

# **Отчет по лабораторной работе №2**

**Дискреционное разграничение прав в Linux. Основные атрибуты**

Бурдина Ксения Павловна

2022 Sep 15th

# Содержание

1. Цель работы	4
2. Ход выполнения лабораторной работы	5
3. Выводы	20
4. Список литературы	21

## Список иллюстраций

2.1. рис 1. Создание учетной записи . . . . .	5
2.2. рис 2. Задание пароля для пользователя . . . . .	5
2.3. рис 3. Вход от имени guest . . . . .	6
2.4. рис 4. Определение директории . . . . .	6
2.5. рис 5. Информация о пользователе по whoami и id . . . . .	6
2.6. рис 6. Вывод groups . . . . .	7
2.7. рис 7. Просмотр файла (н) . . . . .	7
2.8. рис 8. Просмотр файла (к) . . . . .	7
2.9. рис 9. Вывод информации с помощью grep . . . . .	7
2.10. рис 10. Просмотр директорий . . . . .	8
2.11. рис 11. Просмотр информации командой lsattr . . . . .	8
2.12. рис 12. Создание поддиректории и просмотр ls -l . . . . .	9
2.13. рис 13. Просмотр командой lsattr . . . . .	9
2.14. рис 14. Снятие атрибутов с директории . . . . .	10
2.15. рис 15. Попытка создания файла в директории dir1 . . . . .	10
2.16. рис 16. Действия при атрибутах dir1(700) и file(700) . . . . .	11
2.17. рис 17. Действия при атрибутах dir1(700) и file(700) . . . . .	11
2.18. рис 18. Действия при атрибутах dir1(700) и file(000) . . . . .	11
2.19. рис 19. Действия при атрибутах dir1(700) и file(100) . . . . .	12
2.20. рис 20. Действия при атрибутах dir1(700) и file(100) . . . . .	12
2.21. рис 21. Действия при атрибутах dir1(700) и file(200) . . . . .	13
2.22. рис 22. Действия при атрибутах dir1(700) и file(300) . . . . .	14
2.23. рис 23. Действия при атрибутах dir1(700) и file(400) . . . . .	14
2.24. рис 24. Действия при атрибутах dir1(700) и file(500) . . . . .	15
2.25. рис 25. Действия при атрибутах dir1(700) и file(600) . . . . .	15
2.26. рис 26. Таблица прав и разрешений 1 . . . . .	16
2.27. рис 27. Таблица прав и разрешений 2 . . . . .	17
2.28. рис 28. Таблица прав и разрешений 3 . . . . .	18
2.29. рис 29. Таблица минимальных прав для совершения операций . .	19

# 1. Цель работы

Целью данной 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. Ход выполнения лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора):

```
[kpburdina@10 ~]$ sudo useradd guest  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for kpburdina:
```

Рис. 2.1.: рис 1. Создание учетной записи

2. Зададим пароль для пользователя guest (используя учётную запись администратора):

```
[kpburdina@10 ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

Рис. 2.2.: рис 2. Задание пароля для пользователя

3. Войдем в систему от имени пользователя guest:

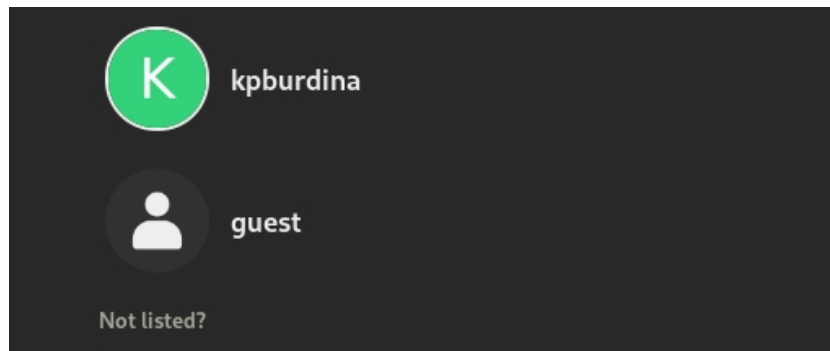


Рис. 2.3.: рис 3. Вход от имени guest

4. Определим директорию, в которой мы находимся, командой `pwd`. Сравнивая с приглашением командной строки, мы видим, что она является домашней директорией:

```
[guest@10 ~]$ pwd
/home/guest
```

Рис. 2.4.: рис 4. Определение директории

5. Уточним имя нашего пользователя командой `whoami`. Увидим, что мы действительно зашли под именем `guest`.

6. Уточним имя нашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и `groups` принимают значение 1001, запомним его:

```
[guest@10 ~]$ cd ..
[guest@10 home]$ whoami
guest
[guest@10 home]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 2.5.: рис 5. Информация о пользователе по `whoami` и `id`

Сравним вывод `id` с выводом команды `groups`:

```
[guest@10 home]$ groups
guest
```

Рис. 2.6.: рис 6. Вывод `groups`

7. Сравнивая полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки, видим, что они совпадают.

8. Просмотрим файл `/etc/passwd`:

```
[guest@10 home]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

Рис. 2.7.: рис 7. Просмотр файла (н)

```
kpburdina:x:1000:1000:kpburdina:/home/kpburdina:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
```

Рис. 2.8.: рис 8. Просмотр файла (к)

Найдем в нём свою учётную запись. Она у нас находится в самом конце. Видим, что `uid` пользователя и `gid` пользователя совпадают со значениями, найденными в предыдущих пунктах.

Мы также можем получить вывод команды с помощью программы `grep` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания. Такой вывод будет выглядеть следующим образом:

```
[guest@10 home]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
```

Рис. 2.9.: рис 9. Вывод информации с помощью `grep`

9. Определим существующие в системе директории:

```
[guest@10 home]$ ls -l /home/  
total 8  
drwx-----. 14 guest      guest      4096 Sep 14 14:08 guest  
drwx-----. 14 kpburdina kpburdina 4096 Sep 14 13:37 kpburdina
```

Рис. 2.10.: рис 10. Просмотр директорий

У нас имеются поддиректории наших учетных записей. Видим, что у обоих пользователей установлены права на чтение, изменение и выполнение только для самого пользователя.

10. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home:

```
[guest@10 home]$ lsattr /home  
lsattr: Permission denied while reading flags on /home/kpburdina  
----- /home/guest
```

Рис. 2.11.: рис 11. Просмотр информации командой lsattr

Можем увидеть, что расширенные атрибуты у директории отсутствуют. Также видно, что на недоступен просмотр расширенных атрибутов директорий других пользователей.

11. Создадим в домашней директории поддиректорию dir1 и определим командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1:



```
[guest@10 ~]$ mkdir dir1
[guest@10 ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Desktop
drwxrwxr-x. 2 guest guest 6 Sep 14 14:16 dir1
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Documents
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Music
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Public
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Templates
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Videos
```

Рис. 2.12.: рис 12. Создание поддиректории и просмотр ls -l

```
[guest@10 ~]$ lsattr
----- .I Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
```

Рис. 2.13.: рис 13. Просмотр командой lsattr

Видим, что у нас в созданной поддиректории имеются права на чтение, исполнение и редактирование у пользователя и группы, а у остальных только на чтение и исполнение.

При этом видим, что доступа к расширенным атрибутам у нас нет.

12. Снимем с директории dir1 все атрибуты командой `chmod 000 dir1` и проверим правильность выполнения команды:

```
[guest@10 ~]$ chmod 000 dir1
[guest@10 ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Desktop
d------. 2 guest guest 6 Sep 14 14:16 dir1
drwxr-xr-x. 2 guest guest 6 Sep 14 14:08 Documents
```

Рис. 2.14.: рис 14. Снятие атрибутов с директории

13. Попытаемся создать в директории `dir1` файл `file1`, однако получим отказ в выполнении операции по созданию файла, так как мы сбросили права на исполнение директории `dir1`. С помощью команды `ls -l /home/guest/dir1` убедились, что файл `file1` не находится внутри директории `dir1`:

```
[guest@10 ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@10 ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
```

Рис. 2.15.: рис 15. Попытка создания файла в директории `dir1`

14. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет ([https://esystem.rudn.ru/pluginfile.php/1651883/mod\\_resource/content/6/002-lab\\_discret\\_attr.pdf](https://esystem.rudn.ru/pluginfile.php/1651883/mod_resource/content/6/002-lab_discret_attr.pdf))[1].

Мы рассматриваем первые три атрибута, которые относятся к владельцу. Это 64 варианта.

Проведем действия с атрибутами директории 700 и атрибутами файла с 000 до 700.

Нам требуется для каждого возможного варианта проверить, будет ли выполняться создание и удаление файла, запись в файл, его чтение, смена директории, просмотр файлов в директории, возможно ли будет переименовывать файл, а также изменять его атрибуты.

Установим атрибуты директории dir1 как 700:

```
[guest@10 dir1]$ rm file
[guest@10 dir1]$ touch file
[guest@10 dir1]$ echo "file" > file
[guest@10 dir1]$ cat file
file
[guest@10 dir1]$ cd
[guest@10 ~]$ cd dir1
[guest@10 dir1]$ ls
file  test
[guest@10 dir1]$ ls -l
total 4
-rw-rw-r--. 1 guest guest 5 Sep 14 23:15 file
drwxr-xr-x. 2 root  root  6 Sep 14 23:07 test
```

Рис. 2.16.: рис 16. Действия при атрибутах dir1(700) и file(700)

```
[guest@10 dir1]$ mv file dir2
[guest@10 dir1]$ mv dir2 file
```

Рис. 2.17.: рис 17. Действия при атрибутах dir1(700) и file(700)

По умолчанию у нас атрибуты созданного файла были 700. Мы видим, что у нас возможны все действия с файлом, просмотр и изменение атрибутов, смена директории, а также просмотр файлов в ней. Занесем эти данные в таблицу.

Теперь изменим атрибуты файла на 000 и проведем все действия с ними:

```
[guest@10 dir1]$ chmod 000 file
[guest@10 dir1]$ ls -l
total 4
----- . 1 guest guest 5 Sep 14 23:15 file
drwxr-xr-x. 2 root  root  6 Sep 14 23:07 test
```

Рис. 2.18.: рис 18. Действия при атрибутах dir1(700) и file(000)

У нас нет никаких прав на работу с файлом, поэтому мы можем создать новый файл, удалить файл и поработать с директорией, в которой у нас есть все права:

сменить, просмотреть содержимое, переименовать файлы, сменить атрибуты файлам.

Изменим атрибуты файла на 100:

```
[guest@10 dir1]$ chmod 100 file
[guest@10 dir1]$ ls -l
total 4
---x----- 1 guest guest 5 Sep 14 23:15 file
-rw-rw-r-- 1 guest guest 0 Sep 14 23:30 file2
```

Рис. 2.19.: рис 19. Действия при атрибутах dir1(700) и file(100)

```
[guest@10 dir1]$ rm file
rm: remove write-protected regular file 'file'? y
[guest@10 dir1]$ ls
file2 test
[guest@10 dir1]$ touch file
[guest@10 dir1]$ chmod 100 file
[guest@10 dir1]$ echo "file1" > file
bash: file: Permission denied
[guest@10 dir1]$ cat file
cat: file: Permission denied
[guest@10 dir1]$ ls
file file2 test
[guest@10 dir1]$ mv file file3
[guest@10 dir1]$ ls
file2 file3 test
```

Рис. 2.20.: рис 20. Действия при атрибутах dir1(700) и file(100)

Видим, что у нас появилась возможность на исполнение файла, но мы по прежнему не смодем записать в него данные или прочитать.

Изменим атрибуты файла на 200:

```

[guest@10 dir1]$ chmod 200 file
[guest@10 dir1]$ echo "слово" > file
[guest@10 dir1]$ cat file
cat: file: Permission denied
[guest@10 dir1]$ ls
file file2 file5 test
[guest@10 dir1]$ ls -l
total 4
--w-----. 1 guest guest 6 Sep 15 00:19 file
-rw-rw-r--. 1 guest guest 0 Sep 14 23:30 file2
-rw-rw-r--. 1 guest guest 0 Sep 15 00:08 file5
drwxr-xr-x. 2 root root 6 Sep 14 23:07 test
[guest@10 dir1]$ mv file file4
[guest@10 dir1]$ ls
file2 file4 file5 test
[guest@10 dir1]$ mv file4 file
[guest@10 dir1]$ ls
file file2 file5 test
[guest@10 dir1]$ rm file
[guest@10 dir1]$ ls
file2 file5 test
[guest@10 dir1]$ touch file

```

Рис. 2.21.: рис 21. Действия при атрибутах dir1(700) и file(200)

Теперь мы имеем право сделать запись в файл, поскольку появилась возможность редактирования файла, но по прежнему нет права на чтение.

Изменим атрибуты на 300:

```

[guest@10 dir1]$ chmod 300 file
[guest@10 dir1]$ rm file
[guest@10 dir1]$ touch file
[guest@10 dir1]$ chmod 300 file
[guest@10 dir1]$ echo "aa" > file
[guest@10 dir1]$ cat file
cat: file: Permission denied
[guest@10 dir1]$ ls
file file2 file5 test
[guest@10 dir1]$ mv file file66
[guest@10 dir1]$ ls
file2 file5 file66 test
[guest@10 dir1]$ mv file66 file
[guest@10 dir1]$ ls -l
total 4
--wx-----. 1 guest guest 3 Sep 15 00:24 file
-rw-rw-r--. 1 guest guest 0 Sep 14 23:30 file2
-rw-rw-r--. 1 guest guest 0 Sep 15 00:08 file5
drwxr-xr-x. 2 root root 6 Sep 14 23:07 test

```

Рис. 2.22.: рис 22. Действия при атрибутах dir1(700) и file(300)

У нас также имеется возможность исполнения файла и редактирования.

Изменим атрибуты на 400:

```

[guest@10 dir1]$ chmod 400 file
[guest@10 dir1]$ ls -l
total 4
-r-----. 1 guest guest 3 Sep 15 00:24 file
-rw-rw-r--. 1 guest guest 0 Sep 14 23:30 file2
-rw-rw-r--. 1 guest guest 0 Sep 15 00:08 file5
drwxr-xr-x. 2 root root 6 Sep 14 23:07 test
[guest@10 dir1]$ echo "bb" > file
bash: file: Permission denied
[guest@10 dir1]$ cat file
aa
[guest@10 dir1]$ ls
file file2 file5 test
[guest@10 dir1]$ cd
[guest@10 ~]$ cd dir1
[guest@10 dir1]$ mv file file66
[guest@10 dir1]$ ls
file2 file5 file66 test
[guest@10 dir1]$ mv file66 file
[guest@10 dir1]$ rm file
rm: remove write-protected regular file 'file'? y
[guest@10 dir1]$ ls
file2 file5 test

```

Рис. 2.23.: рис 23. Действия при атрибутах dir1(700) и file(400)

Теперь у нас есть право на чтение файла, но нет возможности редактирования.

Посмотрим возможности работы с атрибутами файла 500:

```
[guest@10 dir1]$ chmod 500 file
[guest@10 dir1]$ ls -l
total 0
-r-x-----. 1 guest guest 0 Sep 15 00:32 file
-rw-rw-r--. 1 guest guest 0 Sep 14 23:30 file2
-rw-rw-r--. 1 guest guest 0 Sep 15 00:08 file5
drwxr-xr-x. 2 root root 6 Sep 14 23:07 test
[guest@10 dir1]$ echo "bb" > file
bash: file: Permission denied
[guest@10 dir1]$ cat file
[guest@10 dir1]$ rm file
rm: remove write-protected regular empty file 'file'? y
[guest@10 dir1]$ ls
file2 file5 test
```

Рис. 2.24.: рис 24. Действия при атрибутах dir1(700) и file(500)

Мы можем исполнять и читать файл, однако у нас нет права на редактирование.

Завершим просмотр директории dir1 с атрибутами 700 просмотром возможностей файла с атрибутами 600:

```
[guest@10 dir1]$ chmod 600 file
[guest@10 dir1]$ ls -l
total 0
-rw-----. 1 guest guest 0 Sep 15 00:36 file
-rw-rw-r--. 1 guest guest 0 Sep 14 23:30 file2
-rw-rw-r--. 1 guest guest 0 Sep 15 00:08 file5
drwxr-xr-x. 2 root root 6 Sep 14 23:07 test
[guest@10 dir1]$ echo "bb" > file
[guest@10 dir1]$ cat file
bb
[guest@10 dir1]$ rm file
[guest@10 dir1]$ ls
file2 file5 test
```

Рис. 2.25.: рис 25. Действия при атрибутах dir1(700) и file(600)

Видим, что мы можем и прочесть файл, и изменить его. Нет права лишь на

исполнение.

По аналогии проведем действия с другими атрибутами директории dir1 (от 000 до 600). По итогам заполним общую таблицу. Она выглядит следующим образом:

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d-----(000)	-----(000)	-	-	-	-	-	-	-	-
d-----(000)	--x----(100)	-	-	-	-	-	-	-	-
d-----(000)	-w-----(200)	-	-	-	-	-	-	-	-
d-----(000)	-wx-----(300)	-	-	-	-	-	-	-	-
d-----(000)	r-----(400)	-	-	-	-	-	-	-	-
d-----(000)	r-x-----(500)	-	-	-	-	-	-	-	-
d-----(000)	rw-----(600)	-	-	-	-	-	-	-	-
d-----(000)	rw-x-----(700)	-	-	-	-	-	-	-	-
d--x----(100)	-----(000)	-	-	-	-	+	-	-	+
d--x----(100)	--x----(100)	-	-	-	-	+	-	-	+
d--x----(100)	-w-----(200)	-	-	+	-	+	-	-	+
d--x----(100)	-wx-----(300)	-	-	+	-	+	-	-	+
d--x----(100)	r-----(400)	-	-	-	+	+	-	-	+
d--x----(100)	r-x-----(500)	-	-	-	+	+	-	-	+
d--x----(100)	rw-----(600)	-	-	+	+	+	-	-	+
d--x----(100)	rw-x-----(700)	-	-	+	+	+	-	-	+
d-w-----(200)	-----(000)	-	-	-	-	-	-	-	-
d-w-----(200)	--x----(100)	-	-	-	-	-	-	-	-
d-w-----(200)	-w-----(200)	-	-	-	-	-	-	-	-
d-w-----(200)	-wx-----(300)	-	-	-	-	-	-	-	-
d-w-----(200)	r-----(400)	-	-	-	-	-	-	-	-

Рис. 2.26.: рис 26. Таблица прав и разрешений 1



Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d-w-----(200)	r-x-----(500)	-	-	-	-	-	-	-	-
d-w-----(200)	rw-----(600)	-	-	-	-	-	-	-	-
d-w-----(200)	rwX-----(700)	-	-	-	-	-	-	-	-
d-wX-----(300)	----- (000)	+	+	-	-	+	-	+	+
d-wX-----(300)	--X----- (100)	+	+	-	-	+	-	+	+
d-wX-----(300)	-W----- (200)	+	+	+	-	+	-	+	+
d-wX-----(300)	-wX----- (300)	+	+	+	-	+	-	+	+
d-wX-----(300)	r----- (400)	+	+	-	+	+	-	+	+
d-wX-----(300)	r-x----- (500)	+	+	-	+	+	-	+	+
d-wX-----(300)	rw----- (600)	+	+	+	+	+	-	+	+
d-wX-----(300)	rwX----- (700)	+	+	+	+	+	-	+	+
dr----- (400)	----- (000)	-	-	-	-	-	+	-	-
dr----- (400)	--X----- (100)	-	-	-	-	-	+	-	-
dr----- (400)	-W----- (200)	-	-	-	-	-	+	-	-
dr----- (400)	-wX----- (300)	-	-	-	-	-	+	-	-
dr----- (400)	r----- (400)	-	-	-	-	-	+	-	-
dr----- (400)	r-x----- (500)	-	-	-	-	-	+	-	-
dr----- (400)	rw----- (600)	-	-	-	-	-	+	-	-
dr----- (400)	rwX----- (700)	-	-	-	-	-	+	-	-
dr-x----- (500)	----- (000)	-	-	-	-	+	+	-	-
dr-x----- (500)	--X----- (100)	-	-	-	-	+	+	-	-

Рис. 2.27.: рис 27. Таблица прав и разрешений 2

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
dr-x-----(500)	-w-----(200)	-	-	-	-	+	+	-	-
dr-x-----(500)	-wx-----(300)	-	-	-	-	+	+	-	-
dr-x-----(500)	r-----(400)	-	-	-	-	+	+	-	-
dr-x-----(500)	r-x-----(500)	-	-	-	-	+	+	-	-
dr-x-----(500)	rw-----(600)	-	-	-	-	+	+	-	-
dr-x-----(500)	rw-x-----(700)	-	-	-	-	+	+	-	-
drw-----(600)	----- (000)	-	-	-	-	-	+	+	+
drw-----(600)	--x-----(100)	-	-	-	-	-	+	+	+
drw-----(600)	-w-----(200)	-	-	-	-	-	+	+	+
drw-----(600)	-wx-----(300)	-	-	-	-	-	+	+	+
drw-----(600)	r-----(400)	-	-	-	-	-	+	+	+
drw-----(600)	r-x-----(500)	-	-	-	-	-	+	+	+
drw-----(600)	rw-----(600)	-	-	-	-	-	+	+	+
drw-----(600)	rw-x-----(700)	-	-	-	-	-	+	+	+
drwx----- (700)	----- (000)	+	+	-	-	+	+	+	+
drwx----- (700)	--x-----(100)	+	+	-	-	+	+	+	+
drwx----- (700)	-w-----(200)	+	+	+	-	+	+	+	+
drwx----- (700)	-wx-----(300)	+	+	+	-	+	+	+	+
drwx----- (700)	r-----(400)	+	+	-	+	+	+	+	+
drwx----- (700)	r-x-----(500)	+	+	-	+	+	+	+	+
drwx----- (700)	rw-----(600)	+	+	+	+	+	+	+	+
drwx----- (700)	rw-x-----(700)	+	+	+	+	+	+	+	+

Рис. 2.28.: рис 28. Таблица прав и разрешений 3

Проанализировав данную таблицу, можем увидеть минимальные права, которые необходимы для совершения каждой из операций. Занесем данные наблюдения в таблицу:

### 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)

Рис. 2.29.: рис 29. Таблица минимальных прав для совершения операций

### **3. Выводы**

В ходе работы мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

## 4. Список литературы

1. Методические материалы курса ([https://esystem.rudn.ru/pluginfile.php/1651883/mod\\_resource/content/1/lab\\_discret\\_attr.pdf](https://esystem.rudn.ru/pluginfile.php/1651883/mod_resource/content/1/lab_discret_attr.pdf))