

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Калинина Кристина Сергеевна

Содержание

Цель работы	5
Теоретические сведения	6
Выполнение лабораторной работы	8
Выводы	15
Список литературы	16

List of Figures

0.1	Создание учетной записи пользователя guest	8
0.2	Вход под пользователем guest	9
0.3	Использование команды pwd	9
0.4	Использование команды whoami	9
0.5	Использование команд id и groups	10
0.6	Просмотр файла '/etc/passwd'	10
0.7	Просмотр директорий и их прав	11
0.8	Просмотр расширенных атрибутов	11
0.9	Создание dir1	12
0.10	Смена прав dir1	12
0.11	Безуспешная попытка создать файл в dir1	13
0.12	Таблица «Установленные права и разрешённые действия»	13
0.13	Таблица “Минимальные права для совершения операций”	14

List of Tables

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.

Теоретические сведения

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ. *discretion* — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. [1]

Для каждого файла в Linux задается набор разрешений. Разрешения могут быть следующими:

- `r` — `read` — возможность открытия и чтения файла. Для директории это возможность просматривать содержимое директории.
- `w` — `write` — возможность изменения файла. Для директории это возможность добавлять, удалять или переименовывать файлы в директории.
- `x` — `execute` — возможность выполнения файла (запуска файла). [2]

Набор разрешений состоит из 3 блоков `rwX`:

- Первый блок `rwX` определяет права доступа для владельца-пользователя.

- Второй блок `gwx` определяет права доступа для владельца-группы.
- Третий блок `gwx` определяет права доступа для всех остальных. [2]

Для каждого файла или директории в Linux задаются права доступа. Они задаются тремя атрибутами: набором разрешений, именем владельца, именем группы.

Набор разрешений — это три блока прав доступа: права доступа для владельца файла, права доступа для группы, права доступа для всех остальных.

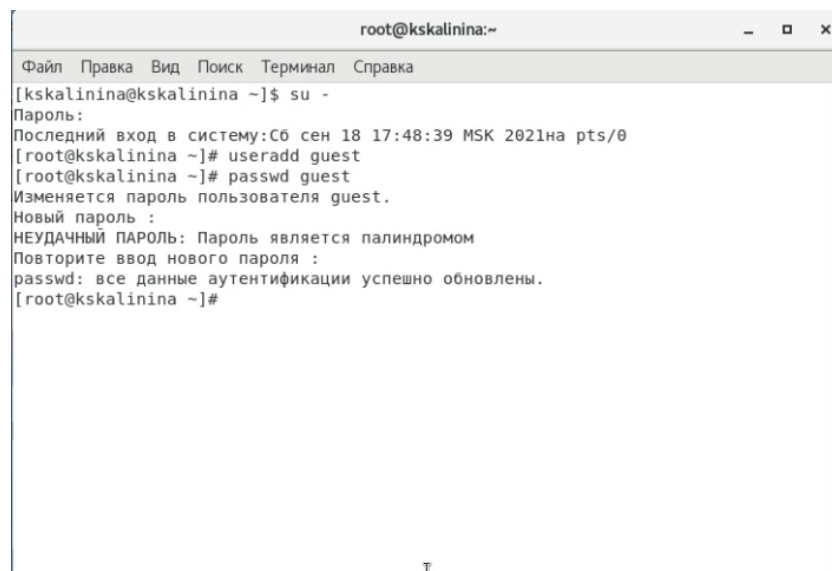
Разрешения записываются символами `r`, `w`, `x`.

Набор разрешений состоит из трех блоков и записывается в виде трех `gwx`, записанных друг за другом в виде одного «слова».

Если какая-либо возможность отключена (запрещена), то вместо соответствующего символа в наборе разрешений ставится прочерк (символ минус). [2]

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest, а также задала для этого пользователя пароль (fig. 0.1).

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

```
[kskalinina@kskalinina ~]$ su -
Пароль:
Последний вход в систему:Сб сен 18 17:48:39 MSK 2021на pts/0
[root@kskalinina ~]# useradd guest
[root@kskalinina ~]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@kskalinina ~]#
```

Figure 0.1: Создание учетной записи пользователя guest

2. Вошла в систему от имени пользователя guest (fig. 0.2).

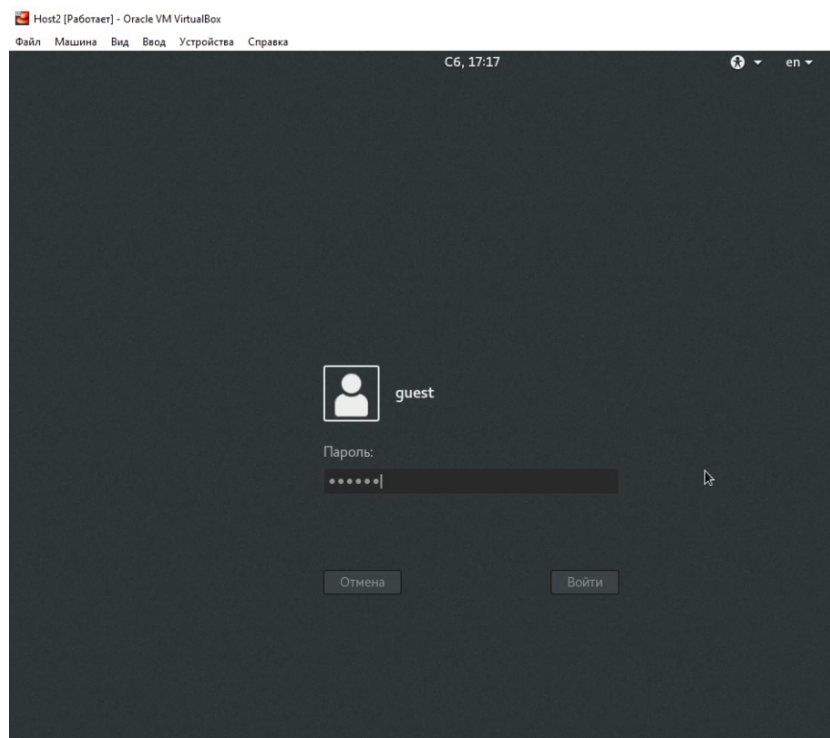


Figure 0.2: Вход под пользователем guest

3. Определите директорию, в которой я нахожусь, командой `pwd`. С помощью этой команды я убедилась, что нахожусь в домашней директории пользователя (fig. 0.3).

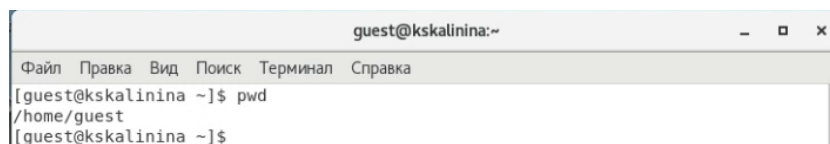


Figure 0.3: Использование команды `pwd`

4. Уточнила имя пользователя командой `whoami` (fig. 0.4).

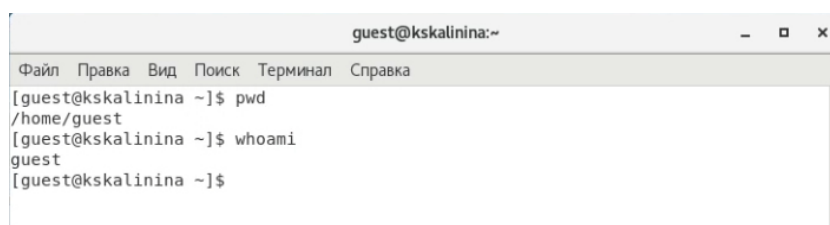
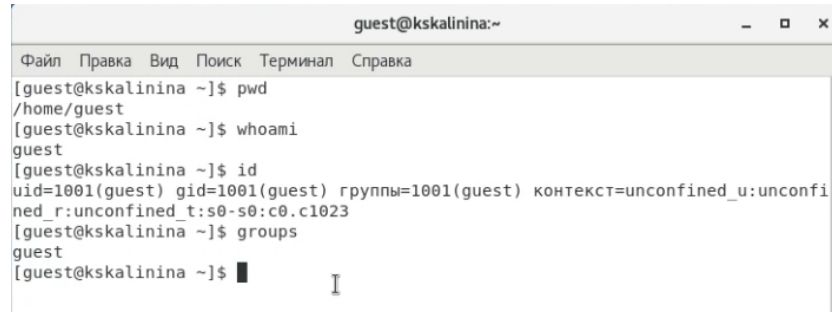


Figure 0.4: Использование команды `whoami`

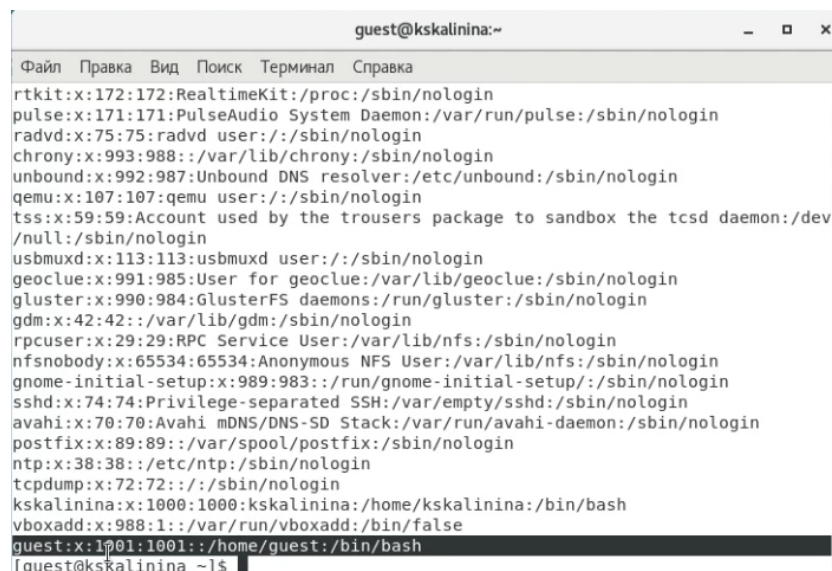
5. Уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Затем воспользовалась командой `groups`, которая дополнительно обозначила домашнюю директорию (fig. 0.5).



```
guest@kskalinina:~  
[guest@kskalinina ~]$ pwd  
/home/guest  
[guest@kskalinina ~]$ whoami  
guest  
[guest@kskalinina ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@kskalinina ~]$ groups  
guest  
[guest@kskalinina ~]$
```

Figure 0.5: Использование команд `id` и `groups`

6. Просмотрела файл `/etc/passwd` командой `cat /etc/passwd` (fig. 0.6). Нашла в нём свою учётную запись, где увидела выведенные ранее значения `uid`, `gid`.



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

Figure 0.6: Просмотр файла `/etc/passwd`

7. Определила существующие в системе директории (fig. 0.5). Увидела директории моих пользователей, в них пользователь имеет права на чтение, запись и исполнение файлов.

```
guest@kskalinina:~  
Файл Правка Вид Поиск Терминал Справка  
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  
kskalinina:x:1000:1000:kskalinina:/home/kskalinina:/bin/bash  
vboxadd:x:988:1:/:var/run/vboxadd:/bin/false  
guest:x:1001:1001:/:home/guest:/bin/bash  
[guest@kskalinina ~]$ ls -l /home/  
итого 8  
drwx-----. 15 guest      guest      4096 окт  2 17:18 guest  
drwx-----. 15 kskalinina kskalinina 4096 окт  2 17:17 kskalinina  
[guest@kskalinina ~]$
```

Figure 0.7: Просмотр директорий и их прав

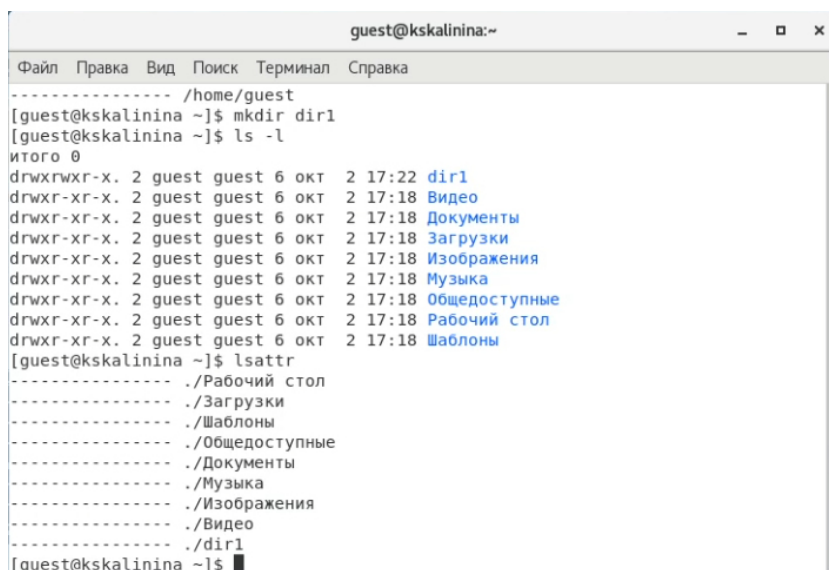
8. Просмотрела, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории '/home'. Увидела, что расширенных атрибутов на поддиректориях моего пользователя нет. Второго пользователя просмотреть не могу (fig. 0.8).

```
guest@kskalinina:~  
Файл Правка Вид Поиск Терминал Справка  
/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  
kskalinina:x:1000:1000:kskalinina:/home/kskalinina:/bin/bash  
vboxadd:x:988:1:/:var/run/vboxadd:/bin/false  
guest:x:1001:1001:/:home/guest:/bin/bash  
[guest@kskalinina ~]$ ls -l /home/  
итого 8  
drwx-----. 15 guest      guest      4096 окт  2 17:18 guest  
drwx-----. 15 kskalinina kskalinina 4096 окт  2 17:17 kskalinina  
[guest@kskalinina ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/kskalinina  
----- /home/guest  
[guest@kskalinina ~]$
```

Figure 0.8: Просмотр расширенных атрибутов

9. Создала в домашней директории поддиректорию dir1. Определила, что она

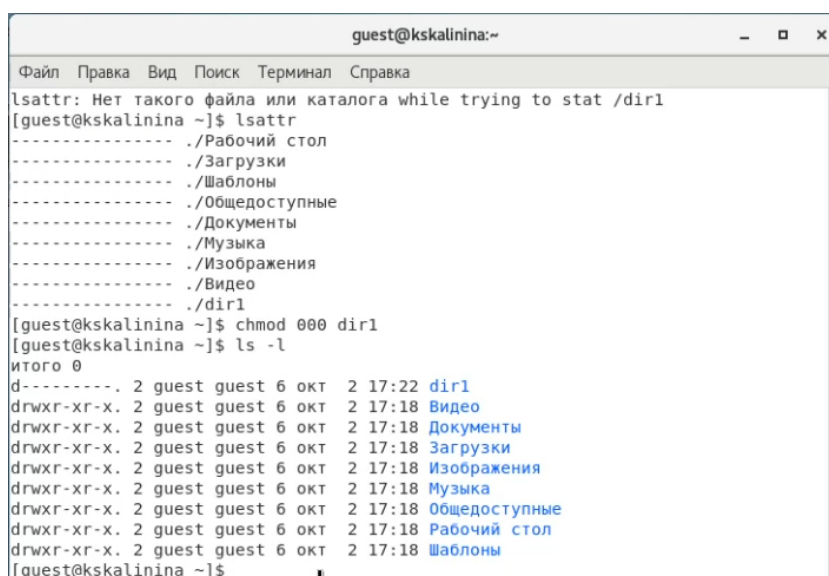
получила права 775, а также не получила расширенных атрибутов (fig. 0.9).



```
guest@kskalinina:~  
Файл Правка Вид Поиск Терминал Справка  
----- /home/guest  
[guest@kskalinina ~]$ mkdir dir1  
[guest@kskalinina ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 окт 2 17:22 dir1  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Видео  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Документы  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Загрузки  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Изображения  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Музыка  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Общедоступные  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Рабочий стол  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Шаблоны  
[guest@kskalinina ~]$ lsattr  
----- ./Рабочий стол  
----- ./Загрузки  
----- ./Шаблоны  
----- ./Общедоступные  
----- ./Документы  
----- ./Музыка  
----- ./Изображения  
----- ./Видео  
----- ./dir1  
[guest@kskalinina ~]$
```

Figure 0.9: Создание dir1

10. Сняла с директории dir1 все атрибуты и проверила это (fig. 0.10).



```
guest@kskalinina:~  
Файл Правка Вид Поиск Терминал Справка  
lsattr: Нет такого файла или каталога while trying to stat /dir1  
[guest@kskalinina ~]$ lsattr  
----- ./Рабочий стол  
----- ./Загрузки  
----- ./Шаблоны  
----- ./Общедоступные  
----- ./Документы  
----- ./Музыка  
----- ./Изображения  
----- ./Видео  
----- ./dir1  
[guest@kskalinina ~]$ chmod 000 dir1  
[guest@kskalinina ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 окт 2 17:22 dir1  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Видео  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Документы  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Загрузки  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Изображения  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Музыка  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Общедоступные  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Рабочий стол  
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Шаблоны  
[guest@kskalinina ~]$
```

Figure 0.10: Смена прав dir1

11. Попыталась создать в директории dir1 файл file1, т.к. прав на создание файла у меня не было, я получила отказ (fig. 0.11).

```
[guest@kskalina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
```

Figure 0.11: Безуспешная попытка создать файл в dir1

12. Заполнила таблицу «Установленные права и разрешённые действия» (fig. 0.12).

Для этого я создала в директории 8 файлов с разными правами на каждом. После этого я меняла права dir1 и пробовала взаимодействовать с каждым из этих файлов, также пыталась зайти внутрь папки. Таким образом я проделала необходимые действия с каждым вариантов прав директории и прав файла .

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

Figure 0.12: Таблица «Установленные права и разрешённые действия»

13. На основе полученной информации из таблицы прошлого пункта (fig. 0.12), я смогла определить те или иные минимально необходимые права для выполнения операций внутри директории dir1. Так как в предыдущем пункте не требовалось создавать подкаталог, я дополнительно попробовала создать dir2 внутри dir1 (меняя права dir1) и удалить её (fig. 0.13).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx-----(300)	(000)
Удаление файла	d-wx-----(300)	(000)
Чтение файла	d--x-----(100)	-r------(400)
Запись в файл	d--x-----(100)	--w------(200)
Переименование файла	d-wx-----(300)	(000)
Создание поддиректории	d-wx-----(300)	-
Удаление поддиректории	d-wx-----(300)	-

Figure 0.13: Таблица “Минимальные права для совершения операций”

Выводы

Таким образом я успешно приобрела практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Дискреционное разграничение доступа Linux. // Debianinstall. 2018. URL: <https://debianinstall.ru/diskretсионное-razgranichenie-dostupa-linux/> (дата обращения 02.10.2021).
2. Права доступа к файлам в Linux. // Pingvinus. 2018. URL: <https://pingvinus.ru/note/file-permissions> (дата обращения 02.10.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..