100	600	-	-	+	+	+	-	-	+
100	700	-	-	+	+	+	-	-	+
200	000	-	-	-	-	-	-	-	-
200	100	-	-	-	-	-	-	-	-
200	200	-	-	-	-	-	-	-	-
200	300	-	-	-	-	-	-	-	-
200	400	-	-	-	-	-	-	-	-
200	500	-	-	-	-	-	-	-	-
200	600	-	-	-	-	-	-	-	-
200	700	-	-	-	-	-	-	-	-
300	000	+	+	-	-	+	-	+	+
300	100	+	+	-	-	+	-	+	+
300	200	+	+	+	-	+	-	+	+
300	300	+	+	+	-	+	-	+	+
300	400	+	+	-	+	+	-	+	+
300	500	+	+	-	+	+	-	+	+
300	600	+	+	+	+	+	-	+	+
300	700	+	+	+	+	+	-	+	+
400	000	-	-	-	-	-	+	-	-
400	100	-	-	-	-	-	+	-	-
400	200	-	-	-	-	-	+	-	-
400	300	-	-	-	-	-	+	-	-

Права дирек- тории	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- тории	Про- смотр файлов в дирек- тории	Пере- име- нова- ние файла	Смена атрибу- тов файла
400	400	-	-	-	-	-	+	-	-
400	500	-	-	-	-	-	+	-	-
400	600	-	-	-	-	-	+	-	-
400	700	-	-	-	-	-	+	-	-
500	000	-	-	-	-	+	+	-	+
500	100	-	-	-	-	+	+	-	+
500	200	-	-	+	-	+	+	-	+
500	300	-	-	+	-	+	+	-	+
500	400	-	-	-	+	+	+	-	+
500	500	-	-	-	+	+	+	-	+
500	600	-	-	+	+	+	+	-	+
500	700	-	-	+	+	+	+	-	+
600	000	-	-	-	-	-	+	-	-
600	100	-	-	-	-	-	+	-	-
600	200	-	-	-	-	-	+	-	-
600	300	-	-	-	-	-	+	-	-
600	400	-	-	-	-	-	+	-	-
600	500	-	-	-	-	-	+	-	-
600	600	-	-	-	-	-	+	-	-
600	700	-	-	-	-	-	+	-	-
700	000	+	+	-	-	+	+	+	+
700	100	+	+	-	-	+	+	+	+
700	200	+	+	+	-	+	+	+	+
700	300	+	+	+	-	+	+	+	+

	Права	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	Сме- на	Про- смотр	Пере- име- нова-	Смена
Права дирек- тории	фай- ла	фай- ла	фай- ла	в файл	фай- ла	рек- тории	файлов в дирек- тории	ние файла	атрибу- тов файла
700	400	+	+	-	+	+	+	+	+
700	500	+	+	-	+	+	+	+	+
700	600	+	+	+	+	+	+	+	+
700	700	+	+	+	+	+	+	+	+

Далее на основе заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1. Опишем это в таблице “Минимальные права для совершения операций” 4.2 Для того чтобы узнать минимально необходимые права для создания и удаления поддиректория, сделаем некоторые действия. (рис. 4.19).

```
[guest@antoyjchubekova ~]$ chmod 000 dir1
[guest@antoyjchubekova ~]$ mkdir dir1/dir2
mkdir: cannot create directory 'dir1/dir2': Permission denied
[guest@antoyjchubekova ~]$ chmod 100 dir1
[guest@antoyjchubekova ~]$ mkdir dir1/dir2
mkdir: cannot create directory 'dir1/dir2': Permission denied
[guest@antoyjchubekova ~]$ chmod 200 dir1
[guest@antoyjchubekova ~]$ mkdir dir1/dir2
mkdir: cannot create directory 'dir1/dir2': Permission denied
[guest@antoyjchubekova ~]$ chmod 300 dir1
[guest@antoyjchubekova ~]$ mkdir dir1/dir2
[guest@antoyjchubekova ~]$ cd dir1/dir2
[guest@antoyjchubekova dir2]$
```

Рис. 4.19: Минимально необходимые права для создания и удаления поддиректория

Таблица 4.2: Минимальные права для совершения операций

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

5 Выводы

В ходе выполнения лабораторной работы №2 я получила 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

- https://esystem.rudn.ru/pluginfile.php/2580978/mod_resource/content/6/002-lab_discret_attr.pdf