

Отчет по лабораторной работе №2

Дисциплина: Информационная безопасность

Выполнила Дяченко Злата Константиновна, НФИбд-03-18

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Шаг 1	6
3.2	Шаг 2	7
3.3	Шаг 3	7
3.4	Шаг 3	8
3.5	Шаг 4	9
3.6	Шаг 5	10
3.7	Шаг 6	11
3.8	Шаг 7	12
3.9	Шаг 8	13
3.10	Шаг 9	13
3.11	Шаг 10	14
3.12	Шаг 11	16
4	Выводы	18

List of Figures

3.1	Создание пользователя и пароля	6
3.2	Определение домашней директории	7
3.3	Выполнение команды <code>whoami</code>	8
3.4	Выполнение команд <code>id</code> и <code>groups</code>	9
3.5	Просмотр файла <code>/etc/passwd</code>	10
3.6	Существующие поддиректории	11
3.7	Просмотр расширенных атрибутов	12
3.8	Новая директория	13
3.9	Проверка работы команды <code>chmod 000 dir1</code>	13
3.10	Попытка создать файл	14
3.11	Процесс проверки	14
3.12	Таблица 1	15
3.13	Таблица 1	15
3.14	Таблица 1	16
3.15	Таблица 1	16
3.16	Таблица 2	17

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.

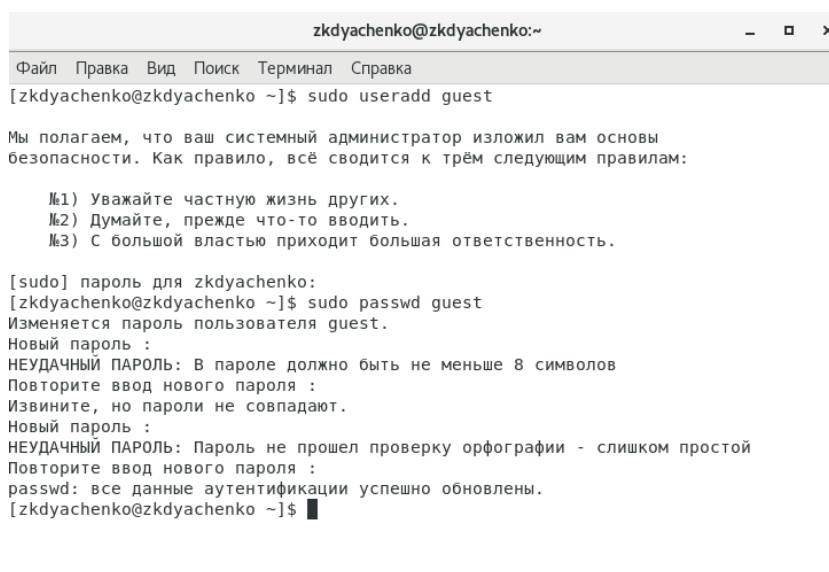
2 Задание

Выполнить все пункты из файла с указаниями к данной лабораторной работе.

3 Выполнение лабораторной работы

3.1 Шаг 1

В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest и задала пароль для этого пользователя, что видно на Рисунке 1 (рис. -fig. 3.1)

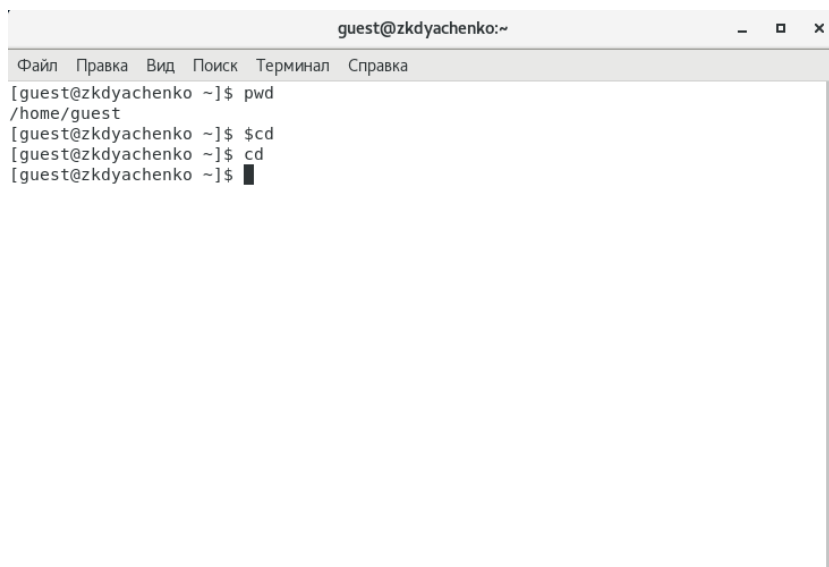


```
zkdyachenko@zkdyachenko:~  
Файл Правка Вид Поиск Терминал Справка  
[zkdyachenko@zkdyachenko ~]$ sudo useradd guest  
  
Мы полагаем, что ваш системный администратор изложил вам основы безопасности. Как правило, всё сводится к трём следующим правилам:  
  
№1) Уважайте частную жизнь других.  
№2) 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 3.1: Создание пользователя и пароля

3.2 Шаг 2

Вошла в систему от имени пользователя `guest` и определила директорию, в которой нахожусь, командой `pwd` (рис. -fig. 3.2). Вывод совпадает с приглашением командной строки до знака `@`. При попытке зайти в домашнюю директорию с помощью команды `cd` (рис. -fig. 3.2), изменений не происходит. Значит, мы уже находимся в домашней директории.



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

Figure 3.2: Определение домашней директории

3.3 Шаг 3

Уточнила имя пользователя командой `whoami` (рис. -fig. 3.3)

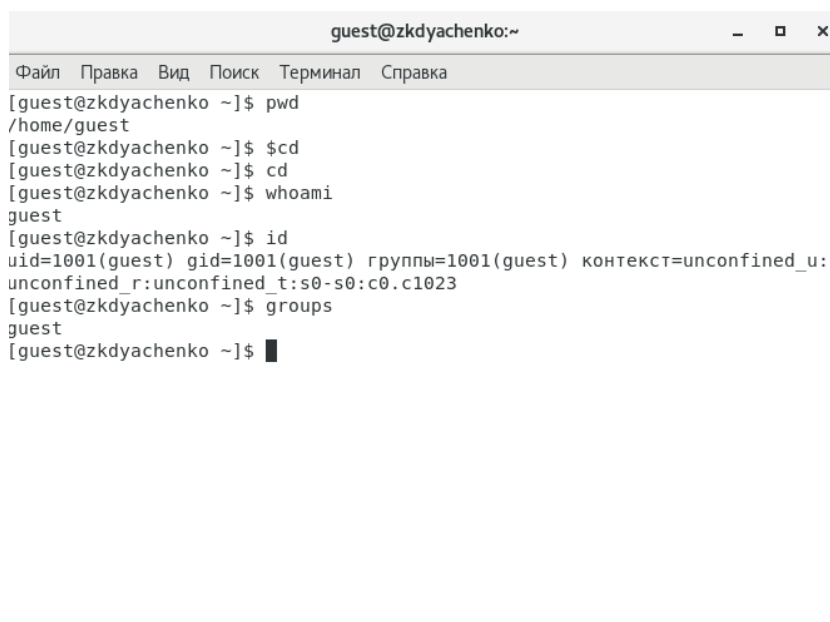
A screenshot of a terminal window titled 'guest@zkdyachenko:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the following commands and output:

```
[guest@zkdyachenko ~]$ pwd
/home/guest
[guest@zkdyachenko ~]$ $cd
[guest@zkdyachenko ~]$ cd
[guest@zkdyachenko ~]$ whoami
guest
[guest@zkdyachenko ~]$
```

Figure 3.3: Выполнение команды `whoami`

3.4 Шаг 3

С помощью команды *id* уточнила имя пользователя, его группу, а также группы, куда входит пользователь с помощью команд *id* и *groups*. Команда *groups* вывела лишь название группы, куда входит пользователь, которое совпадает с названием группы, выведенным командой *id* (рис. -fig. 3.4). Выведенное командой *id* имя пользователя совпадает с приглашением командной строки до знака `@` - именно там и указывается имя пользователя, а после знака `@` - имя машины.



```
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) группы=1001(guest) контекст=unconfined_u:  
unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@zkdyachenko ~]$ groups  
guest  
[guest@zkdyachenko ~]$
```

Figure 3.4: Выполнение команд id и groups

3.5 Шаг 4

Просмотрела файл */etc/passwd* командой *cat /etc/passwd* и нашла в нём свою учётную запись. Для вывода лишь строки с информацией о пользователе *guest* использовала программу *grep* (рис. -fig. 3.5). Записанные в этом файле значения *uid* и *gid* пользователя совпадают с полученными на предыдущем шаге. (рис. -fig. 3.5)

```
guest@zkdychenko:~$ cat /etc/passwd
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
sane: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
zkdychenko:x:1000:1000:zkdychenko:/home/zkdychenko:/bin/bash
vboxadd:x:988:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@zkdychenko ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/home/guest:/bin/bash
[guest@zkdychenko ~]$
```

Figure 3.5: Просмотр файла /etc/passwd

3.6 Шаг 5

Определила существующие в системе директории командой `ls -l /home/` (рис. -fig. 3.6). Удалось получить список поддиректорий директории /home и увидеть, какие права установлены на директориях. Только у владельцев этих директорий есть права на чтение, изменение и вход в соответствующие директории.

```
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/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 ~]$ █
```

Figure 3.6: Существующие поддиректории

3.7 Шаг 6

Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой `lsattr /home` (рис. -fig. 3.7). Удалось увидеть расширенные атрибуты директории данного пользователя - их нет, но не директорий других пользователей - отказано в доступе.

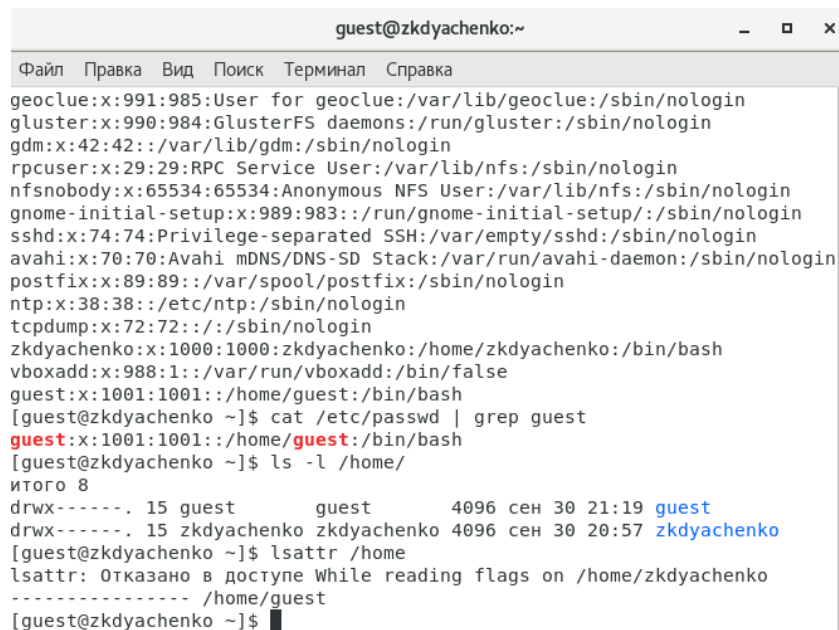
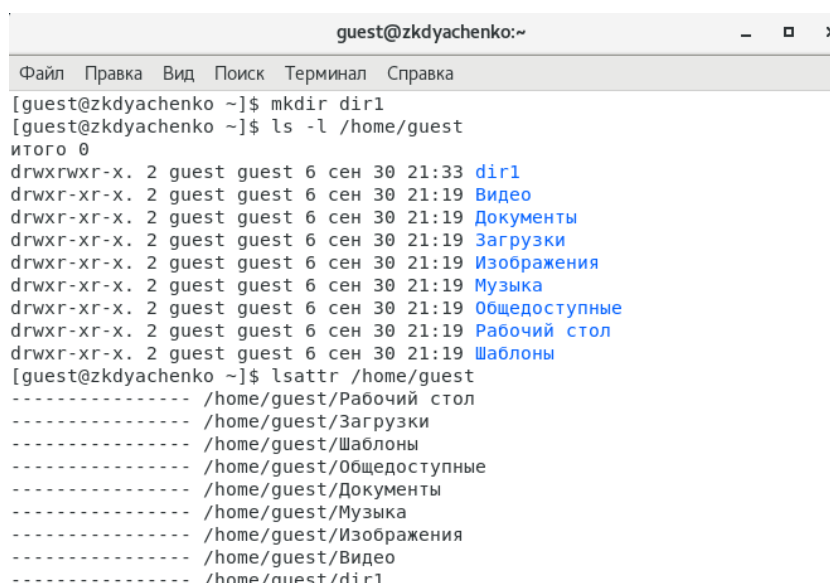
A terminal window titled 'guest@zkdyachenko:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal output lists system users like geoclue, gluster, gdm, rpcuser, nfsnobody, gnome-initial-setup, sshd, avahi, postfix, ntp, tcpdump, and regular users zkdyachenko, vboxadd, guest. It then shows the command 'cat /etc/passwd | grep guest' and 'ls -l /home/' which displays permissions for the 'guest' user's home directory. The permissions are 'drwx-----' for the user 'guest' and 'drwx-----' for the user 'zkdyachenko'. The output also shows the date '4096 сен 30 21:19' and '4096 сен 30 20:57'. The terminal ends with the command 'lsattr /home/' and its output 'lsattr: Отказано в доступе While reading flags on /home/zkdyachenko'.

Figure 3.7: Просмотр расширенных атрибутов

3.8 Шаг 7

Создала в домашней директории поддиректорию dir1. Определила, что на эту директорию были выставлены права доступа drwxrwxr-x: у владельца папки и группы есть права на чтение, изменение и вход в директорию, у остальных есть права только на чтение и вход - изменять директорию они не смогут. Расширенные атрибуты для директории dir1 отсутствуют. (рис. -fig. 3.8)

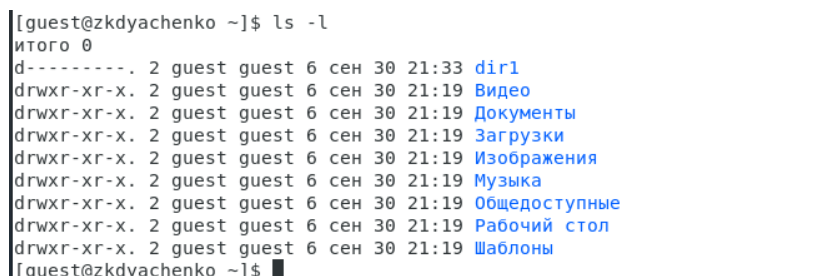


```
guest@zkdyachenko:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@zkdyachenko ~]$ mkdir dir1  
[guest@zkdyachenko ~]$ ls -l /home/guest  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 30 21:33 dir1  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Видео  
drwxr-xr-x. 2 guest guest 6 сен 30 21:19 Документы  
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 3.8: Новая директория

3.9 Шаг 8

Сняла с директории `dir1` все атрибуты и проверьте правильность выполнения команды с помощью `ls -l` (рис. -fig. 3.9)



```
[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 3.9: Проверка работы команды `chmod 000 dir1`

3.10 Шаг 9

Попыталась создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`, но получила отказ в выполнении операции по созданию файла (рис. -fig. 3.10), так как нет прав на изменение данной директории.

Проверить командой `ls -l /home/guest/dir1` действительно ли файл `file1` не находится внутри директории `dir1` невозможно, так как у нас нет прав на вход в директорию и просмотр содержимого.

```
[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 3.10: Попытка создать файл

3.11 Шаг 10

Выполняя действия от имени владельца директории (файлов) (рис. -fig. 3.11), определила опытным путём, какие операции разрешены, а какие нет и заполнила на основе этого Таблицу 1 (рис. -fig. 3.12 - рис. -fig. 3.15).

```
[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 3.11: Процесс проверки

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 3.12: Таблица 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-----	(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 3.13: Таблица 1

Права директор ии	Права файла	Создан ие файла	Удале ние файла	Зап ись в фа йл	Чтение файла	Смена дирек тории	Просмот р файлов в директор ии	Переимен ование файла	Смена атрибутов файла
dr-----	(000)	-	-	-	-	-	-	-	-
dr-----	(100)	-	-	-	-	-	-	-	-
dr-----	(200)	-	-	-	-	-	-	-	-
dr-----	(300)	-	-	-	-	-	-	-	-
dr-----	(400)	-	-	-	-	-	-	-	-
dr-----	(500)	-	-	-	-	-	-	-	-
dr-----	(600)	-	-	-	-	-	-	-	-
dr-----	(700)	-	-	-	-	-	-	-	-
dr-x-----	(000)	-	-	-	-	+	+	-	+
dr-x-----	(100)	-	-	-	-	+	+	-	+
dr-x-----	(200)	-	-	+	-	+	+	-	+
dr-x-----	(300)	-	-	+	-	+	+	-	+
dr-x-----	(400)	-	-	-	+	+	+	-	+
dr-x-----	(500)	-	-	-	+	+	+	-	+
dr-x-----	(600)	-	-	+	+	+	+	-	+
dr-x-----	(700)	-	-	+	+	+	+	-	+

Figure 3.14: Таблица 1

Права директор ии	Права файла	Создан ие файла	Удале ние файла	Зап ись в фа йл	Чтение файла	Смена дирек тории	Просмот р файлов в директор ии	Переимен ование файла	Смена атрибутов файла
drw-----	(000)	-	-	-	-	-	-	-	-
drw-----	(100)	-	-	-	-	-	-	-	-
drw-----	(200)	-	-	-	-	-	-	-	-
drw-----	(300)	-	-	-	-	-	-	-	-
drw-----	(400)	-	-	-	-	-	-	-	-
drw-----	(500)	-	-	-	-	-	-	-	-
drw-----	(600)	-	-	-	-	-	-	-	-
drw-----	(700)	-	-	-	-	-	-	-	-
drwx-----	(000)	+	+	-	-	+	+	+	+
drwx-----	(100)	+	+	-	-	+	+	+	+
drwx-----	(200)	+	+	+	-	+	+	+	+
drwx-----	(300)	+	+	+	-	+	+	+	+
drwx-----	(400)	+	+	-	+	+	+	+	+
drwx-----	(500)	+	+	-	+	+	+	+	+
drwx-----	(600)	+	+	+	+	+	+	+	+
drwx-----	(700)	+	+	+	+	+	+	+	+

Figure 3.15: Таблица 1

3.12 Шаг 11

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1 и заполнила Таблицу 2 (рис. -fig. 3.16)

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 3.16: Таблица 2

4 Выводы

Я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux, опытным путем выяснила минимальные права на директорию и файлы для совершения операций. Результаты работы находятся в репозитории на GitHub, а также есть скринкаст выполнения лабораторной работы.