

Лабораторная работа №2: Дискреционное разграничение прав в Linux. Основные атрибуты

дисциплина: Информационная безопасность

Голова Варвара Алексеевна

2021, 02 October

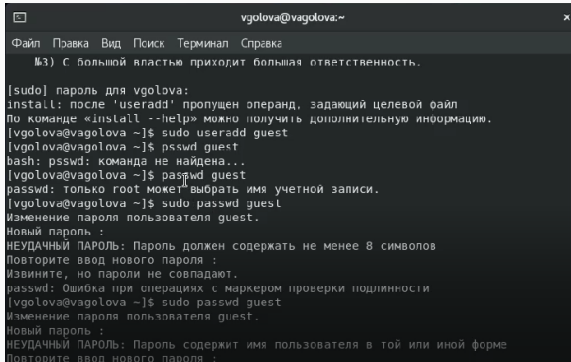
Цель работы

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.

Выполнение работы

Создание учетной записи

В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя `guest` (используя учётную запись администратора): `useradd guest`. Задала пароль для пользователя `guest` (используя учётную запись администратора): `passwd guest`.



```
vagolova@vagolova:~  
Файл Правка Вид Поиск Терминал Справка  
№3) С большой властью приходит большая ответственность.  
  
[sudo] пароль для vagolova:  
install: после 'useradd' пропущен операнд, задающий целевой файл  
по команде «install --help» можно получить дополнительную информацию.  
[vagolova@vagolova ~]$ sudo useradd guest  
[vagolova@vagolova ~]$ passwd guest  
bash: passwd: команда не найдена...  
[vagolova@vagolova ~]$ passwd guest  
passwd: только root может выбрать имя учетной записи.  
[vagolova@vagolova ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов  
Повторите ввод нового пароля :  
Извините, но пароли не совпадают.  
passwd: Ошибка при операциях с маркером проверки подлинности  
[vagolova@vagolova ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль содержит имя пользователя в той или иной форме  
Повторите ввод нового пароля :
```

Вошла в систему от имени пользователя guest.

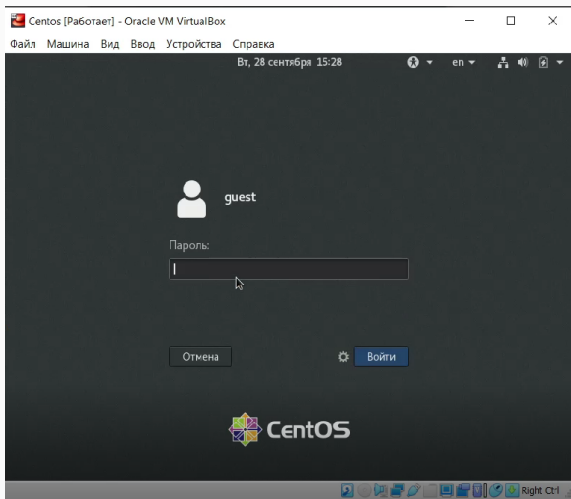


Figure 2: Guest

Определила директорию, в которой я нахожусь, командой `pwd`. Определила, что она является моей домашней директорией.

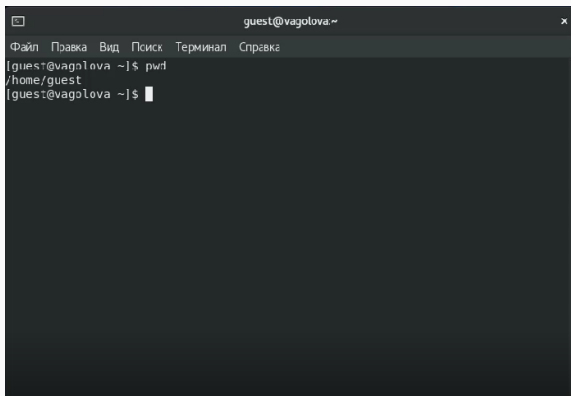
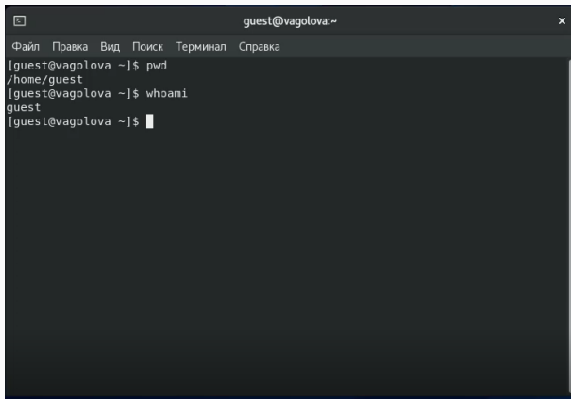
A screenshot of a terminal window titled 'guest@vagolova:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the command 'pwd' being entered and executed, resulting in the output '/home/guest'. The prompt is 'guest@vagolova ~|\$'.

Figure 3: Домашняя директория

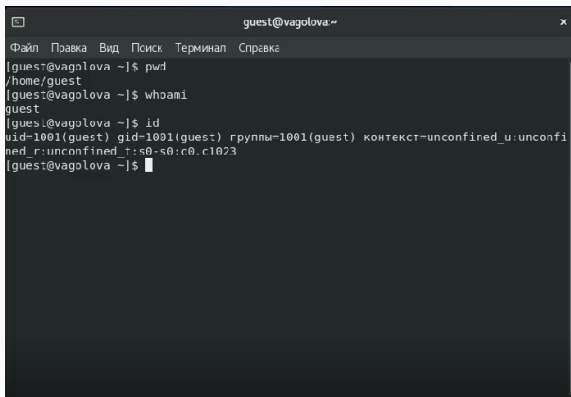
Уточнила имя моего пользователя командой `whoami`.

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

```
[guest@vagalova ~]$ pwd
/home/guest
[guest@vagalova ~]$ whoami
guest
[guest@vagalova ~]$
```

Figure 4: Имя пользователя

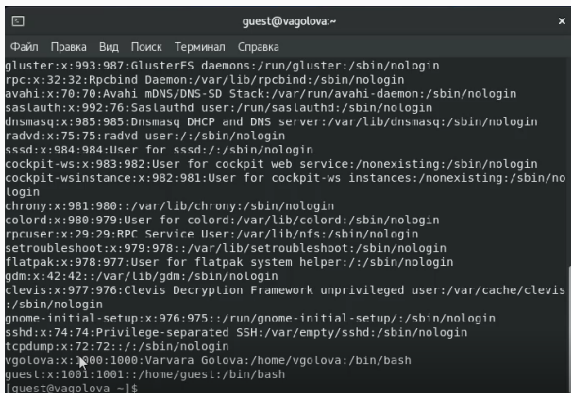
Уточнила имя моего пользователя, его группу, а также группы, куда входит пользователь, командой `id`.

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

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

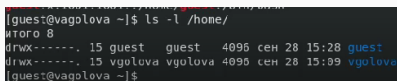
Figure 5: ID

Просмотрела файл `/etc/passwd` командой `cat /etc/passwd`. Нашла в нём свою учётную запись. Определила `uid` пользователя. Определила `gid` пользователя. Сравнила найденные значения с полученными в предыдущих пунктах.

A terminal window titled 'guest@vagolova:~' displays the output of the 'cat /etc/passwd' command. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The output lists system users and regular users with their respective UIDs, GIDs, names, and shell paths.

```
guest@vagolova:~  
Файл Правка Вид Поиск Терминал Справка  
gluster:x:993:987:GlusterFS daemons:/run/gluster:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
sasauth:x:992:76:Sasauthd user:/run/sasauthd:/sbin/nologin  
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
radvd:x:75:75:radvd user:/sbin/nologin  
sssd:x:984:984:User for sssd:/sbin/nologin  
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin  
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin  
chrony:x:981:980:/var/lib/chrony:/sbin/nologin  
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
setroubleshoot:x:979:978:/var/lib/setroubleshoot:/sbin/nologin  
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin  
gnome-initial-setup:x:976:975:/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72:/sbin/nologin  
vagolova:x:1000:1000:Varvara Golova:/home/vagolova:/bin/bash  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@vagolova ~]$
```

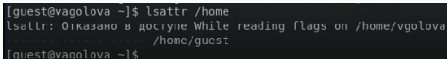
Определила существующие в системе директории командой `ls -l /home/`. Мне удалось получить список поддиректорий директории `/home`.



```
[guest@vago1ova ~]$ ls -l /home/  
итого 8  
drwx-----, 15 guest  guest  4096 сен 28 15:28 guest  
drwx-----, 15 vgo1ova vgo1ova 4096 сен 28 15:09 vgo1ova  
[guest@vago1ova ~]$
```

Figure 7: Дирректории

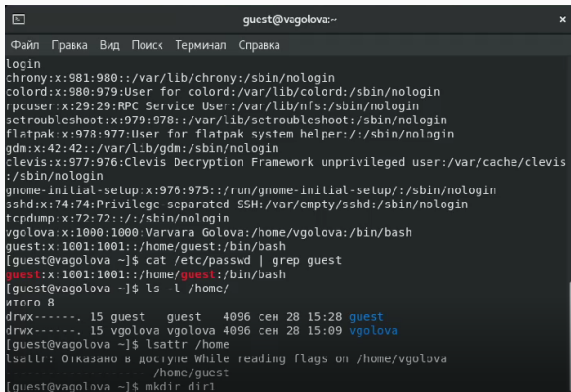
Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Мне не удалось увидеть расширенные атрибуты директории.

A terminal window with a black background and white text. The prompt is [guest@vagolova ~]\$. The command lsattr /home is entered. The output is lsattr: Оказано в доctype While reading flags on /home/vagolova /home/guest. The prompt [guest@vagolova ~]\$ is shown again.

```
[guest@vagolova ~]$ lsattr /home
lsattr: Оказано в доctype While reading flags on /home/vagolova
/home/guest
[guest@vagolova ~]$
```

Figure 8: Расширенные атрибуты

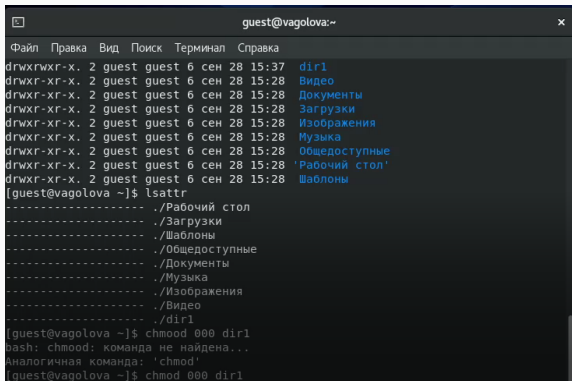
Создала в домашней директории поддиректорию dir1 командой `mkdir dir1`. Определила командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` - 000 000.



```
guest@vagolova:~  
Файл Гравка Вид Поиск Терминал Справка  
login  
chrony:x:981:980::/var/lib/chrony:/sbin/nologin  
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
setroubleshoot:x:979:978::/var/lib/setroubleshoot:/sbin/nologin  
flatpak:x:978:977:User for flatpak system helper:/var/lib/flatpak:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
clevis:x:977:976:clevis decryption framework user:/var/cache/levis  
:/sbin/nologin  
gnome-initial-setup:x:976:975::/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege separated SSH:/var/empty/sshd:/sbin/nologin  
tcpdump:x:72:72::/var/lib/tcpdump:/sbin/nologin  
vgolova:x:1000:1000:Varvara Golova:/home/vgolova:/bin/bash  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@vagolova ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@vagolova ~]$ ls -l /home/  
итого 8  
drwx-----. 15 guest guest 4096 сен 28 15:28 guest  
drwx-----. 15 vgolova vgolova 4096 сен 28 15:09 vgolova  
[guest@vagolova ~]$ lsattr /home  
lsattr: Оказано в доctype while reading flags on /home/vgolova  
/home/guest  
[guest@vagolova ~]$ mkdir dir1
```

Figure 9: Поддиректория

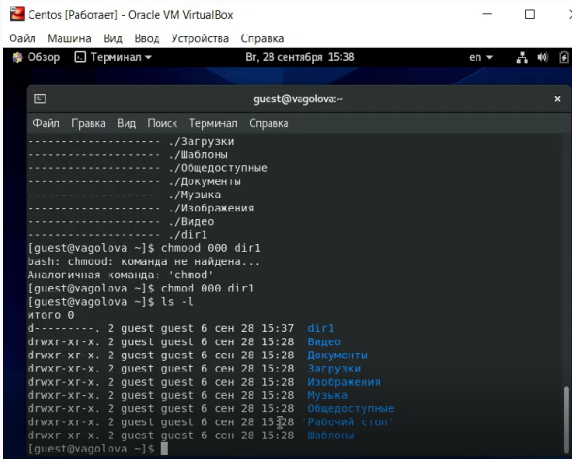
Определила командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` - 000 000.



```
guest@vagolova:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
drwxrwxr-x.  2 guest guest 6 сен 28 15:37  dir1  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  Видео  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  Документы  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  Загрузки  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  Изображения  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  Музыка  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  Общедоступные  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  'Рабочий стол'  
drwxr-xr-x.  2 guest guest 6 сен 28 15:28  Шаблоны  
[guest@vagolova ~]$ lsattr  
----- ./Рабочий стол  
----- ./Загрузки  
----- ./Шаблоны  
----- ./Общедоступные  
----- ./Документы  
----- ./Музыка  
----- ./Изображения  
----- ./Видео  
----- ./dir1  
[guest@vagolova ~]$ chmod 000 dir1  
bash: chmod: команда не найдена...  
Аналогичная команда: 'chmod'  
[guest@vagolova ~]$ chmod 000 dir1
```

Figure 10: Поддиректория

Сняла с директории dir1 все атрибуты командой `chmod 000 dir1` и проверила с её помощью правильность выполнения команды `ls -l`.

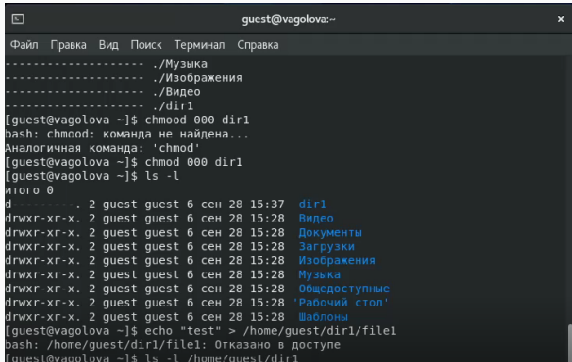


```
Certos [Работаer] - Oracle VM VirtualBox
Оайл Машина Вид Ввод Устройство Справка
Обзор Терминал ▾ Br, 28 сентября 15:38 en [иконки]

guest@vagolova:~
Файл Гравка Вид Поиск Терминал Справка
-----
./Загрузки
./Шаблоны
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1

[guest@vagolova ~]$ chmod 000 dir1
bash: chmod: команда не найдена...
Аналогичная команда: 'chmod'
[guest@vagolova ~]$ chmod 000 dir1
[guest@vagolova ~]$ ls -l
итого 0
d----- 2 guest guest 6 сен 28 15:37 dir1
drwxr-xr-x 2 guest guest 6 сен 28 15:28 Видео
drwxr-xr-x 2 guest guest 6 сен 28 15:28 Документы
drwxr-xr-x 2 guest guest 6 сен 28 15:28 Загрузки
drwxr-xr-x 2 guest guest 6 сен 28 15:28 Изображения
drwxr-xr-x 2 guest guest 6 сен 28 15:28 Музыка
drwxr-xr-x 2 guest guest 6 сен 28 15:28 Общедоступные
drwxr-xr-x 2 guest guest 6 сен 28 15:28 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 сен 28 15:28 Шаблоны
[guest@vagolova ~]$
```

Попыталась создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Я получила отказ в выполнении операции по созданию файла, так как было выявлено несоответствие прав директории. Проверила командой `ls -l /home/guest/dir1` действительно ли файл `file1` не находится внутри директории `dir1`.



```
guest@vagolova: ~  
Файл Гравка Вид Поиск Терминал Справка  
-----  
./Музыка  
./Изображения  
./Видео  
./dir1  
[guest@vagolova ~]$ chmod 000 dir1  
bash: chmod: команда не найдена...  
Аналогичная команда: 'chmod'  
[guest@vagolova ~]$ chmod 000 dir1  
[guest@vagolova ~]$ ls -l  
total 0  
d..... 2 guest guest 6 сен 28 15:37 dir1  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 Видео  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 Документы  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 Загрузки  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 Изображения  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 Музыка  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 Общедоступные  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 'Рабочий стол'  
drwxr-xr-x. 2 guest guest 6 сен 28 15:28 Шаблоны  
[guest@vagolova ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@vagolova ~]$ ls -l /home/guest/dir1
```


Таблица 2.1

Заполнила таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

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(000)	-	-	-	-	-	-	-	-
d-x(100)	d(000)	-	-	-	-	+	-	-	+
d-w(200)	d(000)	+	+	-	-	-	-	-	-
d-wx(300)	d(000)	+	+	-	-	+	-	-	+
dr--(400)	d(000)	-	-	-	-	-	+	-	-
dr-x(500)	d(000)	-	-	-	-	+	+	-	+
drw-(600)	d(000)	+	+	-	-	-	+	-	+
drwx(700)	d(000)	+	+	-	-	+	+	-	+
d(000)	d-x(100)	-	-	-	-	-	-	-	-
d-x(100)	d-x(100)	-	-	-	-	+	-	-	+
d-w(200)	d-x(100)	+	+	-	-	-	-	-	-
d-wx(300)	d-x(100)	+	+	-	-	+	-	-	+
dr--(400)	d-x(100)	-	-	-	-	-	+	-	-
dr-x(500)	d-x(100)	-	-	-	-	+	+	-	+
drw-(600)	d-x(100)	+	+	-	-	-	+	-	-
drwx(700)	d-x(100)	+	+	-	-	+	+	+	+
d(000)	d-w(200)	-	-	+	-	-	-	+	-
d-x(100)	d-w(200)	-	-	+	-	+	-	+	+
d-w(200)	d-w(200)	+	+	-	-	-	-	+	-
d-wx(300)	d-w(200)	+	+	+	-	-	-	+	+
dr--(400)	d-w(200)	-	-	+	-	-	+	+	-
dr-x(500)	d-w(200)	-	-	+	-	+	+	+	+
drw-(600)	d-w(200)	+	+	-	-	-	+	+	-
drwx(700)	d-w(200)	+	+	+	-	+	+	+	+

Таблица 2.1

Заполнила таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

d(000)	d-wx(300)-	-	+	-	-	-	+	-
d-x(100)	d-wx(300)-	-	+	-	+	-	-	+
d-w(200)	d-wx(300)+	+	+	-	-	-	+	-
d-wx(300)	d-wx(300)+	+	+	-	+	-	+	+
dr--(400)	d-wx(300)-	-	+	-	-	+	+	-
dr-x(500)	d-wx(300)-	-	+	-	+	+	+	+
drw-(600)	d-wx(300)+	+	+	-	-	+	+	-
drwx(700)	d-wx(300)+	+	+	-	+	+	+	+
d(000)	dr--(400)-	-	-	+	-	-	-	-
d-x(100)	dr--(400)-	-	-	+	+	-	-	+
d-w(200)	dr--(400)+	+	-	+	-	-	-	-
d-wx(300)	dr--(400)+	+	-	+	+	-	-	+
dr--(400)	dr--(400)-	-	-	+	-	+	-	-
dr-x(500)	dr--(400)-	-	-	+	+	+	-	+
drw-(600)	dr--(400)+	+	-	+	-	+	-	-
drwx(700)	dr--(400)+	+	-	+	+	+	-	+
d(000)	dr-x(500)-	-	-	+	-	-	-	-
d-x(100)	dr-x(500)-	-	-	+	+	-	-	+
d-w(200)	dr-x(500)+	+	-	+	-	-	-	-
d-wx(300)	dr-x(500)+	+	-	+	+	-	-	+
dr--(400)	dr-x(500)-	-	-	+	-	+	-	-
dr-x(500)	dr-x(500)-	-	-	+	+	+	-	+
drw-(600)	dr-x(500)+	+	-	+	-	+	-	-
drwx(700)	dr-x(500)+	+	-	+	+	+	-	+
d(000)	drw-(600)-	-	+	+	-	-	+	-

Figure 14: 2.1

Таблица 2.1

Заполнила таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

d(000)	drw-(600)	-	-	+	+	-	-	+	-
d-x(100)	drw-(600)	-	-	+	+	+	-	+	+
d-w(200)	drw-(600)	+	+	+	+	-	-	+	-
d-wx(300)	drw-(600)	+	+	+	+	-	-	+	+
dr-(400)	drw-(600)	-	-	+	+	-	+	+	-
dr-x(500)	drw-(600)	-	-	+	+	+	+	+	+
drw-(600)	drw-(600)	+	+	+	+	-	-	+	-
drwx(700)	drw-(600)	+	+	+	+	+	+	+	+
d(000)	drwx(700)	-	-	+	+	-	-	+	-
d-x(100)	drwx(700)	-	-	+	+	+	-	+	+
d-w(200)	drwx(700)	+	+	+	+	-	-	+	-
d-wx(300)	drwx(700)	+	+	+	+	+	-	+	+
dr-(400)	drwx(700)	-	-	+	+	-	+	+	-
dr-x(500)	drwx(700)	-	-	+	+	+	+	+	+
drw-(600)	drwx(700)	+	+	+	+	-	-	+	-
drwx(700)	drwx(700)	+	+	+	+	+	+	+	+

Figure 15: 2.1

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполнила табл. 2.2.

2.2

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.