

Отчёт по лабораторной работе 2

Дискреционное разграничение прав в Linux. Основные атрибуты.

Гебриал Ибрам Есам Зекри НПИ-01-18

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретические сведения	7
4	Выполнение лабораторной работы	11
5	Выводы	24

List of Tables

4.1	Установленные права и разрешённые действия	17
4.2	Минимальные права для совершения операций	23

List of Figures

4.1	Создание учетной записи пользователя guest	11
4.2	Создание пароля	11
4.3	Вход в систему от имени пользователя guest	12
4.4	Определение директории	12
4.5	Имя своего пользователя	12
4.6	Информация пользователя	13
4.7	файл /etc/passwd	13
4.8	Определение существующих в системе директории	14
4.9	Расширенные атрибуты	14
4.10	Создание поддиректорию dir1 и права доступа	15
4.11	Расширенные атрибуты директории dir1	15
4.12	Изменение прав доступа	15
4.13	Попытка создания в директории dir1 файла file1	16
4.14	Попытка проверять директорию	16
4.15	Проверка директории	16

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. Создать учётную запись пользователя guest.
2. Получить практические навыки работы с атрибутами файлов.
3. Закрепить теоретические основы дискреционного разграничения доступа.

3 Теоретические сведения

Атрибуты файлов в Linux - это набор из девяти основных битов. Определяющих какие из пользователей обладают правами на чтение, запись. А также запуск файлов для выполнения. Данный набор формирует код, называемый режимом доступа к файлу/каталогу. Первые три бита определяют права доступа для владельца. Следующие — для группы пользователей, к которой относится файл. и последние три бита — права доступа для всех остальных пользователей в системе.

Как это работает?

Для записи кода режима доступа используется восьмеричная запись чисел. Как уже было отмечено, код доступа содержит три «триады» битов — для пользователя, группы и всех остальных, именно в таком порядке. Битам из первой триады соответствуют значения в восьмеричной записи 400, 200 и 100. Для второй триады (т. е. для группы) — 40, 20 и 10. Наконец, для третьей (все остальные) — 4, 2 и 1. В свою очередь, первому биту в каждой триаде соответствует доступ на чтение (r — «read»). Второму — на запись (w — «write») и третьему — на выполнение, т. е. x — «execute».

В традиционной модели прав доступа UNIX предполагается, что каждый пользователь «заперт» в пределах всего одной категории (триады). Это означает, что для неоднозначной ситуации применяются самые строгие права. Например, право на владение всегда определяется только битами из триады владельца. И никак и никогда группой или другими пользователями.

Установка бита чтения (r) в одной из триад (или во всех) задаёт право открывать данный файл для чтения соответствующим категориям пользователей. Наличие

бита записи (w) позволяет изменять файл. При этом возможно его удаление и/или переименование файла, но только в том случае, если заданы соответствующие биты для его родительского каталога, поскольку именно в его записях хранятся имена файлов.

Команда chmod:

Как и следует из ее имени, команда chmod предназначена для смены атрибутов доступа - чтения, изменения и исполнения. В отношении единичного файла делается это просто:

```
chmod [атрибуты] filename
```

Атрибуты доступа могут устанавливаться с использованием как символьной, так и цифровой нотации (подробнее об этом будет говориться в Intro-цикле). Первый способ - указание, для каких атрибутов принадлежности (хозяина, группы и всех остальных) какие атрибуты доступа задействованы. Атрибуты принадлежности обозначаются символами u (от user) для хозяина файла, g (от group) - для группы, o (от other) для прочих и a (от all) - для всех категорий принадлежности вообще. Атрибуты доступа символизируются литерами r (от read), дающей право чтения, w (от write) - право изменения и x (от execute) - право исполнения.

Атрибуты принадлежности соединяются с атрибутами доступа символами + (присвоение атрибута доступа), - (отъятие атрибута) или = (присвоение только данного атрибута доступа с одновременным отъятием всех остальных). Одновременно в строке можно указать (подряд, без пробелов) более чем один из атрибутов принадлежности и несколько (или все) атрибуты доступа.

Для пояснения сказанного приведу несколько примеров. Так, команда

```
chmod u+w filename
```

установит для хозяина (u - от user) право изменения (w - от write) файла filename, а команда

```
chmod a-x filename
```

отнимет у всех пользователей вообще право его исполнения. В случае, если некоторый атрибут доступа присваивается всем категориям принадлежности,

символ `a` можно опустить. Так, команда

```
chmod +x filename
```

в противоположность предыдущей, присвоит атрибут исполнения файла `filename` всем категориям принадлежности (и хозяину, и группе, и прочим).

С помощью команды

```
chmod go=rx filename
```

можно присвоить группе принадлежности файла `filename` и всем прочим (не хозяину и не группе) право на его чтение и исполнение с одновременным отнятием права изменения.

Наконец, команда `chmod` в состоянии установить и дополнительные атрибуты доступа к файлу, такие, как биты `SUID` и `GUID`, или, скажем, атрибут `sticky` (и о них будет разговор в Intro-цикле). Так, в некоторых системах (например, во `FreeBSD` - в `Linux`-дистрибутивах я с таким не встречался) `XFree86` по умолчанию устанавливается без атрибута суидности на исполнимом файле `X`-сервера. Это влечет за собой невозможность (без специальных `wrapper`'ов) запуска Иксов от лица обычного пользователя. Один из способов борьбы - просто присвоить этому файлу бит суидности:

```
chmod u+s /usr/X11R6/bin/XFree86
```

Приведенные примеры можно многократно умножить, но, думается, их достаточно для понимания принципов работы команды `chmod` с символьной нотацией атрибутов.

Цифровая нотация - еще проще. При ней достаточно указать сумму присваиваемых атрибутов в восьмеричном исчислении (4 - атрибут чтения, 2 - атрибут изменения и 1 - атрибут исполнения; 0 символизирует отсутствие любых атрибутов доступа) для хозяина (первая позиция), группы (вторая позиция) и прочих (третья позиция). Все атрибуты доступа, оставшиеся вне этой суммы, автоматически отнимаются у данного файла. То есть команда

```
chmod 000 filename
```

означает снятие с файла `filename` всех атрибутов доступа для всех категорий

принадлежности (в том числе и хозяина) и эквивалентна команде

```
chmod =rwx filename
```

в символьной нотации. А команда

```
chmod 777 filename
```

напротив, устанавливает для всех полный доступ к файлу filename. Для установки дополнительных атрибутов доступа в численной нотации потребуется указать значение четвертого, старшего, регистра. Так, команда для рассмотренного выше примера - присвоения атрибута суидности исполняемому файлу X-сервера, - в численной нотации будет выглядеть как

```
chmod 4711 /usr/X11R6/bin/XFree86
```

Как и для команд `chown` и `chgrp`, наиболее значимые опции команды `chmod` – `reference` и `-R`. И смысл их - идентичен. Первая устанавливает для файла (файлов) атрибуты доступа, идентичные таковым референсного файла, вторая - распространяет действие команды на все вложенные подкаталоги и входящие в них файлы.

Рекурсивное присвоение атрибутов доступа по образцу требует внимания. Так, если рекурсивно отнять для всего содержимого домашнего каталога атрибут исполнения (а он без соблюдения некоторых условий монтирования автоматом присваивается любым файлам, скопированным с носителей файловой структуры FAT или ISO9660 без расширения RockRidge, что подчас мешает), то тем самым станет невозможным вход в любой из вложенных подкаталогов. Впрочем, в разделе про утилиту `find` будет показан один из способов борьбы с таким безобразием.

4 Выполнение лабораторной работы

1. Создал учётную запись пользователя guest (используя учётную запись администратора): (рис. 4.1)

С помощью команды:

`useradd guest`

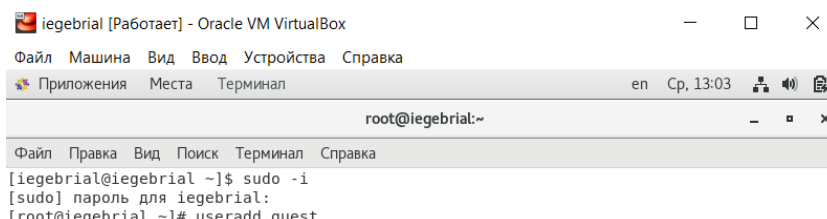


Figure 4.1: Создание учетной записи пользователя guest

2. Задал пароль для пользователя guest: (рис. 4.2)

С помощью команды:

`passwd guest`

```
[root@iegebrial ~]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@iegebrial ~]#
```

Figure 4.2: Создание пароля

3. Вошёл в систему от имени пользователя guest. (рис. 4.3)

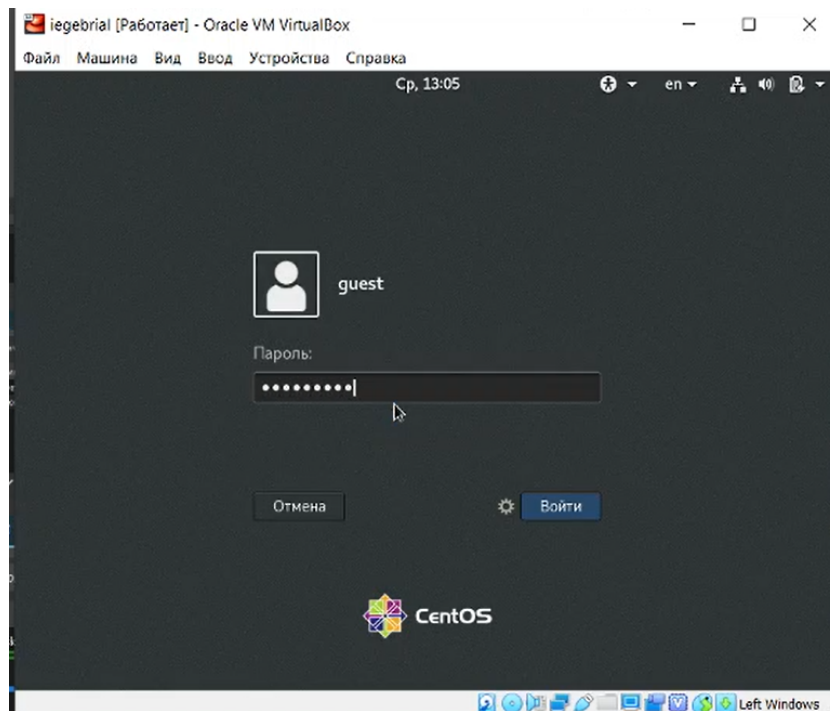


Figure 4.3: Вход в систему от имени пользователя guest

4. Определил директорию, в которой я нахожусь, командой `pwd`. она является своей домашней директорией. (рис. 4.4)

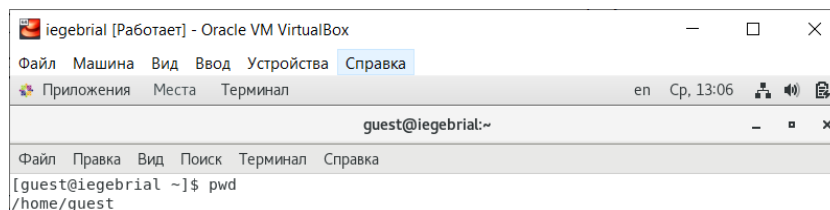


Figure 4.4: Определение директории

5. Уточнил имя своего пользователя командой `whoami`. (рис. 4.5)



Figure 4.5: Имя своего пользователя

6. Уточнил имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните.

Сравнил вывод `id` с выводом команды `groups`. (рис. 4.6)

Команда `id` покажет идентификатор пользователя (`uid`), основную группу пользователя (`gid`) и вторичные группы (`groups`) пользователя.

А команда `groups` распечатает список всех групп, к которым принадлежит текущий зарегистрированный пользователь.

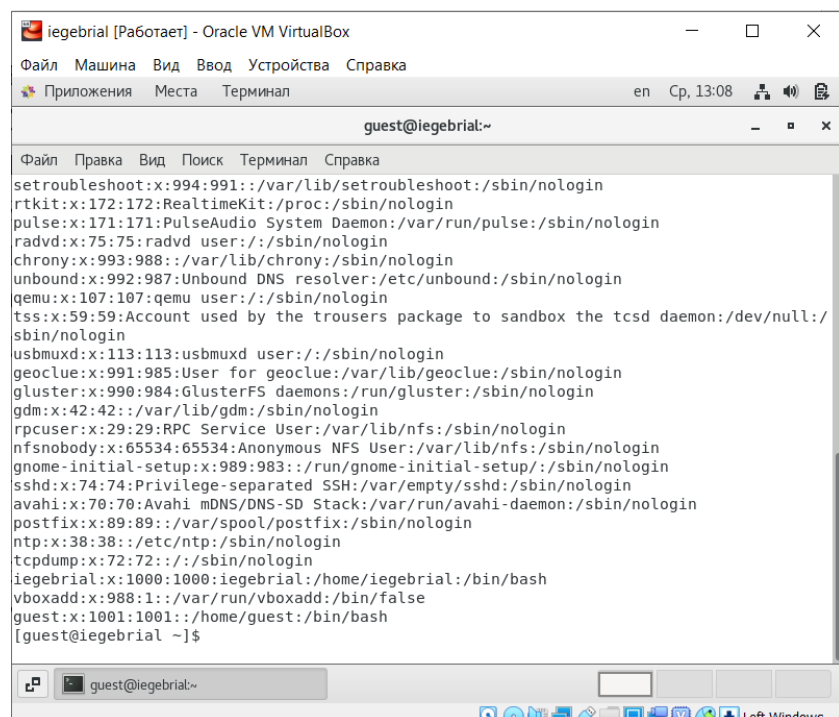
```
[guest@iegebrial ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0.c1023
[guest@iegebrial ~]$ groups
guest
```

Figure 4.6: Информация пользователя

7. Имя пользователя совпадает с именем пользователя в приглашении командной строки.

8. Просмотрел файл `/etc/passwd` командой `cat /etc/passwd`. (рис. 4.7)

Значения `uid` и `gid` пользователя совпадают с их значениями в предыдущих пунктах.



```
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
iegebrial:x:1000:1000:iegebrial:/home/iegebrial:/bin/bash
vboxadd:x:988:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@iegebrial ~]$
```

Figure 4.7: файл `/etc/passwd`

9. Определил существующие в системе директории командой `ls -l /home/` (рис. 4.8)

Нет не удалось мне получить список поддиректорий директории `/home`. На директориях установлены следующие права: r-права на чтение, w-права на запись, x-права на исполнение.

```
vboxadd:x:988:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@iegebrial ~]$
[guest@iegebrial ~]$ ls -l /home/
итого 8
drwx-----. 15 guest      guest      4096 сен 29 13:05 guest
drwx-----. 15 iegebrial iegebrial 4096 сен 29 13:03 iegebrial
```

Figure 4.8: Определение существующих в системе директории

10. Проверил какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home` (рис. 4.9)

Расширенные атрибуты для `guest` не установлены. Не удалось мне увидеть расширенные атрибуты директорий других пользователей.

```
drwx-----. 15 iegebrial iegebrial 4096 сен 29 13:03 iegebrial
[guest@iegebrial ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/iegebrial
----- /home/guest
```

Figure 4.9: Расширенные атрибуты

11. Создал в домашней директории поддиректорию `dir1` командой `mkdir dir1` и определил командами `ls -l` (рис. 4.10)

На директорию `dir1` установлены следующие права: r-права на чтение, w-права на запись, x-права на исполнение для владельца и для основной группы пользователей, а для остальных только чтение и исполнение без права записи.

расширенные атрибуты директории `dir1` `lsattr`. (рис. 4.11)

```
[guest@iegebrial ~]$ mkdir dir1
[guest@iegebrial ~]$ ls -l /home/guest
итого 0
drwxrwxr-x. 2 guest guest 6 сен 29 13:10 dir1
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Видео
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Документы
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Изображения
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Музыка
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Шаблоны
```

Figure 4.10: Создание поддиректории dir1 и права доступа

```
iegebrial [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал en Cp, 13:14
guest@iegebrial:~
Файл Правка Вид Поиск Терминал Справка
[guest@iegebrial ~]$ 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
[guest@iegebrial ~]$
```

Figure 4.11: Расширенные атрибуты директории dir1

12. Снимил с директории dir1 все атрибуты командой `chmod 000 dir1`

и проверил с её помощью правильность выполнения команды `ls -l` (рис. 4.12)

```
[guest@iegebrial ~]$ chmod 000 dir1
[guest@iegebrial ~]$ ls -l
итого 0
d-----. 2 guest guest 6 сен 29 13:10 dir1
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Видео
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Документы
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Изображения
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Музыка
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 Шаблоны
[guest@iegebrial ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@iegebrial ~]$
```

Figure 4.12: Изменение прав доступа

13. Попытался создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` (рис. 4.13)

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

Figure 4.13: Попытка создания в директории dir1 файла file1

Не получилось создать файл в директории dir1 потому что нет прав доступа к директории dir1.

не смогу смотреть `ls -l /home/guest/dir1` так как отключил все права доступа на директорию. (рис. 4.14)

```
drwxr-xr-x. 2 guest guest 6 сен 29 13:05 шаблоны
[guest@iegebrial ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@iegebrial ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
```

Figure 4.14: Попытка проверять директорию

Вернул права доступа пользователю и проверил командой `ls -l /home/guest/dir1` (рис. 4.15)

file1 не находится внутри директории dir1.

```
iegebrial [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  C6, 02:49
guest@iegebrial:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@iegebrial dir1]$ cd
[guest@iegebrial ~]$ ls -l /home/guest/dir1
итого 0
[guest@iegebrial ~]$
```

Figure 4.15: Проверка директории

14. Заполнил таблицу «Установленные права и разрешённые действия» (см. табл. 4.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесил в таблицу знак «+», если не разрешена, знак «-».

Table 4.1: Установленные права и разрешённые действия

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d— (000)	— (000)	-	-	-	-	-	-	-	-
d— (000)	-x (100)	-	-	-	-	-	-	-	-
d— (000)	-w- (200)	-	-	-	-	-	-	-	-
d— (000)	-wx (300)	-	-	-	-	-	-	-	-
d— (000)	r— (400)	-	-	-	-	-	-	-	-
d— (000)	r-x (500)	-	-	-	-	-	-	-	-
d— (000)	rw- (600)	-	-	-	-	-	-	-	-
d— (000)	rwX (700)	-	-	-	-	-	-	-	-
d-x (100)	— (000)	-	-	-	-	+	-	-	+
d-x (100)	-x (100)	-	-	-	-	+	-	-	+
d-x (100)	-w- (200)	-	-	+	-	+	-	-	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-x (100)	-wx (300)	-	-	+	-	+	-	-	+
d-x (100)	r- (400)	-	-	-	+	+	-	-	+
d-x (100)	r-x (500)	-	-	-	+	+	-	-	+
d-x (100)	rw- (600)	-	-	+	+	+	-	-	+
d-x (100)	rwX (700)	-	-	+	+	+	-	-	+
d-w- (200)	— (000)	-	-	-	-	-	-	-	-
d-w- (200)	-x (100)	-	-	-	-	-	-	-	-
d-w- (200)	-w- (200)	-	-	-	-	-	-	-	-
d-w- (200)	-wx (300)	-	-	-	-	-	-	-	-
d-w- (200)	r- (400)	-	-	-	-	-	-	-	-
d-w- (200)	r-x (500)	-	-	-	-	-	-	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-w- (200)	rw- (600)	-	-	-	-	-	-	-	-
d-w- (200)	rwX (700)	-	-	-	-	-	-	-	-
d-wX (300)	— (000)	+	+	-	-	+	-	+	+
d-wX (300)	-X (100)	+	+	-	-	+	-	+	+
d-wX (300)	-w- (200)	+	+	+	-	+	-	+	+
d-wX (300)	-wX (300)	+	+	+	-	+	-	+	+
d-wX (300)	r— (400)	+	+	-	+	+	-	+	+
d-wX (300)	r-X (500)	+	+	-	+	+	-	+	+
d-wX (300)	rw- (600)	+	+	+	+	+	-	+	+
d-wX (300)	rwX (700)	+	+	+	+	+	-	+	+
dr— (400)	— (000)	-	-	-	-	-	+	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
dr-	-x	-	-	-	-	-	+	-	-
(400)	(100)								
dr-	-w-	-	-	-	-	-	+	-	-
(400)	(200)								
dr-	-wx	-	-	-	-	-	+	-	-
(400)	(300)								
dr-	r-	-	-	-	-	-	+	-	-
(400)	(400)								
dr-	r-x	-	-	-	-	-	+	-	-
(400)	(500)								
dr-	rw-	-	-	-	-	-	+	-	-
(400)	(600)								
dr-	rwX	-	-	-	-	-	+	-	-
(400)	(700)								
dr-x	—	-	-	-	-	+	+	-	+
(500)	(000)								
dr-x	-x	-	-	-	-	+	+	-	+
(500)	(100)								
dr-x	-w-	-	-	+	-	+	+	-	+
(500)	(200)								
dr-x	-wx	-	-	+	-	+	+	-	+
(500)	(300)								

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
dr-x (500)	r— (400)	-	-	-	+	+	+	-	+
dr-x (500)	r-x (500)	-	-	-	+	+	+	-	+
dr-x (500)	rw- (600)	-	-	+	+	+	+	-	+
dr-x (500)	rwX (700)	-	-	+	+	+	+	-	+
drw- (600)	— (000)	-	-	-	-	-	+	-	-
drw- (600)	-x (100)	-	-	-	-	-	+	-	-
drw- (600)	-w- (200)	-	-	-	-	-	+	-	-
drw- (600)	-wX (300)	-	-	-	-	-	+	-	-
drw- (600)	r— (400)	-	-	-	-	-	+	-	-
drw- (600)	r-x (500)	-	-	-	-	-	+	-	-
drw- (600)	rw- (600)	-	-	-	-	-	+	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
drw- (600)	rwX (700)	-	-	-	-	-	+	-	-
drwx (700)	— (000)	+	+	-	-	+	+	+	+
drwx (700)	-X (100)	+	+	-	-	+	+	+	+
drwx (700)	-w- (200)	+	+	+	-	+	+	+	+
drwx (700)	-wx (300)	+	+	+	-	+	+	+	+
drwx (700)	r— (400)	+	+	-	+	+	+	+	+
drwx (700)	r-X (500)	+	+	-	+	+	+	+	+
drwx (700)	rw- (600)	+	+	+	+	+	+	+	+
drwx (700)	rwX (700)	+	+	+	+	+			

15. На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните (см. табл. 4.1).

Table 4.2: Минимальные права для совершения операций

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

5 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.