

Отчёт

по лабораторной работе 2

Кочетов Андрей Владимирович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	17

List of Figures

3.1	рис.1. Пользователь и пароль	7
3.2	рис.2. Вход.	8
3.3	рис.3. Директория и пользователь	8
3.4	рис.4. Сравнение команд	9
3.5	рис.5. Сравнение значений	9
3.6	рис.6. Определение поддиректорий	10
3.7	рис.7. Атрибуты	10
3.8	рис.8. Права доступа	11
3.9	рис.9. Атрибуты	11
3.10	рис.10. Снятие атрибутов и проверка	12
3.11	рис.11. Нет доступа	12

List of Tables

1 Цель работы

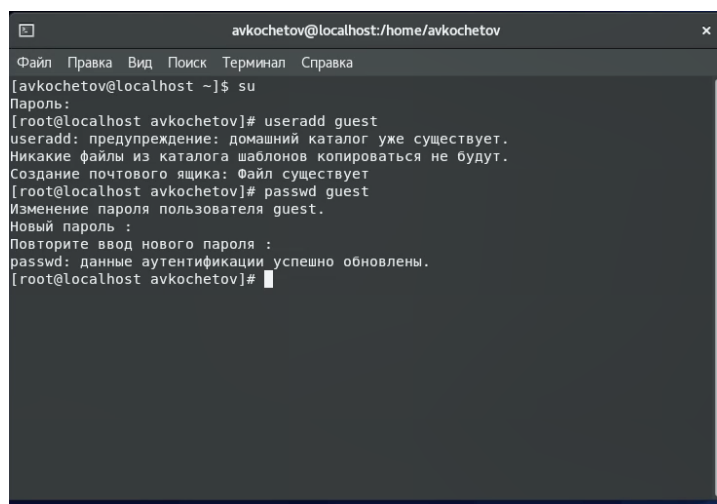
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Задание

Лабораторная работа подразумевает создание нового пользователя, работу с директориями, сравнение пользователей, настройку прав и заполнение таблиц прав.

3 Выполнение лабораторной работы

1. Создаю новую учетную запись guest и задаю к ней пароль(рис.1).

A screenshot of a terminal window titled 'avkochetov@localhost:/home/avkochetov'. The terminal shows the following commands and output:

```
[avkochetov@localhost ~]$ su
Пароль:
[root@localhost avkochetov]# useradd guest
useradd: предупреждение: домашний каталог уже существует.
Никакие файлы из каталога шаблонов копироваться не будут.
Создание почтового ящика: Файл существует
[root@localhost avkochetov]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@localhost avkochetov]#
```

Figure 3.1: рис.1. Пользователь и пароль

2. Захожу в систему под новым пользователем(рис.2).

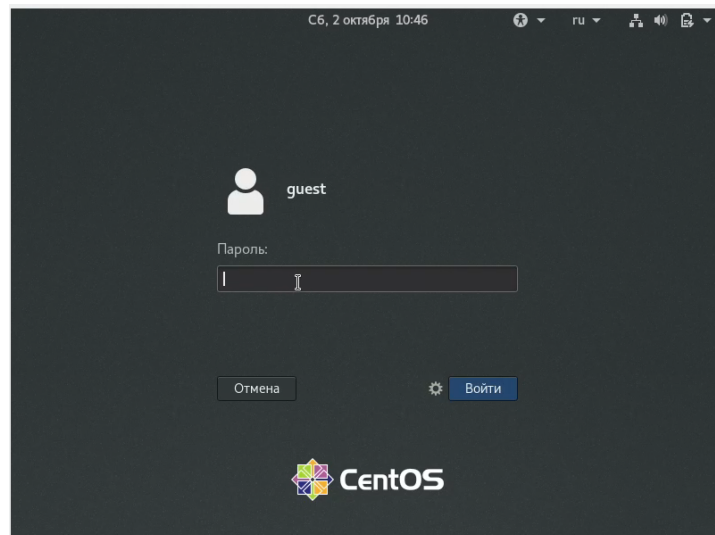


Figure 3.2: рис.2. Вход.

3. Определил директорию при помощи команды `pwd`, убедился, что нахожусь в домашней директории и уточнил имя пользователя командой `whoami`(рис.3).

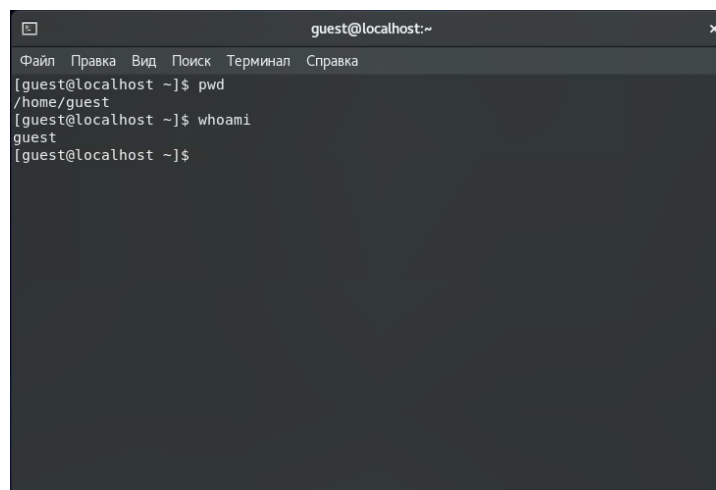
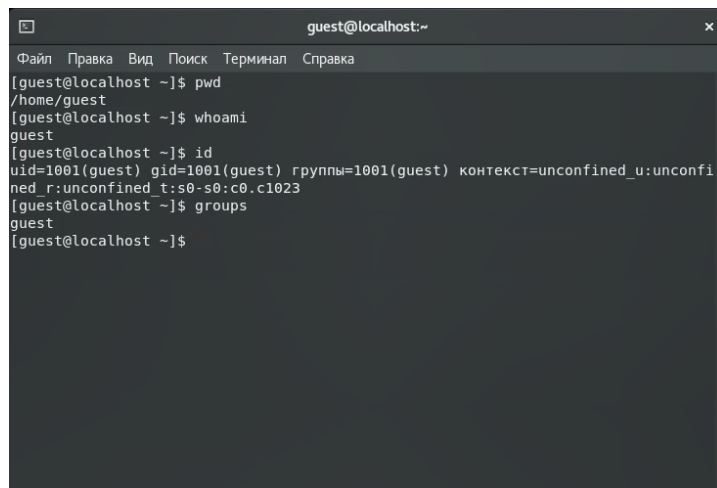


Figure 3.3: рис.3. Директория и пользователь

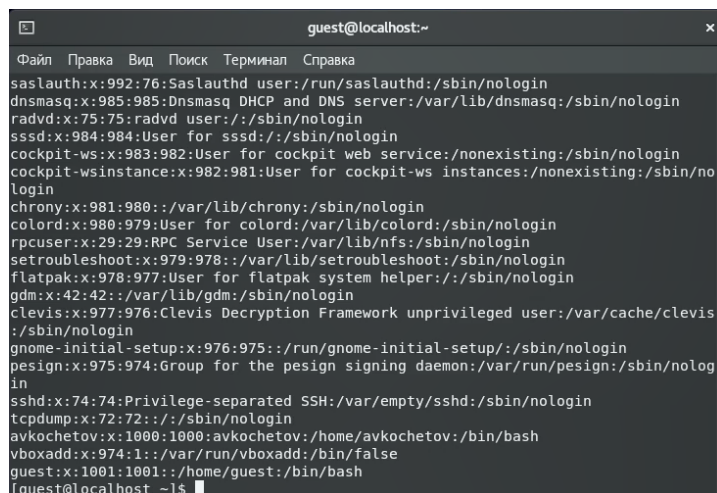
4. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id` и сравнил значения с командой `groups`(рис.4). Команда `groups` выводит те группы, в которых состоит наш пользователь. Сравнил. Можно сделать вывод, что эти команды выдают одинаковые значения.

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

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

Figure 3.4: рис.4. Сравнение команд

5. Просмотрел файл /etc/passwd командой `cat /etc/passwd`(рис.5). Нашел свою учётную запись. Определил uid, gid пользователя. Сравните значения. Они совпадают.

A terminal window titled 'guest@localhost:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal shows the output of the command `cat /etc/passwd`:

```
saslauth:x:992:76:Saslauthd user:/run/saslauthd:/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/levis:/sbin/nologin
gnome-initial-setup:x:976:975:/run/gnome-initial-setup:/sbin/nologin
pesign:x:975:974:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
avkochetov:x:1000:1000:avkochetov:/home/avkochetov:/bin/bash
vboxadd:x:974:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@localhost ~]$
```

Figure 3.5: рис.5. Сравнение значений

6. Определил существующие в системе директории командой `ls -l /home/`(рис.6). Удалось определить существующие поддиректории директории /home. Флаг «d» говорит, что guest и avkochetov – это каталоги. Для обоих каталогов – полные права (rwx).

```

guest@localhost:~
Файл Правка Вид Поиск Терминал Справка
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
pesign:x:975:974:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:./sbin/nologin
avkochetov:x:1000:1000:avkochetov:/home/avkochetov:/bin/bash
vboxadd:x:974:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 15 avkochetov avkochetov 4096 окт  2 10:37 avkochetov
drwx-----. 15 guest      guest      4096 окт  2 10:48 guest
[guest@localhost ~]$

```

Figure 3.6: рис.6. Определение поддиректорий

7. Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой lsattr /home(рис.7). Расширенные атрибуты других пользователей увидеть не удалось, так как недостаточно прав – отказано в доступе.

```

guest@localhost:~
Файл Правка Вид Поиск Терминал Справка
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
pesign:x:975:974:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:./sbin/nologin
avkochetov:x:1000:1000:avkochetov:/home/avkochetov:/bin/bash
vboxadd:x:974:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 15 avkochetov avkochetov 4096 окт  2 10:37 avkochetov
drwx-----. 15 guest      guest      4096 окт  2 10:48 guest
[guest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/avkochetov
----- /home/guest
[guest@localhost ~]$

```

Figure 3.7: рис.7. Атрибуты

8. Создаю в домашней директории поддиректорию dir1 и определяю, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис.8-9).

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
tcpdump:x:72:72:::/sbin/nologin  
avkochevov:x:1000:1000:avkochevov:/home/avkochevov:/bin/bash  
vboxadd:x:974:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@localhost ~]$ ls -l /home/  
итого 8  
drwx----- 15 avkochevov avkochevov 4096 окт 2 10:37 avkochevov  
drwx----- 15 guest guest 4096 окт 2 10:48 guest  
[guest@localhost ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/avkochevov  
----- /home/guest  
[guest@localhost ~]$ mkdir dir1  
[guest@localhost ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 окт 2 10:55 dir1  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Видео  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Документы  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Загрузки  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Изображения  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Музыка  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Общедоступные  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 'Рабочий стол'  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Шаблоны  
[guest@localhost ~]$
```

Figure 3.8: рис.8. Права доступа

```
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Загрузки  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Изображения  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Музыка  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Общедоступные  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 'Рабочий стол'  
drwxr-xr-x. 2 guest guest 6 окт 2 10:47 Шаблоны  
[guest@localhost ~]$ lsattr  
----- ./Рабочий стол  
----- ./Загрузки  
----- ./Шаблоны  
----- ./Общедоступные  
----- ./Документы  
----- ./Музыка  
----- ./Изображения  
----- ./Видео  
----- ./dir1  
[guest@localhost ~]$
```

Figure 3.9: рис.9. Атрибуты

9. Снимаю с директории dir1 все атрибуты командой `chmod 000 dir1` и проверяю с её помощью правильность выполнения команды `ls -l`(рис.10).

```

guest@localhost:~
Файл  Правка  Вид  Поиск  Терминал  Справка
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Шаблоны
[guest@localhost ~]$ lsattr
-----
./Рабочий стол
./Загрузки
./Шаблоны
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d----- 2 guest guest 6 окт  2 10:55 dir1
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Видео
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Документы
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Шаблоны
[guest@localhost ~]$

```

Figure 3.10: рис.10. Снятие атрибутов и проверка

10. Попытался создать в директории dir1 файл file1 и проверить действительно ли он не находится внутри директории dir1(рис.11). Увидел, что не могу производить никакие действия с dir1, потому что ранее снял все атрибуты.

```

guest@localhost:~
Файл  Правка  Вид  Поиск  Терминал  Справка
-----
./Шаблоны
./Общедоступные
./Документы
./Музыка
./Изображения
./Видео
./dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d----- 2 guest guest 6 окт  2 10:55 dir1
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Видео
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Документы
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 10:47 Шаблоны
[guest@localhost ~]$ echo 'test' > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@localhost ~]$

```

Figure 3.11: рис.11. Нет доступа

11. Заполняю таблицу, выполняя действия от имени владельца директории, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Прав-ка дир.	Права файла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние файла	Смена дир.	Про-	Пере-	Смена атр. файла
							смотр фай- лов в дир.	имено- вание файла	
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(000)	(100)	-	-	-	-	-	-	-	-
d(100)	(100)	-	-	-	-	+	-	-	+
d(200)	(100)	-	-	-	-	-	-	-	-
d(300)	(100)	+	+	-	-	+	-	+	+
d(400)	(100)	-	-	-	-	-	+	-	-
d(500)	(100)	-	-	-	-	+	+	-	+
d(600)	(100)	-	-	-	-	-	+	-	-
d(700)	(100)	+	+	-	-	+	+	+	+
d(000)	(200)	-	-	-	-	-	-	-	-
d(100)	(200)	-	-	-	-	+	-	-	+
d(200)	(200)	-	-	-	-	-	-	-	-
d(300)	(200)	+	+	-	-	+	-	+	+
d(400)	(200)	-	-	-	-	-	+	-	-
d(500)	(200)	-	-	-	-	+	+	-	+
d(600)	(200)	-	-	-	-	-	+	-	-
d(700)	(200)	+	+	-	-	+	+	+	+

Прав- ка дир.	Права файла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние файла	Смена дир.	Про-	Пере-	Смена атр. файла
							смотр фай- лов в дир.	имено- вание файла	
d(000)	(300)	-	-	-	-	-	-	-	-
d(100)	(300)	-	-	-	-	+	-	-	+
d(200)	(300)	-	-	-	-	-	-	-	-
d(300)	(300)	+	+	-	-	+	-	+	+
d(400)	(300)	-	-	-	-	-	+	-	-
d(500)	(300)	-	-	-	-	+	+	-	+
d(600)	(300)	-	-	-	-	-	+	-	-
d(700)	(300)	+	+	-	-	+	+	+	+
d(000)	(400)	-	-	-	-	-	-	-	-
d(100)	(400)	-	-	-	+	+	-	-	+
d(200)	(400)	-	-	-	-	-	-	-	-
d(300)	(400)	+	+	-	+	+	-	+	+
d(400)	(400)	-	-	-	-	-	+	-	-
d(500)	(400)	-	-	-	+	+	+	-	+
d(600)	(400)	-	-	-	-	-	+	-	-
d(700)	(400)	+	+	-	+	+	+	+	+
d(000)	(500)	-	-	-	-	-	-	-	-
d(100)	(500)	-	-	-	+	+	-	-	+
d(200)	(500)	-	-	-	-	-	-	-	-
d(300)	(500)	+	+	-	+	+	-	+	+
d(400)	(500)	-	-	-	-	-	+	-	-
d(500)	(500)	-	-	-	+	+	+	-	+
d(600)	(500)	-	-	-	-	-	+	-	-
d(700)	(500)	+	+	-	+	+	+	+	+

Прав- ка дир.	Права файла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние файла	Смена дир.	Про- смотр фай- лов в дир.	Пере- имено- вание файла	Смена атр. файла
d(000)	(600)	-	-	-	-	-	-	-	-
d(100)	(600)	-	-	-	+	+	-	-	+
d(200)	(600)	-	-	-	-	-	-	-	-
d(300)	(600)	+	+	-	+	+	-	+	+
d(400)	(600)	-	-	-	-	-	+	-	-
d(500)	(600)	-	-	-	+	+	+	-	+
d(600)	(600)	-	-	-	-	-	+	-	-
d(700)	(600)	+	+	-	+	+	+	+	+
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(700)	-	-	-	+	+	-	-	+
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(700)	-	-	-	+	+	+	-	+
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(700)	+	+	+	+	+	+	+	+

12. На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	300	000
Удаление файла	300	000
Чтение файла	100	400

Операция	Минимальные права на директорию	Минимальные права на файл
Запись в файл	300	600
Переименование файла	300	000
Создание поддиректории	300	—
Удаление поддиректории	300	—

4 Выводы

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.