

Лабораторная работа №2

Дисциплина: Информационная безопасность

Боровикова Карина Владимировна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	24
	Список литературы	25

Список иллюстраций

4.1	Создание учетной записи guest	9
4.2	Изменение пароля учетной записи guest	9
4.3	Вход в систему под новым пользователем guest	10
4.4	Домашняя директория пользователя guest	10
4.5	Файл /etc/passwd	11
4.6	Директории в /home/	12
4.7	Расширенные атрибуты поддиректории	12
4.8	Права доступа на директорию	13
4.9	Атрибуты директорий	13
4.10	Изменение прав доступа на dir1	14
4.11	Попытки взаимодействия с каталогом dir1	14
4.12	Проверка возможных действий для прав доступа	15

Список таблиц

4.1	Установленные права и разрешенные действия	16
4.2	Минимальные права для совершения операций	23

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

- Произвести работу в консоли с атрибутами от имени пользователя *guest*;
- Составить опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

3 Теоретическое введение

В данной лабораторной работе нам предстоит поработать с правами доступа файлов и директорий. **Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами.

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

- **r** — read (чтение) — право просматривать содержимое файла;
- **w** — write (запись) — право изменять содержимое файла;
- **x** — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

- **owner** (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но владельцем можно сделать и кого-то другого.
- **group** (группа) — пользователи с общими заданными правами.
- **others** (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами.[01?]

Чтобы увидеть текущие назначения владельца, вы можете использовать команду `ls -l`. Эта команда показывает пользователя и группу-владельца.

С помощью команды `ls` вы можете отобразить владельца файлов в данном каталоге. Иногда может оказаться полезным получить список всех файлов в системе, в которых в качестве владельца указан данный пользователь или группа. Для этого вы можете использовать `find`. Аргумент `find -user` может быть использован для этой цели.

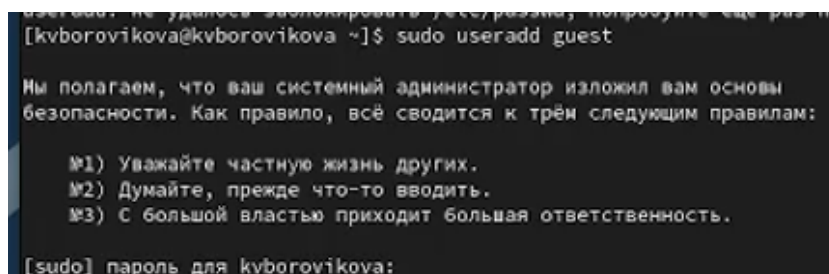
Чтобы применить соответствующие разрешения, первое, что нужно учитывать, это владение. Для этого есть команда `chown`.^[02?]

Для того, чтобы позволить обычным пользователям выполнять программы от имени суперпользователя без знания его пароля была придумана такая вещь, как SUID и SGID биты. Рассмотрим эти полномочия подробнее.

- **SUID** - если этот бит установлен, то при выполнении программы, `id` пользователя, от которого она запущена заменяется на `id` владельца файла. Фактически, это позволяет обычным пользователям запускать программы от имени суперпользователя;
- **SGID** - этот флаг работает аналогичным образом, только разница в том, что пользователь считается членом группы, с которой связан файл, а не групп, к которым он действительно принадлежит. Если SGID флаг установлен на каталог, все файлы, созданные в нем, будут связаны с группой каталога, а не пользователя. Такое поведение используется для организации общих папок;
- **Sticky-bit** - этот бит тоже используется для создания общих папок. Если он установлен, то пользователи могут только создавать, читать и выполнять файлы, но не могут удалять файлы, принадлежащие другим пользователям.

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора) (рис. 4.1): `useradd guest`.



```
useradd: не удалось зашифровать /etc/passwd; попробуйте еще раз не
[kvborovikova@kvborovikova ~]$ sudo useradd guest

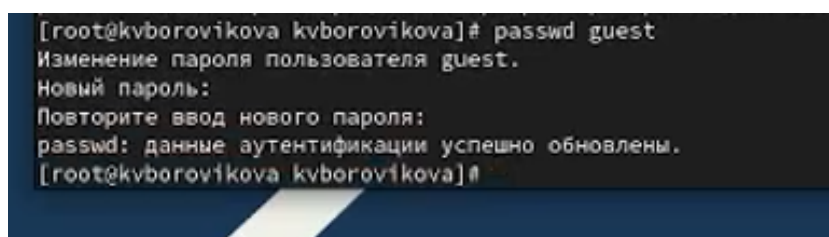
Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

    №1) Уважайте частную жизнь других.
    №2) Думайте, прежде что-то вводить.
    №3) С большой властью приходит большая ответственность.

[sudo] пароль для kvborovikova:
```

Рис. 4.1: Создание учетной записи guest

2. Зададим пароль для пользователя guest (используя учётную запись администратора) (рис. 4.2): `passwd guest`.



```
[root@kvborovikova kvborovikova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@kvborovikova kvborovikova]#
```

Рис. 4.2: Изменение пароля учетной записи guest

3. Перезапустила машину и вошла в систему от имени пользователя guest (рис. 4.3).

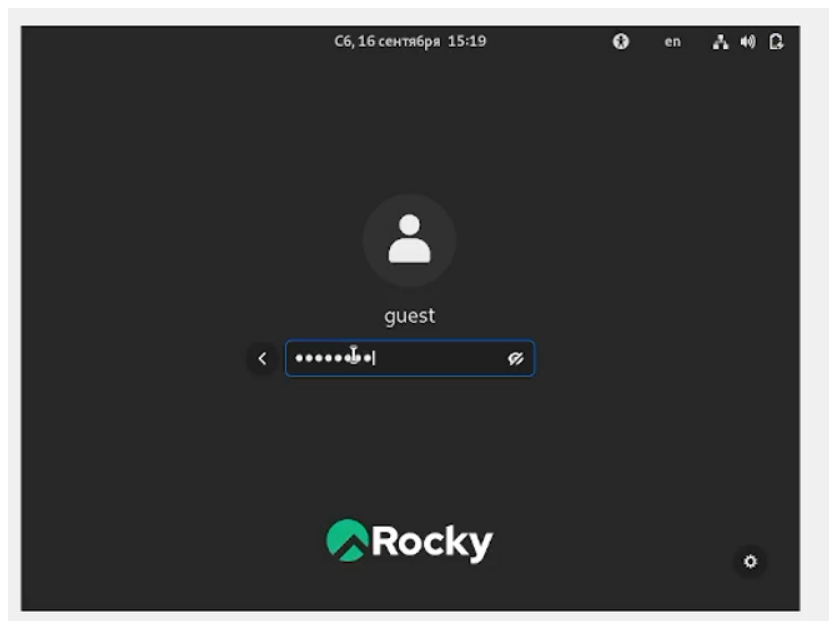


Рис. 4.3: Вход в систему под новым пользователем guest

4. Определим директорию, в которой находимся, командой `pwd`(рис. 4.4). Сравнив её с приглашением командной строки. В командной строке видим символ `~`, что свидетельствует о том, что мы находимся в домашней директории. Определим, является ли она действительно домашней директорией, введя команду `cd`, которая позволяет перейти в домашнюю директорию. Видим, что ничего не меняется. **Мы находимся в своей домашней директории.**

```
guest@kvborovikova:~  
[guest@kvborovikova ~]$ pwd  
/home/guest  
[guest@kvborovikova ~]$ cd  
[guest@kvborovikova ~]$ pwd  
/home/guest  
[guest@kvborovikova ~]$ whoami  
guest  
[guest@kvborovikova ~]$ id  
uid=1001(guest) gid=1001(guest) rpnny=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@kvborovikova ~]$ groups  
guest  
[guest@kvborovikova ~]$ cat /etc/passwd
```

Рис. 4.4: Домашняя директория пользователя guest

5. Уточним имя пользователя командой `whoami` (рис. 4.4). Видим, что имя нашего пользователя - **guest**.

6. Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой `id` (рис. 4.4).

Видим следующие данные: `uid = 1001(guest)`, `gid = 1001(guest)`, `groups = 1001(guest)`.

Сравним вывод `id` с выводом команды `groups` (рис. 4.4).

Данная команда показывает группы текущего пользователя, аналогично выводу команды `id`, группы пользователя `guest` - это группа `guest`.

7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.

Команда `whoami` дала нам понять, что имя пользователя - `guest`. В начале приглашения командной строки как раз указано имя нашего пользователя - все сходится.

8. Просмотрим файл `/etc/passwd` (рис. 4.5):

```
cat /etc/passwd
```

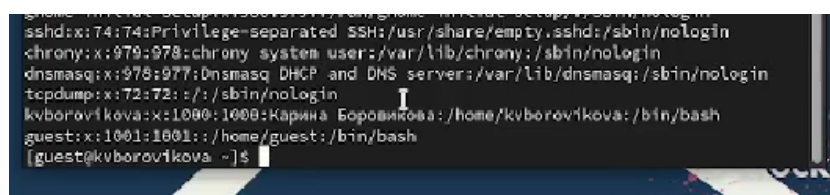


Рис. 4.5: Файл `/etc/passwd`

Найдем в нем последнюю запись - запись о текущем пользователе (выделено на рис. 4.5). Данная строка показывает, что `uid = 1001`, `gid = 1001`, что соответствует результатам предыдущих команд.

9. Определим существующие в системе директории командой `ls -l /home/` (рис. 4.6).

```
guest@x1001-1001: /home/ guest: /bin/bash
[guest@kvborovikova ~]$ ls -l /home
итого 8
drwx-----, 14 guest      guest      4096 сен 16 15:19 guest
drwx-----, 14 kvborovikova kvborovikova 4096 сен 16 15:19 kvborovikova
[guest@kvborovikova ~]$ ls -l /home/
итого 8
drwx-----, 14 guest      guest      4096 сен 16 15:19 guest
drwx-----, 14 kvborovikova kvborovikova 4096 сен 16 15:19 kvborovikova
[guest@kvborovikova ~]$
```

Рис. 4.6: Директории в /home/

Нам удалось получить список поддиректорий директории /home. Директории имеют следующие права: владельцы данных директорий обладают полными правами (на чтение, запись и выполнение), в то время как группы и другие пользователи обладают нулевыми правами.

10. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой (рис. 4.7):

`lsattr /home`

```
[guest@kvborovikova ~]$ lsattr /home
lsattr: отказано в доступе While reading flags on /home/kvborovikova
----- /home/guest
[guest@kvborovikova ~]$
```

Рис. 4.7: Расширенные атрибуты поддиректории

Нам удалось просмотреть расширенные атрибуты своей домашней директории - оказалось, что никаких расширенных атрибутов нет. В то же время нам отказывают в доступе к просмотру расширенных атрибутов директории другого пользователя (рис. [fig?];007).

11. Создадим в домашней директории поддиректорию `dir1` командой `mkdir dir1`.

Определим командами `ls -l` (рис. 4.8) и `lsattr` (рис. 4.9), какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

```

[guest@kvborovikova ~]$ mkdir dir1
[guest@kvborovikova ~]$ ls -l /home/guest/
итого 0
drwxr-xr-x. 2 guest guest 6 сен 16 15:25 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Документы
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Изображения
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Музыка
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Шаблоны
[guest@kvborovikova ~]$
```

Рис. 4.8: Права доступа на директорию

```

drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Шаблоны
[guest@kvborovikova ~]$ 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@kvborovikova ~]$
```

Рис. 4.9: Атрибуты директорий

Видим, что в директории `dir1` ее владелец обладает полными правами (`rwX`), а группы пользователей и другие пользователи имеют права только на чтение и выполнение (`r-x`). Расширенных атрибутов у каталога нет.

12. Снимем с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверим правильность выполнения с помощью команды `ls -l` (рис. 4.10).

```

[guest@kvborovikova ~]$ chmod 000 dir1
[guest@kvborovikova ~]$ ls -l /home/guest/
иторо 0
d-----, 2 guest guest 6 сен 16 15:25 dir1
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Видео
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Документы
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Загрузки
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Изображения
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Музыка
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Общедоступные
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 'Рабочий стол'
drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Шаблоны
[guest@kvborovikova ~]$
```

Рис. 4.10: Изменение прав доступа на dir1

Видим, что теперь на директорию dir1 нет никаких прав.

13. Попытаемся создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`.

```

drwxr-xr-x, 2 guest guest 6 сен 16 15:19 Шаблоны
[guest@kvborovikova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@kvborovikova ~]$
```

Рис. 4.11: Попытки взаимодействия с каталогом dir1

Мы получили отказ в выполнении операции по созданию файла, потому что мы не обладаем правами на это, поскольку в предыдущих шагах мы обнулили все права данного каталога.

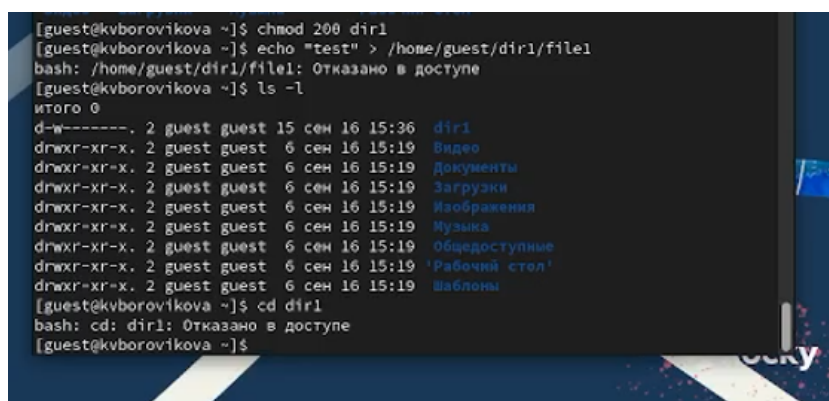
Из-за нулевых прав мы также не можем посмотреть содержимое каталога. Если попытаться взаимодействовать с файлом система ответит, что такого файла нет, значит файл не создался, что логично, поскольку у нас нет прав на создание файлов в данной директории.

14. Заполните 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, занесите в таблицу знак «+», если не разрешена, знак «-».

Для определения опытным путем будем использовать следующие действия в соответствии со столбцами таблицы:

- `cd dir1` - смена директории;
- `touch <новый_файл>` - создание файла;
- `rm <новый_файл>` - удаление файла;
- `ls -l (dir1)` - просмотр файлов в директории;
- `echo "test" > <файл_с_установленными_правами>` - запись в файл;
- `cat <файл_с_установленными_правами>` - чтение файла;
- `mv <файл_с_установленными_правами> <переименование>` - переименование файла;
- `chattr <атрибуты> <файл_с_установленными_правами>` смена атрибутов файла.

В качестве примера приведу осуществление проверки для прав доступа `d-w----- (200)`, `-----(000)` (рис. ??)



```
[guest@kvborovikova ~]$ chmod 200 dir1
[guest@kvborovikova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@kvborovikova ~]$ ls -l
итого 0
d-w-----. 2 guest guest 15 сен 16 15:36 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Документы
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Изображения
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Музыка
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 16 15:19 Шаблоны
[guest@kvborovikova ~]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest@kvborovikova ~]$
```

Рис. 4.12: Проверка возможных действий для прав доступа

Остальные действия можно найти в видеозаписи к лабораторной работе. Заполненная табл. 4.1 краткого описания стандартных каталогов Unix.

Таблица 4.1: Установленные права и разрешенные действия

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
----- (000)	----- (000)	-	-	-	-	-	-	-	-
----- (000)	-- x----- (100)	-	-	-	-	-	-	-	-
----- (000)	- w----- (200)	-	-	-	-	-	-	-	-
----- (000)	- wx----- (300)	-	-	-	-	-	-	-	-
----- (000)	r----- (400)	-	-	-	-	-	-	-	-
----- (000)	r- x----- (500)	-	-	-	-	-	-	-	-
----- (000)	rw----- (600)	-	-	-	-	-	-	-	-
----- (000)	rw- x----- (700)	-	-	-	-	-	-	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
--x----- (100)	----- (000)	-	-	-	-	+	-	-	-
--x----- (100)	-- x----- (100)	-	-	-	-	+	-	-	-
--x----- (100)	- w----- (200)	-	-	+	-	+	-	-	-
--x----- (100)	- wx----- (300)	-	-	+	-	+	-	-	-
--x----- (100)	r----- (400)	-	-	+	+	+	-	-	+
--x----- (100)	r- x----- (500)	-	-	-	+	+	-	-	+
--x----- (100)	rw----- (600)	-	+	+	+	+	-	-	+
--x----- (100)	rwX----- (700)	-	+	+	+	+	-	-	+
-w----- (200)	----- (000)	-	-	-	-	-	-	-	-

Права ди- ректории	Права файла	Со-	Уда-				Про-	Пере-	Смена
		зда- ние	ле- ние	За- пись	Чте- ние	Смена	фай- лов	име- нова- ние	
		фай- ла	фай- ла	в файл	ла	дирек- тории	дирек- тории	фай- ла	аттри- бутов файла
-w----- (200)	-- x----- (100)	-	-	-	-	-	-	-	-
-w----- (200)	- w----- (200)	-	-	-	-	-	-	-	-
-w----- (200)	- wx----- (300)	-	-	-	-	-	-	-	-
-w----- (200)	r----- (400)	-	-	-	-	-	-	-	-
-w----- (200)	r- x----- (500)	-	-	-	-	-	-	-	-
-w----- (200)	rw----- (600)	-	-	-	-	-	-	-	-
-w----- (200)	rwX----- (700)	-	-	-	-	-	-	-	-
-wx----- (300)	-----+ (000)	+	+	-	-	+	-	+	-
-wx----- (300)	-- x----- (100)	+	+	-	-	+	-	+	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
-wx----- (300)	- w----- (200)	+	+	+	-	+	-	+	-
-wx----- (300)	- wx----- (300)	+	+	+	-	+	-	+	-
-wx----- (300)	r----- (400)	+	+	-	+	+	-	+	+
-wx----- (300)	r- x----- (500)	+	+	-	+	+	-	+	+
-wx----- (300)	rw----- (600)	+	+	+	+	+	-	+	+
-wx----- (300)	rwX----- (700)	+	+	+	+	+	-	+	+
r----- (400)	----- (000)	-	-	-	-	-	+	-	-
r----- (400)	-- x----- (100)	-	-	-	-	-	+	-	-
r----- (400)	- w----- (200)	-	-	-	-	-	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
r----- (400)	- wx----- (300)	-	-	-	-	-	+	-	-
r----- (400)	r----- (400)	-	-	-	-	-	+	-	-
r----- (400)	r- x----- (500)	-	-	-	-	-	+	-	-
r----- (400)	rw----- (600)	-	-	-	-	-	+	-	-
r----- (400)	rwX----- (700)	-	-	-	-	-	+	-	-
r-x----- (500)	----- (000)	-	-	-	-	+	+	-	-
r-x----- (500)	-- x----- (100)	-	-	-	-	+	+	-	-
r-x----- (500)	- w----- (200)	-	-	+	-	+	+	-	-
r-x----- (500)	- wx----- (300)	-	-	+	-	+	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
r-x----- (500)	r----- (400)	-	-	+	+	+	+	-	+
r-x----- (500)	r- x----- (500)	-	-	-	+	+	+	-	+
r-x----- (500)	rw----- (600)	-	+	+	+	+	+	-	+
r-x----- (500)	rwX----- (700)	-	+	+	+	+	+	-	+
rw----- (600)	----- (000)	-	-	-	-	-	+	-	-
rw----- (600)	-- x----- (100)	-	-	-	-	-	+	-	-
rw----- (600)	- w----- (200)	-	-	-	-	-	+	-	-
rw----- (600)	- wx----- (300)	-	-	-	-	-	+	-	-
rw----- (600)	r----- (400)	-	-	-	-	-	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
rw----- (600)	r- x----- (500)	-	-	-	-	-	+	-	-
rw----- (600)	rw----- (600)		-	-	-	-	+	-	-
rw----- (600)	rwX----- (700)		-	-	-	-	+	-	-
rwX----- (700)	-----+ (000)	+	+	-	-	+	+	+	-
rwX----- (700)	-- x----- (100)	+	+	-	-	+	+	+	-
rwX----- (700)	- w----- (200)	+	+	+	-	+	+	+	-
rwX----- (700)	- wx----- (300)	+	+	+	-	+	+	+	-
rwX----- (700)	r-----+ (400)	+	+	-	+	+	+	+	+
rwX----- (700)	r- x----- (500)	+	+	-	+	+	+	+	+

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
rwX----- (700)	rw-----+	+	+	+	+	+	+	+	+
rwX----- (700)	rwX-----+	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы 4.1 определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 4.2.

Таблица 4.2: Минимальные права для совершения операций

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)	-----(000)
Удаление поддиректории	d-wx---(300)	-----(000)

5 Выводы

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. Заполнила опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

Список литературы