

Отчет по лабораторной работе 2

Дисциплина: Информационная безопасность

Дяченко Злата Константиновна, НФИбд-03-18

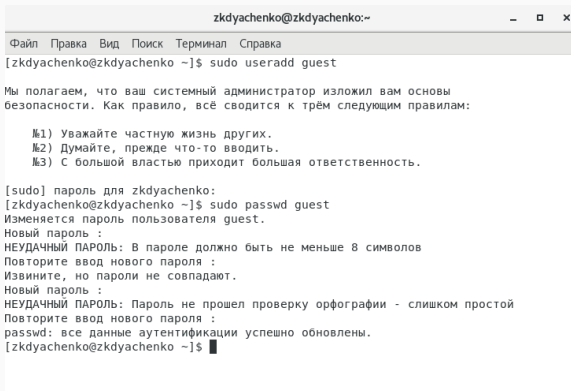
Данная лабораторная работа выполнялась мной для приобретения практических навыков работы в консоли с атрибутами файлов, закрепления теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Цель выполнения лабораторной работы

Выполняя все задачи, определить опытным путем минимально необходимые права для выполнения операций внутри директории.

Задачи выполнения лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создать учётную запись пользователя `guest` и задать пароль для этого пользователя (рис. -fig. 1)

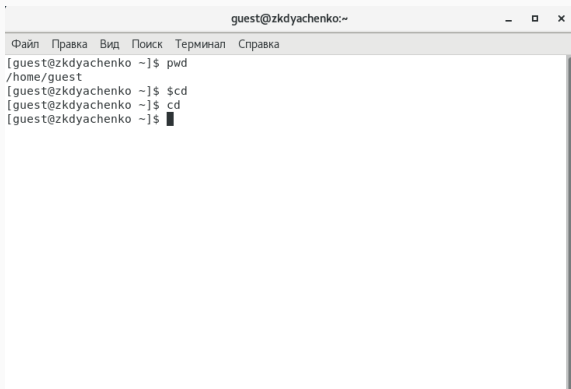


```
zkdyachenko@zkdyachenko:~  
Файл Правка Вид Поиск Терминал Справка  
[zkdyachenko@zkdyachenko ~]$ sudo useradd guest  
  
Мы полагаем, что ваш системный администратор изложил вам основы  
безопасности. Как правило, всё сводится к трём следующим правилам:  
  
№1) Уважайте частную жизнь других.  
№2) Думайте, прежде что-то вводить.  
№3) С большой властью приходит большая ответственность.  
  
[sudo] пароль для zkdyachenko:  
[zkdyachenko@zkdyachenko ~]$ sudo passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов  
Повторите ввод нового пароля :  
Извините, но пароли не совпадают.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[zkdyachenko@zkdyachenko ~]$
```

Figure 1: Создание пользователя и пароля

Задачи выполнения лабораторной работы

Войти в систему от имени пользователя guest и определить директорию, в которой нахожусь - она является домашней (рис. -fig. 2).



```
guest@zkdyachenko:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@zkdyachenko ~]$ pwd  
/home/guest  
[guest@zkdyachenko ~]$ $cd  
[guest@zkdyachenko ~]$ cd  
[guest@zkdyachenko ~]$ █
```

Figure 2: Определение домашней директории

Задачи выполнения лабораторной работы

Уточнить имя пользователя командой *whoami* (рис. -fig. 3)

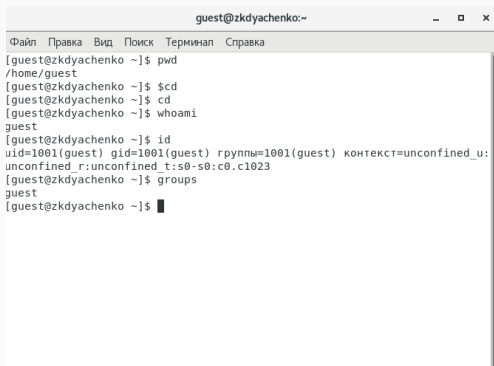


```
guest@zkdyachenko:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@zkdyachenko ~]$ pwd  
/home/guest  
[guest@zkdyachenko ~]$ $cd  
[guest@zkdyachenko ~]$ cd  
[guest@zkdyachenko ~]$ whoami  
guest  
[guest@zkdyachenko ~]$
```

Figure 3: Выполнение команды *whoami*

Задачи выполнения лабораторной работы

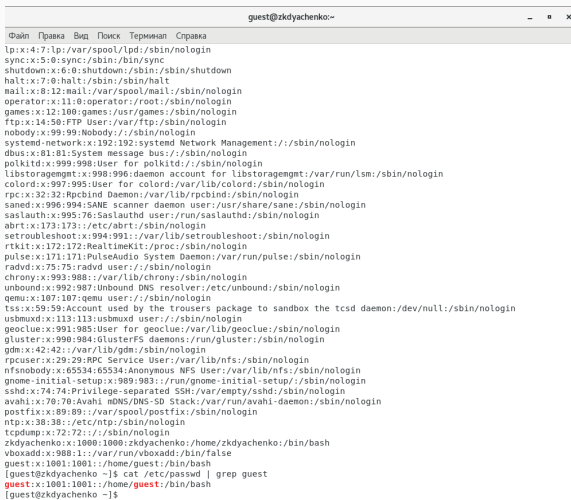
С помощью команды *id* уточнить имя пользователя, его группу, а также группы, куда входит пользователь с помощью команд *id* и *groups* (рис. -fig. 4). Сравнить выведенные значения *uid* и *gid* пользователя с их значениями в файле */etc/passwd* (рис. -fig. 5)



```
guest@zkdyachenko:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@zkdyachenko ~]$ pwd  
/home/guest  
[guest@zkdyachenko ~]$ $cd  
[guest@zkdyachenko ~]$ cd  
[guest@zkdyachenko ~]$ whoami  
guest  
[guest@zkdyachenko ~]$ id  
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:  
unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@zkdyachenko ~]$ groups  
guest  
[guest@zkdyachenko ~]$ █
```

Figure 4: Выполнение команд *id* и *groups*

Задачи выполнения лабораторной работы

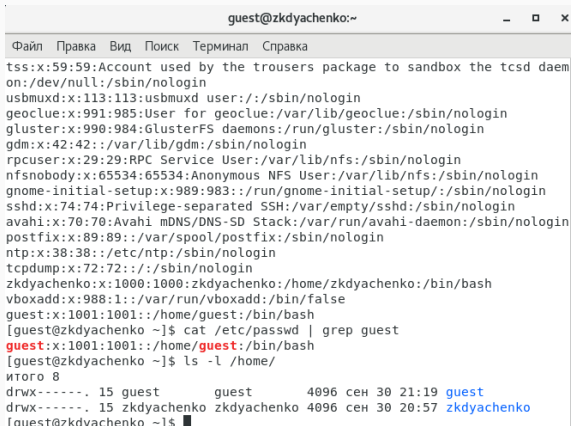


```
guest@zkdyachenko:~  
Файл Правка Вид Поиск Терминал Справка  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:/:/sbin/nologin  
systemd:network:x:192:192:systemd Network Management:/:/sbin/nologin  
dbus:x:81:81:System message bus:/:/sbin/nologin  
polkitd:x:999:998:User for polkitd:/:/sbin/nologin  
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin  
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin  
saned:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin  
saslauthd:x:995:76:Saslauthd user:/run/saslauthd:/sbin/nologin  
abrt:x:173:173:/:etc/abrt:/sbin/nologin  
setroubleshoot:x:994:991:/:var/lib/setroubleshoot:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
chrony:x:993:988:/:var/lib/chrony:/sbin/nologin  
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
qemu:x:107:107:qemu user:/:/sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
gnome-initial-setup:x:989:983:/:run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin  
ntp:x:38:38:/:etc/ntp:/sbin/nologin  
tcpdump:x:72:72:/:/sbin/nologin  
zkdyachenko:x:1000:1000:zkdyachenko:/home/zkdyachenko:/bin/bash  
vboxadd:x:988:1:/:var/run/vboxadd:/bin/false  
guest:x:1001:1001:/:home/guest:/bin/bash  
[guest@zkdyachenko ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:/:home/guest:/bin/bash  
[guest@zkdyachenko ~]$
```

Figure 5: Просмотр файла /etc/passwd

Задачи выполнения лабораторной работы

Определить существующие в системе директории и права командой `ls -l /home/` (рис. -fig. 6).

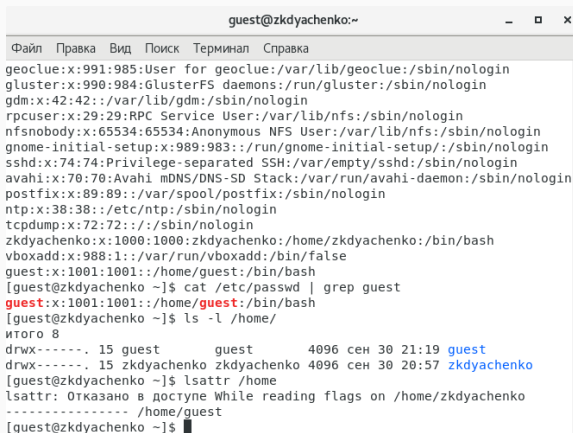


```
guest@zkdyachenko:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daem  
on:/dev/null:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin  
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
gnome-initial-setup:x:989:983:/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89:/var/spool/postfix:/sbin/nologin  
ntp:x:38:38:/etc/ntp:/sbin/nologin  
tcpdump:x:72:72:/sbin/nologin  
zkdyachenko:x:1000:1000:zkdyachenko:/home/zkdyachenko:/bin/bash  
vboxadd:x:988:1:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@zkdyachenko ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@zkdyachenko ~]$ ls -l /home/  
итого 8  
drwx-----. 15 guest          guest          4096 сен 30 21:19 guest  
drwx-----. 15 zkdyachenko  zkdyachenko  4096 сен 30 20:57 zkdyachenko  
[guest@zkdyachenko ~]$
```

Figure 6: Существующие поддиректории

Задачи выполнения лабораторной работы

Проверить, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой `lsattr /home` (рис. -fig. 7).



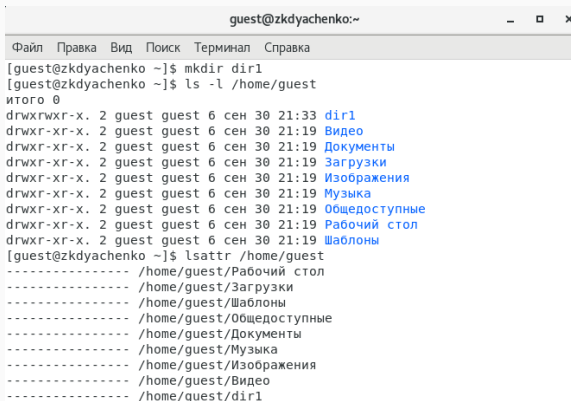
```
guest@zkdyachenko:~  
Файл Правка Вид Поиск Терминал Справка  
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42:./var/lib/gdm:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
gnome-initial-setup:x:989:983:./run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89:./var/spool/postfix:/sbin/nologin  
ntp:x:38:38:./etc/ntp:/sbin/nologin  
tcpdump:x:72:72:./sbin/nologin  
zkdyachenko:x:1000:1000:zkdyachenko:/home/zkdyachenko:/bin/bash  
vboxadd:x:988:1:./var/run/vboxadd:/bin/false  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@zkdyachenko ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:./home/guest:/bin/bash  
[guest@zkdyachenko ~]$ ls -l /home/  
итого 8  
drwx-----. 15 guest      guest      4096 сен 30 21:19 guest  
drwx-----. 15 zkdyachenko zkdyachenko 4096 сен 30 20:57 zkdyachenko  
[guest@zkdyachenko ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/zkdyachenko  
----- /home/guest  
[guest@zkdyachenko ~]$
```

Figure 7: Просмотр расширенных атрибутов

Задачи выполнения лабораторной работы

Создать в домашней директории поддиректорию dir1.

Определить, какие права и атрибуты были выставлены (рис. -fig. 8)



```
guest@zkdyachenko:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@zkdyachenko ~]$ mkdir dir1  
[guest@zkdyachenko ~]$ ls -l /home/guest  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 30 21:33 dir1  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Видео  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Документы  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Загрузки  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Изображения  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Музыка  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Общедоступные  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Рабочий стол  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Шаблоны  
[guest@zkdyachenko ~]$ lsattr /home/guest  
----- /home/guest/Рабочий стол  
----- /home/guest/Загрузки  
----- /home/guest/Шаблоны  
----- /home/guest/Общедоступные  
----- /home/guest/Документы  
----- /home/guest/Музыка  
----- /home/guest/Изображения  
----- /home/guest/Видео  
----- /home/guest/dir1
```

Figure 8: Новая директория

Задачи выполнения лабораторной работы

Снять с директории dir1 все атрибуты (рис. -fig. 9).
Попытаться создать файл (рис. -fig. 10).

```
[guest@zkdyachenko ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 30 21:33 dir1
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Видео
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Документы
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Изображения
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Музыка
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Шаблоны
[guest@zkdyachenko ~]$
```

Figure 9: Проверка работы команды `chmod 000 dir1`

Задачи выполнения лабораторной работы

```
[guest@zkdyachenko ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@zkdyachenko ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@zkdyachenko ~]$
```

Figure 10: Попытка создать файл

Задачи выполнения лабораторной работы

Выполняя действия от имени владельца директории (файлов) (рис. -fig. 11), определить опытным путём, какие операции разрешены, а какие нет и заполнить на основе этого Таблицу 1.

```
[guest@zkdyachenko ~]$ chmod 200 dir1/fileb
[guest@zkdyachenko ~]$ chmod 000 dir1
[guest@zkdyachenko ~]$ touch dir1/file1
touch: невозможно выполнить touch для «dir1/file1»: Отказано в доступе
[guest@zkdyachenko ~]$ rm dir1/fileb
rm: невозможно удалить «dir1/fileb»: Отказано в доступе
[guest@zkdyachenko ~]$ echo "text" > dir1/fileb
bash: dir1/fileb: Отказано в доступе
[guest@zkdyachenko ~]$ cat dir1/fileb
cat: dir1/fileb: Отказано в доступе
[guest@zkdyachenko ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@zkdyachenko ~]$ ls dir1
ls: невозможно открыть каталог dir1: Отказано в доступе
[guest@zkdyachenko ~]$ mv dir1/fileb dir1/filebb
mv: не удалось получить доступ к «dir1/filebb»: Отказано в доступе
[guest@zkdyachenko ~]$ chmod 200 dir1/fileb
chmod: невозможно получить доступ к «dir1/fileb»: Отказано в доступе
```

Figure 11: Процесс проверки

Задачи выполнения лабораторной работы

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)	-	-	-	-	-	-	-	-
d-----	(100)	-	-	-	-	-	-	-	-
d-----	(200)	-	-	-	-	-	-	-	-
d-----	(300)	-	-	-	-	-	-	-	-
d-----	(400)	-	-	-	-	-	-	-	-
d-----	(500)	-	-	-	-	-	-	-	-
d-----	(600)	-	-	-	-	-	-	-	-
d-----	(700)	-	-	-	-	-	-	-	-
d--x----	(000)	-	-	-	-	+	-	-	+
d--x----	(100)	-	-	-	-	+	-	-	+
d--x----	(200)	-	-	+	-	+	-	-	+
d--x----	(300)	-	-	+	-	+	-	-	+
d--x----	(400)	-	-	-	+	+	-	-	+
d--x----	(500)	-	-	-	+	+	-	-	+
d--x----	(600)	-	-	+	+	+	-	-	+
d--x----	(700)	-	-	+	+	+	-	-	+

Figure 12: Таблица 1

Задачи выполнения лабораторной работы

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-----	(000)	-	-	-	-	-	-	-	-
d-w-----	(100)	-	-	-	-	-	-	-	-
d-w-----	(200)	-	-	-	-	-	-	-	-
d-w-----	(300)	-	-	-	-	-	-	-	-
d-w-----	(400)	-	-	-	-	-	-	-	-
d-w-----	(500)	-	-	-	-	-	-	-	-
d-w-----	(600)	-	-	-	-	-	-	-	-
d-w-----	(700)	-	-	-	-	-	-	-	-
d-wx-----	(000)	+	+	-	-	+	-	+	+
d-wx-----	(100)	+	+	-	-	+	-	+	+
d-wx-----	(200)	+	+	+	-	+	-	+	+
d-wx-----	(300)	+	+	+	-	+	-	+	+
d-wx-----	(400)	+	+	-	+	+	-	+	+
d-wx-----	(500)	+	+	-	+	+	-	+	+
d-wx-----	(600)	+	+	+	+	+	-	+	+
d-wx-----	(700)	+	+	+	+	+	-	+	+

Figure 13: Таблица 1

Задачи выполнения лабораторной работы

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
<small>chmod</small> dr-----	(000)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-----	(100)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-----	(200)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-----	(300)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-----	(400)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-----	(500)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-----	(600)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-----	(700)	-	-	-	-	-	-	-	-
<small>chmod</small> dr-x-----	(000)	-	-	-	-	+	+	-	+
<small>chmod</small> dr-x-----	(100)	-	-	-	-	+	+	-	+
<small>chmod</small> dr-x-----	(200)	-	-	+	-	+	+	-	+
<small>chmod</small> dr-x-----	(300)	-	-	+	-	+	+	-	+
<small>chmod</small> dr-x-----	(400)	-	-	-	+	+	+	-	+
<small>chmod</small> dr-x-----	(500)	-	-	--	+	+	+	-	+
<small>chmod</small> dr-x-----	(600)	-	-	+	+	+	+	-	+
<small>chmod</small> dr-x-----	(700)	-	-	+	+	+	+	-	+

Figure 14: Таблица 1

Задачи выполнения лабораторной работы

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
<u>drw</u> -----	(000)	-	-	-	-	-	-	-	-
<u>drw</u> -----	(100)	-	-	-	-	-	-	-	-
<u>drw</u> -----	(200)	-	-	-	-	-	-	-	-
<u>drw</u> -----	(300)	-	-	-	-	-	-	-	-
<u>drw</u> -----	(400)	-	-	-	-	-	-	-	-
<u>drw</u> -----	(500)	-	-	-	-	-	-	-	-
<u>drw</u> -----	(600)	-	-	-	-	-	-	-	-
<u>drw</u> -----	(700)	-	-	-	-	-	-	-	-
<u>drwx</u> -----	(000)	+	+	-	-	+	+	+	+
<u>drwx</u> -----	(100)	+	+	-	-	+	+	+	+
<u>drwx</u> -----	(200)	+	+	+	-	+	+	+	+
<u>drwx</u> -----	(300)	+	+	+	-	+	+	+	+
<u>drwx</u> -----	(400)	+	+	-	+	+	+	+	+
<u>drwx</u> -----	(500)	+	+	-	+	+	+	+	+
<u>drwx</u> -----	(600)	+	+	+	+	+	+	+	+
<u>drwx</u> -----	(700)	+	+	+	+	+	+	+	+

Figure 15: Таблица 1

Задачи выполнения лабораторной работы

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1 и заполнила Таблицу 2 (рис. -fig. 16)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx-----	-----
Удаление файла	d-wx-----	-----
Чтение файла	d--x-----	-r-----
Запись в файл	d--x-----	--w-----
Переименование файла	d-wx-----	-----
Создание поддиректории	d-wx-----	-----
Удаление поддиректории	d-wx-----	-----
Смена директории	d--x-----	-----
Просмотр файлов в директории и смена атрибутов файла	dr-x-----	-----

Figure 16: Таблица 2

Результаты выполнения лабораторной работы

Результатом выполнения работы стали заполненные опытным путем таблицы, которые отражают проделанную мной работу. Кроме того, были приобретены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.