

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Ганина Таисия Сергеевна, НКАбд-01-22

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	18
	Список литературы	19

Список иллюстраций

4.1	Новый пользователь guest	9
4.2	Выбор пользователя	9
4.3	Директории	10
4.4	Имя пользователя, группы	10
4.5	cat /etc/passwd	10
4.6	Права директорий	11
4.7	Права директорий	11
4.8	dir1 и ее права	11
4.9	chmod 000	12
4.10	Создание файла, не получилось	12
4.11	Тесты 1	12
4.12	Тесты 2	13
4.13	Тесты 3	13
4.14	Тесты 4	14

Список таблиц

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

1. Работа с атрибутами файлов.
2. Заполнение таблицы 2.1
3. Заполнение таблицы 2.2

3 Теоретическое введение

В основе механизмов разграничения прав доступа лежат имена пользователей и имена групп пользователей. В Linux каждый пользователь имеет уникальное имя, под которым он входит в систему (логинится). Кроме того, в системе создается некоторое число групп пользователей, причем каждый пользователь может быть включен в одну или несколько групп.

Создает и удаляет группы системный администратор (суперпользователь), он же может изменять состав участников той или иной группы. Члены разных групп могут иметь разные права по доступу к файлам Linux.

Права доступа подразделяются на три типа:

- чтение — r (сокращение от read);
- запись — w (сокращение от write);
- выполнение — x (сокращение от execute).

Эти типы прав доступа могут быть предоставлены трем классам пользователей: владельцу файла, группе, в которую входит владелец, и всем (прочим) пользователям. Владельца и группу файла в дальнейшем можно поменять с помощью команд `chown` и `chgrp`.

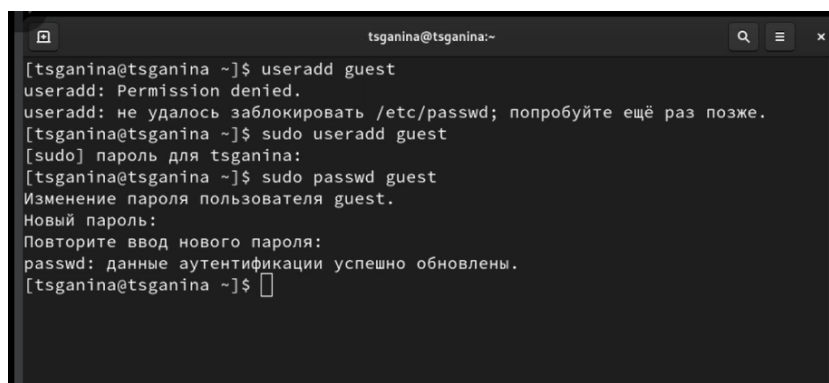
Разрешение на чтение позволяет пользователю читать содержимое файлов, а в случае каталогов — просматривать перечень имен файлов в каталоге (используя, например, команду `ls`).

Разрешение на запись позволяет пользователю писать в файл и изменять его. Для каталогов это дает право создавать в каталоге новые файлы и каталоги, или удалять файлы в этом каталоге.

Разрешение на выполнение позволяет пользователю выполнять файлы (как бинарные программы, так и командные файлы). Разрешение на выполнение применительно к каталогам означает возможность выполнять команды, например, `cd`.

4 Выполнение лабораторной работы

1. Создание нового пользователя, задание пароля (см. рис. 4.1).



```
tsganina@tsganina:~$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[tsganina@tsganina ~]$ sudo useradd guest
[sudo] пароль для tsganina:
[tsganina@tsganina ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[tsganina@tsganina ~]$
```

Рис. 4.1: Новый пользователь guest

2. Переключение на нового пользователя (см. рис. 4.2).

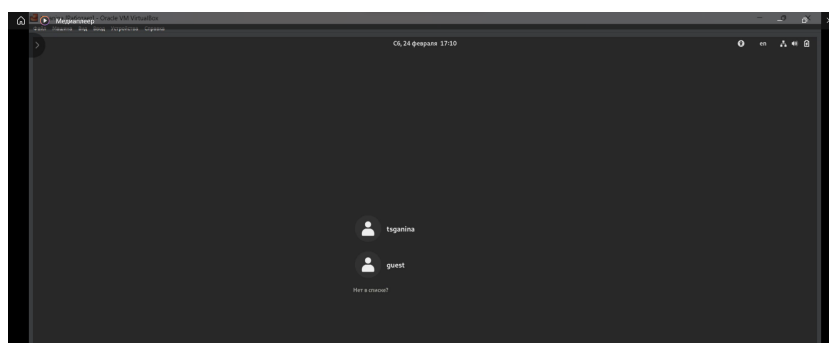
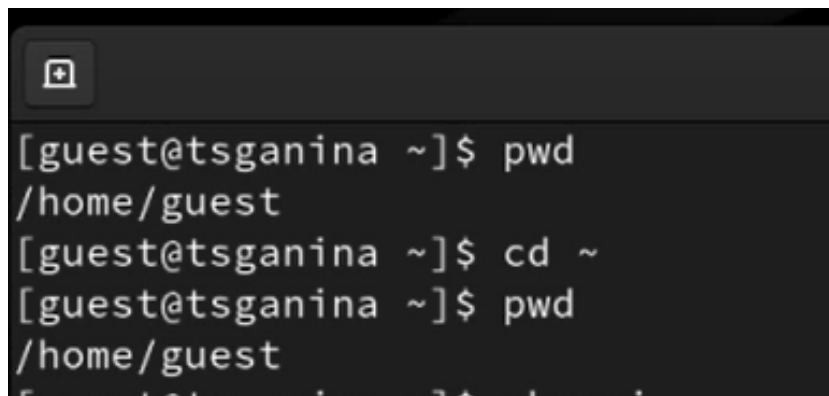


Рис. 4.2: Выбор пользователя

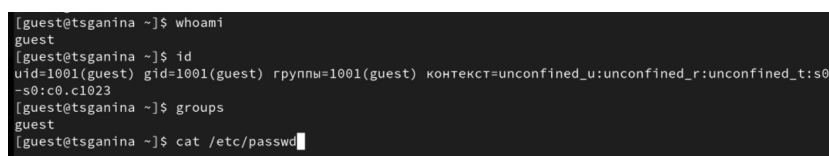
3. Определяю директорию, в которой нахожусь, командой `pwd`. Сравниваю её с приглашением командной строки. Она является домашней директорией (см. рис. 4.3).



```
[guest@tsganina ~]$ pwd
/home/guest
[guest@tsganina ~]$ cd ~
[guest@tsganina ~]$ pwd
/home/guest
```

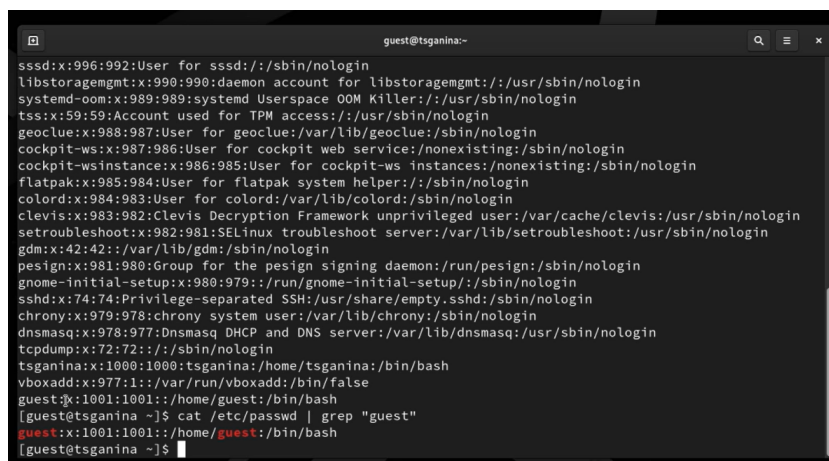
Рис. 4.3: Директории

4. Уточняю имя пользователя, группу, и группы куда входит пользователь. Имя пользователя совпадает с приглашением командной строки. Просматриваю файл `/etc/passwd` командой `cat /etc/passwd`, нахожу там свою учетную запись. (см. рис. 4.4, 4.5).



```
[guest@tsganina ~]$ whoami
guest
[guest@tsganina ~]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0
~s0:c0.c1023
[guest@tsganina ~]$ groups
guest
[guest@tsganina ~]$ cat /etc/passwd
```

Рис. 4.4: Имя пользователя, группы



```
sssd:x:996:992:User for sssd:/usr/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/usr/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/usr/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/usr/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/usr/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/usr/sbin/nologin
clevis:x:983:982:CLEVIS Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/usr/sbin/nologin
design:x:981:980:Group for the design signing daemon:/run/design:/usr/sbin/nologin
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/usr/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/usr/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/usr/sbin/nologin
tsganina:x:1000:1000:tsganina:/home/tsganina:/bin/bash
vboxadd:x:977:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
[guest@tsganina ~]$ cat /etc/passwd | grep "guest"
guest:x:1001:1001:/home/guest:/bin/bash
[guest@tsganina ~]$
```

Рис. 4.5: `cat /etc/passwd`

5. Определяю существующие в системе директории, посмотреть их получилось, права:

- guest: drwx---
- tsganina drwx---

Команда lsattr /home не работает. Увидеть не получилось ни расширенные атрибуты директории, ни расширенные атрибуты директорий других пользователей (см. рис. 4.6, 4.7).

```
[guest@tsganina ~]$ ls -l /home/
итого 8
drwx-----, 14 guest    guest    4096 фев 24 17:11 guest
drwx-----, 16 tsganina tsganina 4096 фев 24 17:10 tsganina
[guest@tsganina ~]$
```

Рис. 4.6: Права директорий

```
[guest@tsganina ~]$ ls -l /home/
итого 8
drwx-----, 14 guest    guest    4096 фев 24 17:11 guest
drwx-----, 16 tsganina tsganina 4096 фев 24 17:10 tsganina
[guest@tsganina ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/tsganina
----- /home/guest
[guest@tsganina ~]$ 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
[guest@tsganina ~]$ mkdir dir1
[guest@tsganina ~]$
```

Рис. 4.7: Права директорий

6. Создаю папку dir1. Определяю права доступа (см. рис. 4.8).

```
----- /home/guest/Видео
[guest@tsganina ~]$ mkdir dir1
[guest@tsganina ~]$ ls -l
итого 8
drwxr-xr-x, 2 guest guest 6 фев 24 17:28 dir1
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 Видео
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 Документы
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 Загрузки
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 Изображения
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 Музыка
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 Общедоступные
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 'Рабочий стол'
drwxr-xr-x, 2 guest guest 6 фев 24 17:11 Шаблоны
[guest@tsganina ~]$
```

Рис. 4.8: dir1 и ее права

7. Снимаю все атрибуты. Проверяю правильность исполнения (см. рис. 4.9).

```
[guest@tsganina ~]$ lsattr /home/guest/dir1
[guest@tsganina ~]$ lsattr /home/guest/dir1
[guest@tsganina ~]$ chmod 000 dir1
[guest@tsganina ~]$ ls -l
иторо 0
d----- 2 guest guest 6 фев 24 17:28 dir1
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Видео
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Документы
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Загрузки
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Изображения
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Музыка
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Общедоступные
drwxr-xr-x 2 guest guest 6 фев 24 17:11 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Шаблоны
[guest@tsganina ~]$
```

Рис. 4.9: chmod 000

8. Пытаюсь создать файл file1. Отказано в доступе, потому что я ранее сняла все атрибуты доступа (см. рис. 4.10).

```
[guest@tsganina ~]$ chmod 000 dir1
[guest@tsganina ~]$ ls -l
иторо 0
d----- 2 guest guest 6 фев 24 17:28 dir1
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Видео
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Документы
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Загрузки
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Изображения
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Музыка
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Общедоступные
drwxr-xr-x 2 guest guest 6 фев 24 17:11 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Шаблоны
[guest@tsganina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@tsganina ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@tsganina ~]$ chmod 700 dir1
[guest@tsganina ~]$ ls -l /home/guest/dir1
иторо 0
[guest@tsganina ~]$
```

Рис. 4.10: Создание файла, не получилось

9. Выполняю тестовые действия для заполнения таблицы.

```
guest@tsganina ~$ ls -l
иторо 0
d----- 2 guest guest 6 фев 24 17:28 dir1
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Видео
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Документы
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Загрузки
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Изображения
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Музыка
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Общедоступные
drwxr-xr-x 2 guest guest 6 фев 24 17:11 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 фев 24 17:11 Шаблоны
[guest@tsganina ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@tsganina ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@tsganina ~]$ chmod 700 dir1
[guest@tsganina ~]$ ls -l /home/guest/dir1
иторо 0
[guest@tsganina ~]$ echo "test" > /home/guest/dir1/file1
[guest@tsganina ~]$ ls -l /home/guest/dir1
иторо 4
-rw-r--r-- 1 guest guest 5 фев 24 18:05 file1
[guest@tsganina ~]$ chmod 000 dir1/file1
[guest@tsganina ~]$ ls -l /home/guest/dir1
иторо 4
----- 1 guest guest 5 фев 24 18:05 file1
[guest@tsganina ~]$ chmod 100 dir1/file1
[guest@tsganina ~]$ ls -l /home/guest/dir1
иторо 4
--x----- 1 guest guest 5 фев 24 18:05 file1
[guest@tsganina ~]$ chmod 200 dir1/file1
[guest@tsganina ~]$ ls -l /home/guest/dir1
иторо 4
--w----- 1 guest guest 5 фев 24 18:05 file1
[guest@tsganina ~]$ ls dir1/
file1
[guest@tsganina ~]$ rm dir1/file1
rm: невозможно удалить 'dir1/file1': Нет такого файла или каталога
[guest@tsganina ~]$ rm -r dir1/
```

Рис. 4.11: Тесты 1

```
gust@totsaganina:~$ rm dir1/file
rm: невозможно удалить 'dir1/file': Нет такого файла или каталога
gust@totsaganina:~$ rm dir1/file
gust@totsaganina:~$ ls dir1
gust@totsaganina:~$ echo "test" > /home/guest/dir1/file
gust@totsaganina:~$ chmod 200 dir1/file
gust@totsaganina:~$ ls dir1
file1
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-rw-r-----. 1 guest guest 5 фев 24 18:08 file1
gust@totsaganina:~$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
gust@totsaganina:~$ chmod 300 dir1/file1
gust@totsaganina:~$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-rwx-----. 1 guest guest 5 фев 24 18:08 /home/guest/dir1/file1
gust@totsaganina:~$ chmod 400 dir1/file1
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-r-----. 1 guest guest 5 фев 24 18:08 file1
gust@totsaganina:~$ cat dir1/file1
test
gust@totsaganina:~$ chmod 500 dir1/file1
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-r-r-----. 1 guest guest 5 фев 24 18:08 file1
gust@totsaganina:~$ cat dir1/file1
test
gust@totsaganina:~$ rm dir1/file1
rm: удалить записанную от записи обычный файл 'dir1/file1'? y
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 0
gust@totsaganina:~$ chmod 200 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Нет такого файла или каталога
```

Рис. 4.12: Тесты 2

```
gust@totsaganina:~$ chmod 200 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Нет такого файла или каталога
gust@totsaganina:~$ echo "test" > /home/guest/dir1/file1
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-rw-r-----. 1 guest guest 5 фев 24 18:11 file1
gust@totsaganina:~$ chmod 600 dir1/file1
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-rwx-----. 1 guest guest 5 фев 24 18:11 file1
gust@totsaganina:~$ chmod 700 dir1/file1
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-rwx-----. 1 guest guest 5 фев 24 18:11 file1
gust@totsaganina:~$ chmod 600 dir1/file1
gust@totsaganina:~$ ls -l /home/guest/dir1
иторо 4
-rw-r-----. 1 guest guest 5 фев 24 18:11 file1
gust@totsaganina:~$ chmod 600 dir1
gust@totsaganina:~$ gedit /home/guest/dir1/file1
** (gedit:85469): WARNING **: 18:16:06.862: Set document metadata failed: Ошибка установки метаданных файла: Отказано в доступе
gust@totsaganina:~$ chmod 100 dir1
gust@totsaganina:~$ gedit /home/guest/dir1/file1
gust@totsaganina:~$ ls -l /home/guest/
иторо 0
drwxr-xr-x. 2 guest guest 6 фев 24 17:11 dir1
drwxr-xr-x. 2 guest guest 6 фев 24 17:11 Документы
drwxr-xr-x. 2 guest guest 6 фев 24 17:11 Заргрузки
drwxr-xr-x. 2 guest guest 6 фев 24 17:11 Избранное
drwxr-xr-x. 2 guest guest 6 фев 24 17:11 Музыка
drwxr-xr-x. 2 guest guest 6 фев 24 17:11 Перегруженные
drwxr-xr-x. 2 guest guest 6 фев 24 17:11 Рабочий стол
gust@totsaganina:~$ cat dir1/file1
***
```

Рис. 4.13: Тесты 3

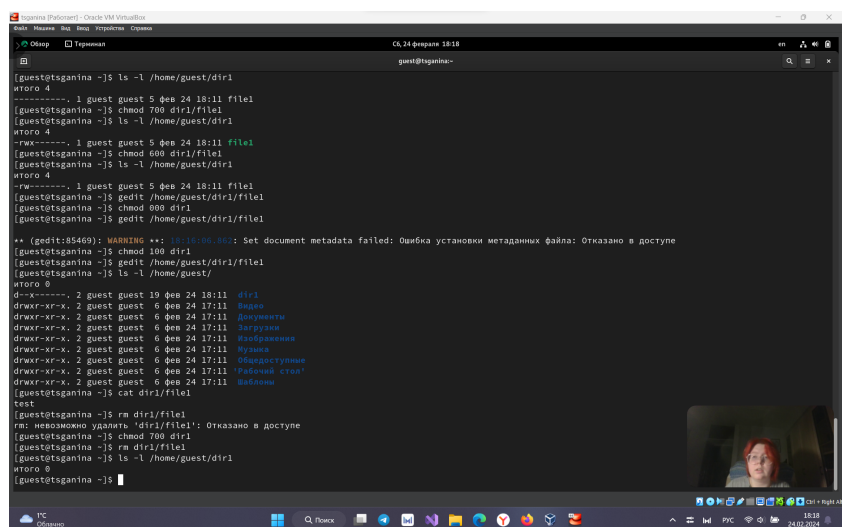


Рис. 4.14: Тесты 4

10. Таблица 2.1.

Права ди- ректо- рии	Права файла	Со- зда- ние файла	Уда- ление файла	За- пись в файл	Чте- ние файла	Сме- на ди- ректо- рии	Про- смотр фай- лов в ди- ректо- рии	Пере- име- нова- ние файла	Сме- на атри- бутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+

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

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

11. Таблица 2.2.

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

5 Выводы

Были получены практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Руководство к лабораторной работе
2. Права доступа Линукс