

Отчёт по лабораторной работе №2

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

1	Цель работы	4
2	Задания	5
3	Выполнение лабораторной работы	6
3.1	Знакомство с пользователями и их атрибутами	6
3.2	Заполнение таблиц 2.1 и 2.2	10
3.3	Как работает система нумерации прав	10
3.4	Таблица 2.1 “Установленные права и разрешённые действия” . . .	13
3.5	Таблица 2.2 “Минимальные права для совершения операций” . . .	17
4	Выводы	18
5	Список литературы	19

Список иллюстраций

3.1	Новый пользователь	6
3.2	Новый пользователь успешно создан	7
3.3	Команда pwd	7
3.4	Имя пользователя	8
3.5	Группы, пользователи и их ID	8
3.6	Пользователи, группы и их ID	8
3.7	Директории пользователей	9
3.8	Аттрибуты пользователей	9
3.9	Аттрибуты dir1	9
3.10	Аттрибуты dir1 больше нет	10
3.11	Не выходит создать файл в папке dir1	10
3.12	Схема: Права и их нумерация	11
3.13	Процесс заполнения таблицы 1	12
3.14	Процесс заполнения таблицы 2	12
3.15	Процесс заполнения таблицы 3	13

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

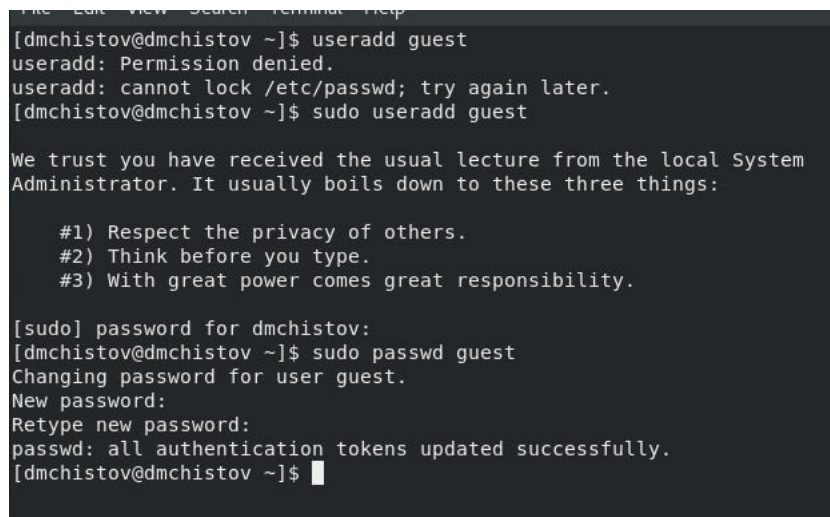
2 Задания

1. Знакомство с пользователями и их атрибутами
2. Заполнение таблиц 2.1 и 2.2

3 Выполнение лабораторной работы

3.1 Знакомство с пользователями и их атрибутами

Добавляю нового пользователя - guest, затем задаю ему пароль (рис. 3.1).



```
File Edit View Search Terminal Help
[dmchistov@dmchistov ~]$ useradd guest
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
[dmchistov@dmchistov ~]$ 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 dmchistov:
[dmchistov@dmchistov ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[dmchistov@dmchistov ~]$
```

Рис. 3.1: Новый пользователь

Видно, что новый пользователь успешно создан. Захожу в него. (рис. 3.2).

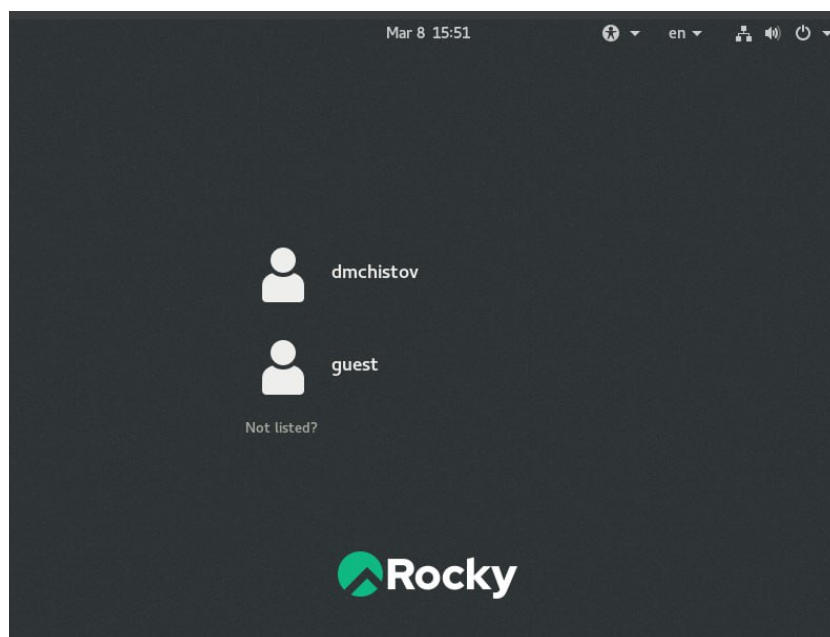


Рис. 3.2: Новый пользователь успешно создан

Командой `pwd` определяю своё местоположение в файловой системе - я нахожусь в домашнем каталоге пользователя `guest`, это также можно было определить по значку `~` в командной строке (рис. 3.3).

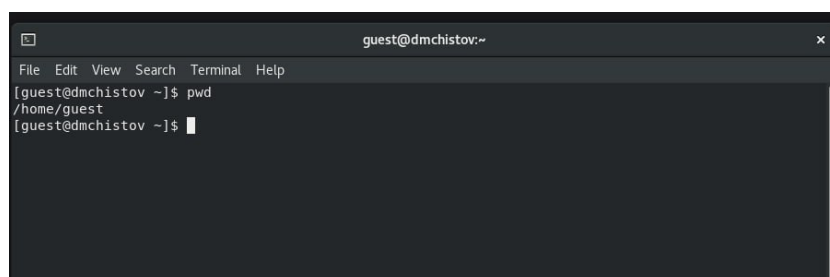


Рис. 3.3: Команда `pwd`

Командой `whoami`, уточняю имя пользователя - `guest` (рис. 3.4).

```
[guest@dmchistov ~]$ whoami
guest
[guest@dmchistov ~]$
```

Рис. 3.4: Имя пользователя

Командой `id` получаю информацию о `uid` и `gid` - таким образом я получил `id` пользователя и его группы, затем командой `groups` вывожу группу - там также указана группа `guest` (рис. 3.5).

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

Рис. 3.5: Группы, пользователи и их ID

Командой `cat /etc/passwd | grep guest` (`grep guest` пишу, чтобы прочитать информацию исключительно о нашем пользователе - `guest`) определяю `uid` и `gid` пользователя, сравниваю их с выводом команды `id`, всё совпадает (рис. 3.6).

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

Open

ids.txt

~

```
uid=1001(guest) gid=1001(guest) groups=1001(guest)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 3.6: Пользователи, группы и их ID

Командой `ls -l /home/` определяю существующие в системе директории - определил, что в `home` теперь домашняя директория пользователя `guest` и домашняя директория пользователя `dmchistov` - моего основного пользователя. Права у каждой директорий стоят полные для пользователей (700) (рис. 3.7).


```
[guest@dmchistov ~]$ ls -l /home/
total 8
drwx----- 15 dmchistov dmchistov 4096 Mar  8 15:51 dmchistov
drwx----- 15 guest      guest      4096 Mar  8 16:00 guest
```

Рис. 3.7: Директории пользователей

Командой `lsattr` определяю расширенные атрибуты каждой директории внутри `/home`, однако мне не удалось узнать об атрибутах директории `dmchistov`, т.к. это другой пользователь, зато получилось узнать об атрибутах пользователя `guest` (рис. 3.8).

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

Рис. 3.8: Атрибуты пользователей

Создаю директорию `dir1` и командой `ls -l` узнаю о её правах (рис. 3.9).

```
File Edit View Search Terminal Help
[guest@dmchistov ~]$ rm -r dir1
[guest@dmchistov ~]$ mkdir dir1
[guest@dmchistov ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Desktop
drwxrwxr-x. 2 guest guest  6 Mar  8 16:15 dir1
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Documents
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Downloads
-rw-rw-r-- 1 guest guest 114 Mar  8 15:58 ids.txt
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Music
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Pictures
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Public
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Templates
drwxr-xr-x. 2 guest guest  6 Mar  8 15:51 Videos
[guest@dmchistov ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/dmchistov
----- /home/guest
[guest@dmchistov ~]$ lsattr /home/guest/dir1/
[guest@dmchistov ~]$
```

Рис. 3.9: Атрибуты dir1

Командой `chmod 000 dir1`, снимаю все атрибуты с директории `dir1`, командой `ls -l` подтверждаю, что у директории больше нет никаких прав (рис. 3.10).

```
[guest@dmchistov ~]$ chmod 000 dir1
[guest@dmchistov ~]$ ls -l
total 4
drwxr-xr-x. 2 guest guest 6 Mar 8 15:51 Desktop
d----- . 2 guest guest 6 Mar 8 16:15 dir1
drwxr-xr-x. 2 guest guest 6 Mar 8 15:51 Documents
```

Рис. 3.10: Атрибуты dir1 больше нет

Попытаюсь создать в директории dir1 файл, однако получаю отказ, т.к. ранее я снял все права доступа к этой директории, поэтому ни один пользователь не может получить доступ к этой папке, соответственно и не может создать файл (рис. 3.11).

```
[guest@dmchistov ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@dmchistov ~]$ ls -l /home/guest/dir1/
ls: cannot open directory '/home/guest/dir1/': Permission denied
[guest@dmchistov ~]$
[guest@dmchistov ~]$ chmod 700 dir1
[guest@dmchistov ~]$ ls -l /home/guest/dir1/
total 0
[guest@dmchistov ~]$ ls /home/guest/dir1/
[guest@dmchistov ~]$
```

Рис. 3.11: Не выходит создать файл в папке dir1

3.2 Заполнение таблиц 2.1 и 2.2

Теперь, перехожу к заполнению таблиц - требуется определить опытным путём, какие комбинации прав для файла и директории позволяет пользователю совершать те или иные действия с директориями и файлами внутри них.

3.3 Как работает системе нумерации прав

В интернете я нашёл удобную схему, которая показывает число и соответствующее ему право (рис. 3.12):

1 - execute, 2 - write, 3 - write & execute, 4 - read, 5 - read & execute, 6 - read & write, 7 - read & write & execute

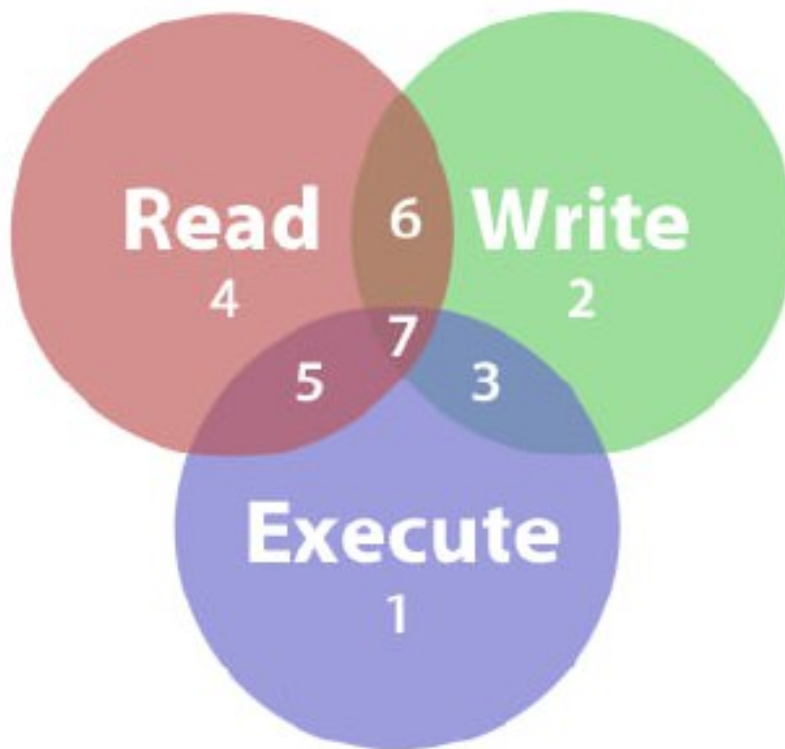


Рис. 3.12: Схема: Права и их нумерация

Пользуясь такой схемой, сначала я устанавливал права для директории, затем устанавливал каждый тип прав для файла, внутри этой директории и каждый проверял те или иные действия, затем заносил результат в таблицу. Затем задавал следующие права для директории, заново задавал права для файла и проверял операции. И так далее (рис. 3.13), (рис. 3.14), (рис. 3.15):

```

File Edit View Search Terminal Help
[guest@dmchistov dir1]$ cd ..
[guest@dmchistov ~]$ rm dir1/test.txt
rm: cannot remove 'dir1/test.txt': Permission denied
[guest@dmchistov ~]$ echo "aoiughahguoahoghaoughaso" > test.txt
[guest@dmchistov ~]$ cat dir1/test.txt
cat: dir1/test.txt: Permission denied
[guest@dmchistov ~]$ chmod 700 dir1
[guest@dmchistov ~]$ cat dir1/test.txt
cat: dir1/test.txt: Permission denied
[guest@dmchistov ~]$ chmod 100 dir1
[guest@dmchistov ~]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest@dmchistov ~]$ cd dir1
[guest@dmchistov dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest@dmchistov dir1]$ mv dir1/test.txt dir1/testik.txt
mv: cannot stat 'dir1/test.txt': No such file or directory
[guest@dmchistov dir1]$ chmod 400 test.txt
[guest@dmchistov dir1]$ cd ..
[guest@dmchistov ~]$ echo "sijgpsjgjsigj" > dir1/test.txt
bash: dir1/test.txt: Permission denied
[guest@dmchistov ~]$ cat dir1/test.txt
yo yo yolushki
[guest@dmchistov ~]$

```

Рис. 3.13: Процесс заполнения таблицы 1

```

drwxr-xr-x. 2 guest guest    6 Mar  8 15:51 Templates
-rw-rw-r--. 1 guest guest    9 Mar  8 17:28 test.txt
drwxr-xr-x. 2 guest guest    6 Mar  8 15:51 Videos
[guest@dmchistov ~]$ chmod 700 dir1
[guest@dmchistov ~]$ cd dir1
[guest@dmchistov dir1]$ chmod 100 test.txt
[guest@dmchistov dir1]$ cd ..
[guest@dmchistov ~]$ chmod 200 dir1
[guest@dmchistov ~]$ rm dir1/test.txt
rm: cannot remove 'dir1/test.txt': Permission denied
[guest@dmchistov ~]$ echo "sagjpsg" > dir1/test.txt
bash: dir1/test.txt: Permission denied
[guest@dmchistov ~]$ cd dir1/dir2
bash: cd: dir1/dir2: Permission denied
[guest@dmchistov ~]$ cd dir1
bash: cd: dir1: Permission denied

```

Рис. 3.14: Процесс заполнения таблицы 2

```
dir1 testik.txt
[guest@dmchistov ~]$ rm testik.txt
[guest@dmchistov ~]$ mv dir1/testik.txt dir1/test.txt
mv: failed to access 'dir1/test.txt': Permission denied
[guest@dmchistov ~]$ chmod 400 dir1/testik.txt
chmod: cannot access 'dir1/testik.txt': Permission denied
[guest@dmchistov ~]$ chmod 700 dir1
[guest@dmchistov ~]$ chmod 400 dir1/testik.txt
[guest@dmchistov ~]$ chmod 400 dir1
[guest@dmchistov ~]$ cat dir1/testik.txt
cat: dir1/testik.txt: Permission denied
[guest@dmchistov ~]$ echo yolk > dir1/testik.txt
bash: dir1/testik.txt: Permission denied
[guest@dmchistov ~]$ mv dir1/testik.txt dir1/test.txt
mv: failed to access 'dir1/test.txt': Permission denied
[guest@dmchistov ~]$ chmod 700 dir1
[guest@dmchistov ~]$ chmod 000 dir1/testik.txt
[guest@dmchistov ~]$ chmod 500 dir1
[guest@dmchistov ~]$ touch dir1/yomayo.txt
touch: cannot touch 'dir1/yomayo.txt': Permission denied
[guest@dmchistov ~]$ rm dir1/testik.txt
rm: remove write-protected regular file 'dir1/testik.txt'? y
rm: cannot remove 'dir1/testik.txt': Permission denied
[guest@dmchistov ~]$ echo Kapeč > dir1/testik.txt
bash: dir1/testik.txt: Permission denied
[guest@dmchistov ~]$ cat dir1/testik.txt
cat: dir1/testik.txt: Permission denied
[guest@dmchistov ~]$ cd dir1/dir2
[guest@dmchistov dir2]$ cd ..
[guest@dmchistov dir1]$ cd ..
[guest@dmchistov ~]$ cd dir1
[guest@dmchistov dir1]$ cd ..
[guest@dmchistov ~]$ ls dir1
dir2 testik.txt
[guest@dmchistov ~]$ mv dir1/testik.txt dir1/test.txt
mv: cannot move 'dir1/testik.txt' to 'dir1/test.txt': Permission denied
[guest@dmchistov ~]$ chmod 100 dir1/testik.txt
[guest@dmchistov ~]$ rm dir1/testik.txt
rm: remove write-protected regular file 'dir1/testik.txt'? y
rm: cannot remove 'dir1/testik.txt': Permission denied
[guest@dmchistov ~]$ echo ägsagsgsä > dir1/testik.txt
bash: dir1/testik.txt: Permission denied
[guest@dmchistov ~]$ cat dir1/testik.txt
cat: dir1/testik.txt: Permission denied
[guest@dmchistov ~]$ mv dir1/testik.txt dir1/test.txt
mv: cannot move 'dir1/testik.txt' to 'dir1/test.txt': Permission denied
[guest@dmchistov ~]$ chmod 200 dir1/testik.txt
[guest@dmchistov ~]$
```

Рис. 3.15: Процесс заполнения таблицы 3

По итогу получилась вот такая таблица:

3.4 Таблица 2.1 “Установленные права и разрешённые действия”

Права							Про-		
	Пра-						смотр	Пере-	
ди-рек-то-рии	ва	Созда-ние	Удале-ние	За-пись в файл	Чте-ние файла	Смена дирек-тории	фай-лов в дирек-тории	име-нова-ние файла	Смена атри-бутов файла
d(000) (000)		-	-	-	-	-	-	-	-
d(000) (100)		-	-	-	-	-	-	-	-
d(000) (200)		-	-	-	-	-	-	-	-

Пра-							Про-		
ва							смотр	Пере-	
ди-	Пра-						фай-	име-	Смена
рек-	ва	Созда-	Удале-	За-	Чте-	Смена	лов в	нова-	аттри-
то-	фай-	ние	ние	пись в	ние	дирек-	дирек-	ние	бутов
рии	ла	файла	файла	файл	файла	тории	тории	файла	файла
d(000) (300)		-	-	-	-	-	-	-	-
d(000) (400)		-	-	-	-	-	-	-	-
d(000) (500)		-	-	-	-	-	-	-	-
d(000) (600)		-	-	-	-	-	-	-	-
d(000) (700)		-	-	-	-	-	-	-	-
d(100) (000)		-	-	-	-	+	-	-	+
d(100) (100)		-	-	-	-	+	-	-	+
d(100) (200)		-	-	+	-	+	-	-	+
d(100) (300)		-	-	+	-	+	-	-	+
d(100) (400)		-	-	-	+	+	-	-	+
d(100) (500)		-	-	-	+	+	-	-	+
d(100) (600)		-	-	+	+	+	-	-	+
d(100) (700)		-	-	+	+	+	-	-	+
d(200) (000)		-	-	-	-	-	-	-	-
d(200) (100)		-	-	-	-	-	-	-	-
d(200) (200)		-	-	-	-	-	-	-	-
d(200) (300)		-	-	-	-	-	-	-	-
d(200) (400)		-	-	-	-	-	-	-	-
d(200) (500)		-	-	-	-	-	-	-	-
d(200) (600)		-	-	-	-	-	-	-	-
d(200) (700)		-	-	-	-	-	-	-	-
d(300) (000)		+	+	-	-	+	-	+	+
d(300) (100)		+	+	-	-	+	-	+	+

Пра-							Про-		
ва							смотр	Пере-	
ди-	Пра-						фай-	име-	Смена
рек-	ва	Созда-	Удале-	За-	Чте-	Смена	лов в	нова-	аттри-
то-	фай-	ние	ние	пись в	ние	дирек-	дирек-	ние	бутов
рии	ла	файла	файла	файл	файла	тории	тории	файла	файла
d(300) (200)		+	+	+	-	+	-	+	+
d(300) (300)		+	+	+	-	+	-	+	+
d(300) (400)		+	+	-	+	+	-	+	+
d(300) (500)		+	+	-	+	+	-	+	+
d(300) (600)		+	+	+	+	+	-	+	+
d(300) (700)		+	+	+	+	+	-	+	+
d(400) (000)		-	-	-	-	-	+	-	-
d(400) (100)		-	-	-	-	-	+	-	-
d(400) (200)		-	-	-	-	-	+	-	-
d(400) (300)		-	-	-	-	-	+	-	-
d(400) (400)		-	-	-	-	-	+	-	-
d(400) (500)		-	-	-	-	-	+	-	-
d(400) (600)		-	-	-	-	-	+	-	-
d(400) (700)		-	-	-	-	-	+	-	-
d(500) (000)		-	-	-	-	+	+	-	+
d(500) (100)		-	-	-	-	+	+	-	+
d(500) (200)		-	-	+	-	+	+	-	+
d(500) (300)		-	-	+	-	+	+	-	+
d(500) (400)		-	-	-	+	+	+	-	+
d(500) (500)		-	-	-	+	+	+	-	+
d(500) (600)		-	-	+	+	+	+	-	+
d(500) (700)		-	-	+	+	+	+	-	+
d(600) (000)		-	-	-	-	-	+	-	-

Права							Про-		
ди-	Пра-						смотр	Пере-	
рек-	ва	Созда-	Удале-	За-	Чте-	Смена	фай-	име-	Смена
то-	фай-	ние	ние	пись в	ние	дирек-	лов в	нова-	аттри-
рии	ла	файла	файла	файл	файла	тории	дирек-	ние	бутов
							тории	файла	файла
d(600) (100)		-	-	-	-	-	+	-	-
d(600) (200)		-	-	-	-	-	+	-	-
d(600) (300)		-	-	-	-	-	+	-	-
d(600) (400)		-	-	-	-	-	+	-	-
d(600) (500)		-	-	-	-	-	+	-	-
d(600) (600)		-	-	-	-	-	+	-	-
d(600) (700)		-	-	-	-	-	+	-	-
d(700) (000)		+	+	-	-	+	+	+	+
d(700) (100)		+	+	-	-	+	+	+	+
d(700) (200)		+	+	+	-	+	+	+	+
d(700) (300)		+	+	+	-	+	+	+	+
d(700) (400)		+	+	-	+	+	+	+	+
d(700) (500)		+	+	-	+	+	+	+	+
d(700) (600)		+	+	+	+	+	+	+	+
d(700) (700)		+	+	+	+	+	+	+	+

Опираясь на эту таблицу, я заполнил таблицу 2.2. Там просто требуется определить какие минимальные права нужны для файла и директории, чтобы выполнить ту или иную операцию. Заполнял просто определяя первую встретившуюся строчку, где стоит + для нужной мне операции, затем смотрел в ячейку с правами для директории и правами для файла.

В конце концов получилась вот такая таблица:

3.5 Таблица 2.2 “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

4 Выводы

При выполнении данной лабораторной работы я получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

5 Список литературы

Лабораторная работы №2