
ЛР №2. Дискреционное разграничение прав в Linux. Основные атрибуты

Информационная безопасность

Доборщук Владимир Владимирович,
НФИбд-01-18

2 октября 2021

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
1. Взаимодействие с пользователем	6
2. Работа с атрибутами	9
Заключение	20

Список иллюстраций

1	Взаимодействие с учетной записью нового пользователя	6
2	Информация о пользователе guest	7
3	Информация о пользователе vvdoborschuk	8
4	Файл /etc/passwd	9
5	Вывод информации от guest	10
6	Вывод информации от vvdoborschuk	10
7	Работа с директориями и файлами	11
8	Атрибуты 100	12
9	Атрибуты 200	13
10	Атрибуты 300. Часть 1	14
11	Атрибуты 300. Часть 2	15
12	Атрибуты 400	16
13	Атрибуты 500	17
14	Атрибуты 600	18

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.

Задачи:

- анализ атрибутов директорий/файлов;
- укрепление навыков манипуляции учетными записями;
- укрепление навыков взаимодействия с файловой системой.

Теоретическое введение

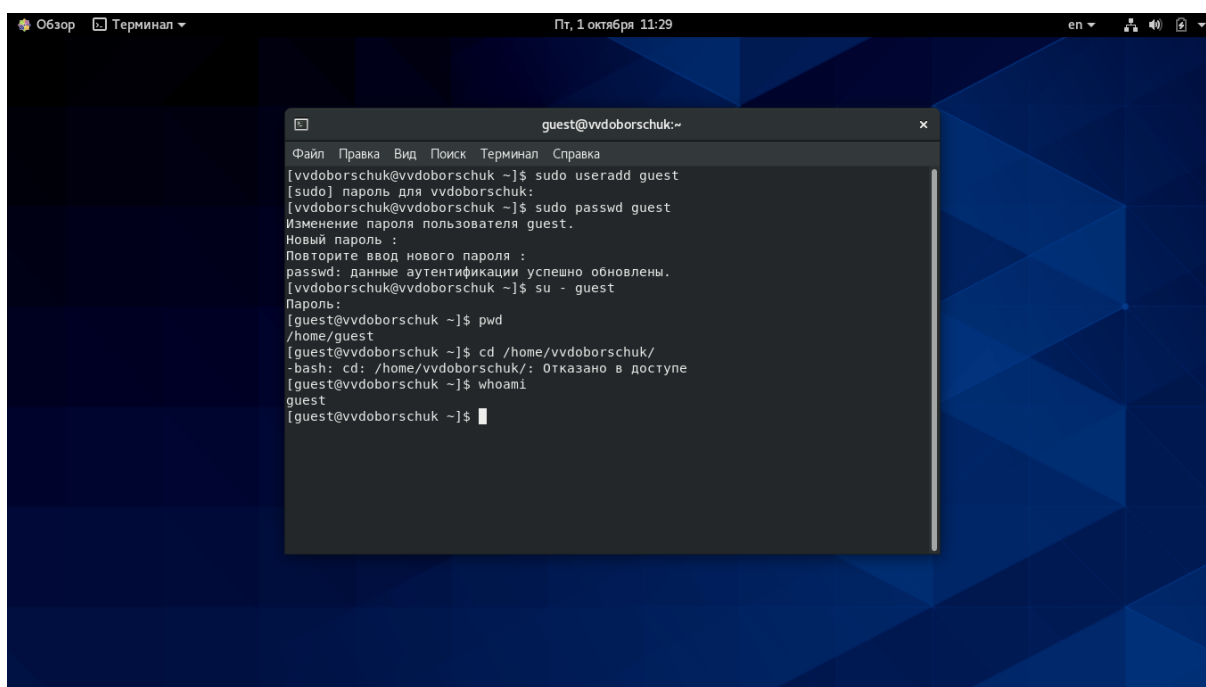
Для выполнения данной лабораторной работы мы использовали данные источники, в виде описания лабораторной работы, а также свободные источники в интернете.

Выполнение лабораторной работы

1. Взаимодействие с пользователем

Зайдя в терминал, мы сделали следующие вещи:

- создали учетную запись для guest;
- задали пароль для guest;
- вошли в систему от лица guest;
- определили домашнюю директорию для текущего пользователя;
- уточнили имя текущего пользователя.



```
guest@vvdoborschuk:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[vvdoborschuk@vvdoborschuk ~]$ sudo useradd guest  
[sudo] пароль для vvdoborschuk:  
[vvdoborschuk@vvdoborschuk ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль :  
Повторите ввод нового пароля :  
passwd: данные аутентификации успешно обновлены.  
[vvdoborschuk@vvdoborschuk ~]$ su - guest  
Пароль:  
[guest@vvdoborschuk ~]$ pwd  
/home/guest  
[guest@vvdoborschuk ~]$ cd /home/vvdoborschuk/  
-bash: cd: /home/vvdoborschuk/: Отказано в доступе  
[guest@vvdoborschuk ~]$ whoami  
guest  
[guest@vvdoborschuk ~]$
```

Рис. 1: Взаимодействие с учетной записью нового пользователя

Далее, с помощью команды `id` мы уточнили имя пользователя, его группу и группы, куда он входит. Также использовали команду `groups`, благодаря которой мы получаем также группы, в которые входит наш текущий пользователь (что также описано командой `id`).

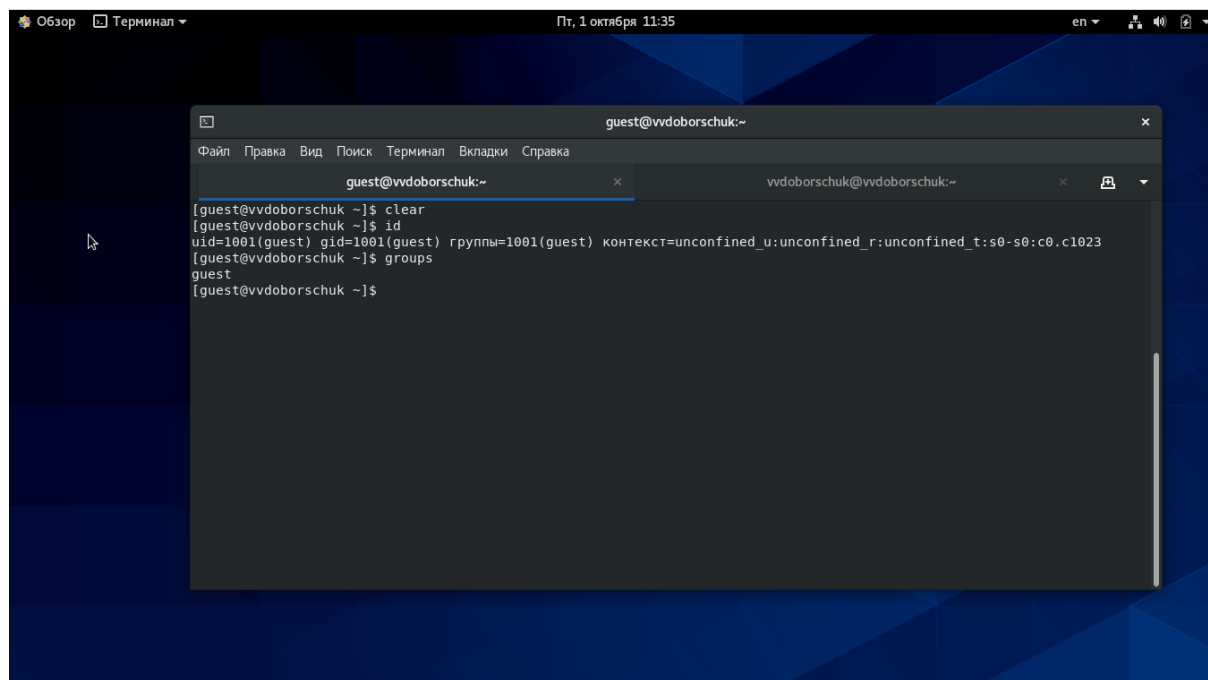


Рис. 2: Информация о пользователе guest

Сравнивая это с данными изначального пользователя, видим основные различия в имени и основной группе пользователей, а также “дефолтный” пользователь входит в группу wheel, в отличие от пользователя guest.

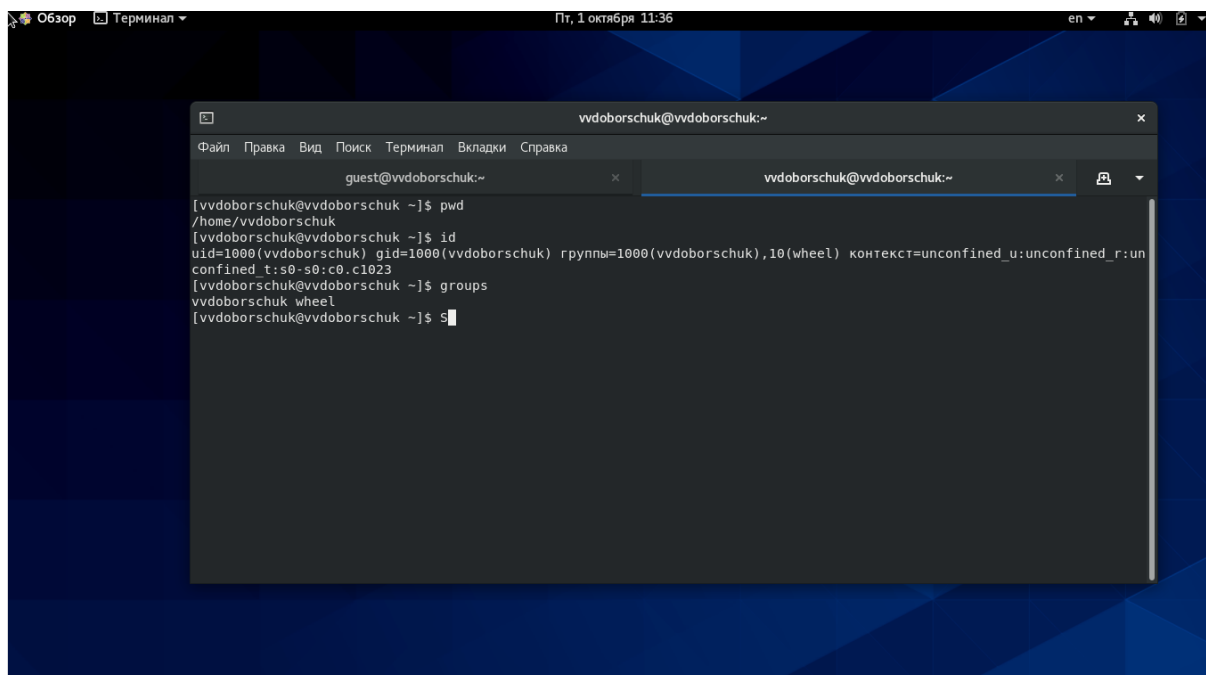


Рис. 3: Информация о пользователе vvdoborschuk

С помощью команды `cat /etc/passwd` и фильтра `grep` получили также часть данных о наших пользователях в системе.

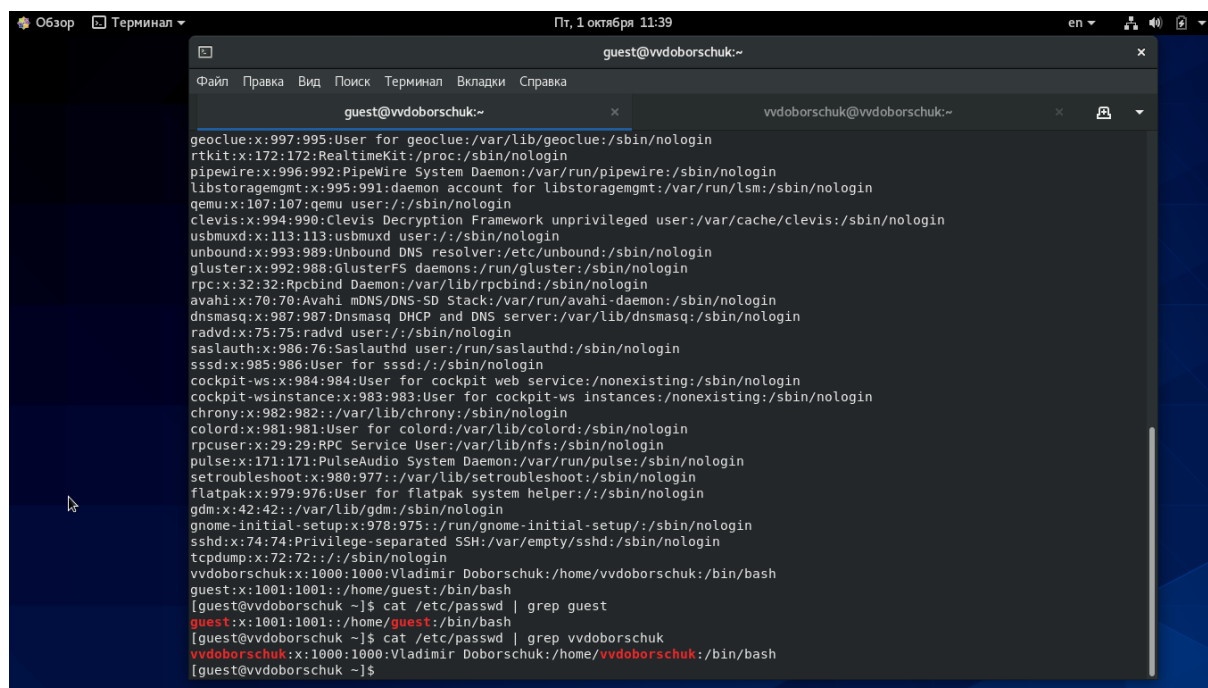


Рис. 4: Файл /etc/passwd

2. Работа с атрибутами

Мы попытались определить, какие директории существуют в каталоге /home.

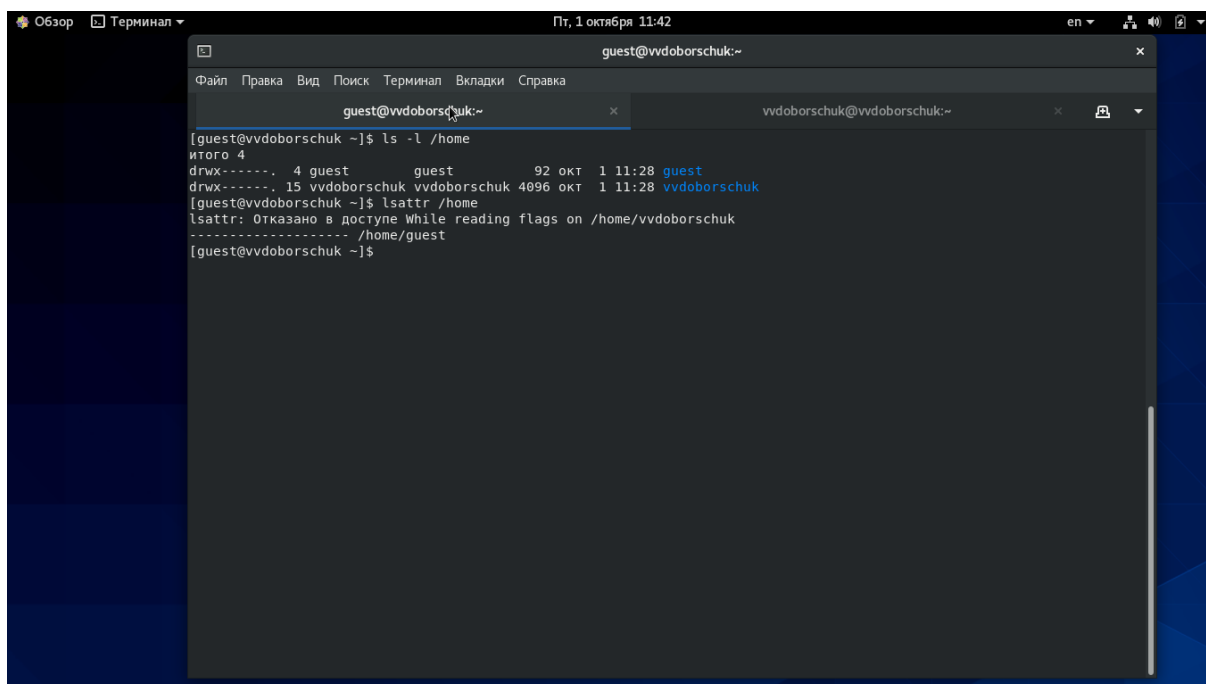


Рис. 5: Вывод информации от guest

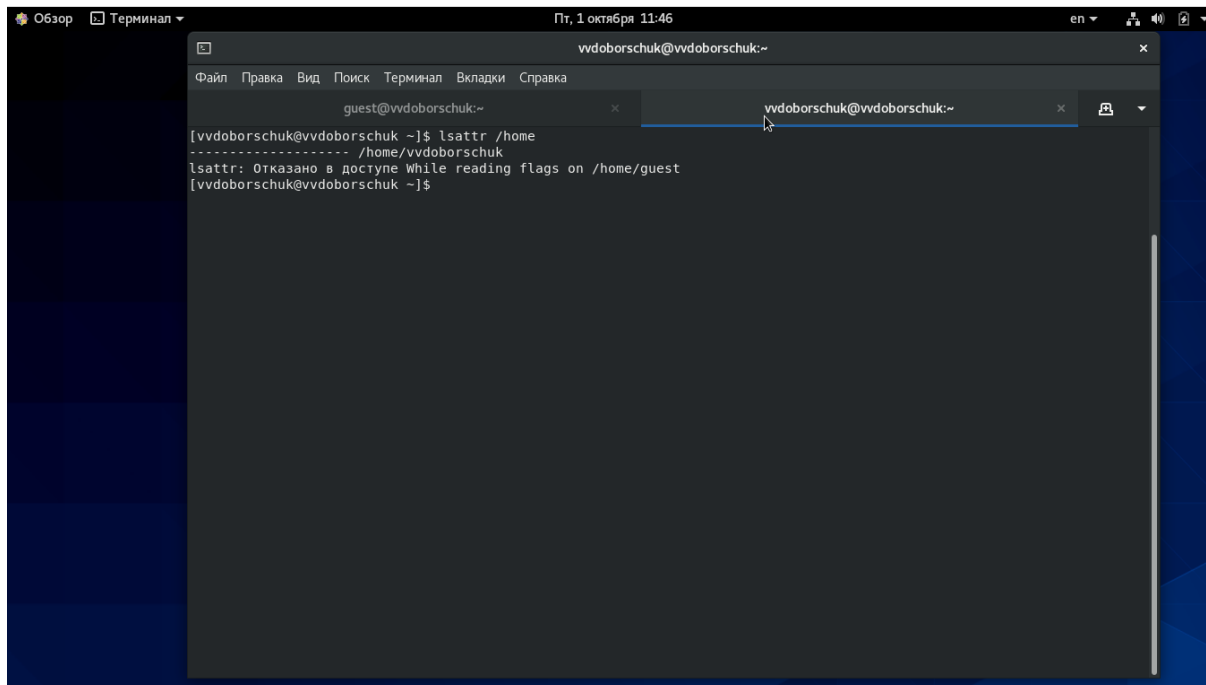


Рис. 6: Вывод информации от vvdoborschuk

Видно, что мы смогли получить список каталогов от любого из данных нам пользователей, но нам недоступны расширенные атрибуты других пользователей.

Выполнили пункты 11-13, параллельно приступив к заполнению нашей таблицы.

```

guest@vvdoborschuk:~$ mkdir dir1
guest@vvdoborschuk:~$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 окт  1 11:47 dir1
guest@vvdoborschuk:~$ lsattr .
----- ./dir1
guest@vvdoborschuk:~$ chmod 000 dir1/
guest@vvdoborschuk:~$ ls -l
итого 0
d-----. 2 guest guest 6 окт  1 11:47 dir1
guest@vvdoborschuk:~$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Отказано в доступе
guest@vvdoborschuk:~$ ls -l /home/guest/dir1/
ls: невозможно открыть каталог '/home/guest/dir1/': Отказано в доступе
guest@vvdoborschuk:~$ cd dir1/
-bash: cd: dir1/: Отказано в доступе
guest@vvdoborschuk:~$
    
```

Рис. 7: Работа с директориями и файлами

Мы не смогли записать файл `/home/guest/dir1/file1`, т.к. права на директорию `dir1` эквивалентны (000), что означает запрет на чтение, запись и исполняемость внутри директории. Также, файл не создавался внутри директории, как показал проверка.

Перед заполнением таблицы, мы экспериментально проверили все возможные варианты атрибутов для индивидуального пользователя.

```

Пт, 1 октября 12:10
guest@vvdoborschuk:~
Файл Правка Вид Поиск Терминал Справка
[guest@vvdoborschuk ~]$ chmod 100 dir1/
[guest@vvdoborschuk ~]$ ls -l
итого 0
d--x----- 2 guest guest 6 окт  1 11:47 dir1
[guest@vvdoborschuk ~]$ cd dir1/
[guest@vvdoborschuk dir1]$ ls -l
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@vvdoborschuk dir1]$ touch file1
touch: невозможно выполнить touch для 'file1': Отказано в доступе
[guest@vvdoborschuk dir1]$ cd ..
[guest@vvdoborschuk ~]$ chmod 700 dir1/
[guest@vvdoborschuk ~]$ touch dir1/file1
[guest@vvdoborschuk ~]$ chmod 100 dir1/
[guest@vvdoborschuk ~]$ ls
dir1
[guest@vvdoborschuk ~]$ ls -l
итого 0
d--x----- 2 guest guest 19 окт  1 12:07 dir1
[guest@vvdoborschuk ~]$ cd dir1/
[guest@vvdoborschuk dir1]$ ls -l
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@vvdoborschuk dir1]$ lsattr .
[guest@vvdoborschuk dir1]$ cd ..
[guest@vvdoborschuk ~]$ lsattr .
lsattr: Отказано в доступе While reading flags on ./dir1
[guest@vvdoborschuk ~]$ cd dir1/
[guest@vvdoborschuk dir1]$ chmod 100 file1
[guest@vvdoborschuk dir1]$ ls -l
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@vvdoborschuk dir1]$ cd ..
[guest@vvdoborschuk ~]$ chmod 000 dir1
[guest@vvdoborschuk ~]$ chmod 100 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@vvdoborschuk ~]$

```

Рис. 8: Атрибуты 100

```

guest@vvdoborschuk:~
Файл Правка Вид Поиск Терминал Справка
[guest@vvdoborschuk ~]$ chmod 200 dir1
[guest@vvdoborschuk ~]$ ls -l
итого 0
d-w-----. 2 guest guest 19 окт  1 12:07 dir1
[guest@vvdoborschuk ~]$ cd dir1/
-bash: cd: dir1/: Отказано в доступе
[guest@vvdoborschuk ~]$ ls -l dir1/
ls: невозможно открыть каталог 'dir1/': Отказано в доступе
[guest@vvdoborschuk ~]$ mv dir1/file1 dir1/file
mv: не удалось получить доступ к 'dir1/file': Отказано в доступе
[guest@vvdoborschuk ~]$ chmod 700 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@vvdoborschuk ~]$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
[guest@vvdoborschuk ~]$ echo "test" > dir1/file1
-bash: dir1/file1: Отказано в доступе
[guest@vvdoborschuk ~]$ echo "test" > dir1/file2
-bash: dir1/file2: Отказано в доступе
[guest@vvdoborschuk ~]$ rm dir1/file1
rm: невозможно удалить 'dir1/file1': Отказано в доступе

```

Рис. 9: Атрибуты 200

```

guest@vvdoborschuk:~
Файл Правка Вид Поиск Терминал Справка
[guest@vvdoborschuk ~]$ chmod 300 dir1/
[guest@vvdoborschuk ~]$ echo "test" > dir1/file2
[guest@vvdoborschuk ~]$ echo "test" > dir1/file3
[guest@vvdoborschuk ~]$ rm dir1/file2
[guest@vvdoborschuk ~]$ rm dir1/file1
rm: удалить защищенный от записи пустой обычный файл 'dir1/file1'? y
[guest@vvdoborschuk ~]$ cat dir1/file3
test
[guest@vvdoborschuk ~]$ ls -l dir1/file3
-rw-rw-r--. 1 guest guest 5 окт  1 12:18 dir1/file3
[guest@vvdoborschuk ~]$ cd dir1/
[guest@vvdoborschuk dir1]$ ls -l
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@vvdoborschuk dir1]$ cd ..
[guest@vvdoborschuk ~]$ ls -l dir1/file3
-rw-rw-r--. 1 guest guest 5 окт  1 12:18 dir1/file3
[guest@vvdoborschuk ~]$ ls -l
итого 0
d-wx-----. 2 guest guest 19 окт  1 12:18 dir1
[guest@vvdoborschuk ~]$ rm dir1/*
rm: невозможно удалить 'dir1/*': Нет такого файла или каталога
[guest@vvdoborschuk ~]$ rm dir1/*
rm: невозможно удалить 'dir1/*': Нет такого файла или каталога
[guest@vvdoborschuk ~]$ rm dir1/
rm: невозможно удалить 'dir1/': Это каталог
[guest@vvdoborschuk ~]$ rm dir1/file1
rm: невозможно удалить 'dir1/file1': Нет такого файла или каталога
[guest@vvdoborschuk ~]$ rm dir1/file2
rm: невозможно удалить 'dir1/file2': Нет такого файла или каталога
[guest@vvdoborschuk ~]$ rm dir1/file3
[guest@vvdoborschuk ~]$ ls -l dir1/
ls: невозможно открыть каталог 'dir1/': Отказано в доступе
[guest@vvdoborschuk ~]$ ss

```

Рис. 10: Атрибуты 300. Часть 1

```

guest@vvdoborschuk:~/dir1
Файл Правка Вид Поиск Терминал Справка
[guest@vvdoborschuk ~]$ chmod 700 dir1/
[guest@vvdoborschuk ~]$ ls -l
итого 0
drwx-----. 2 guest guest 6 окт  1 12:22 dir1
[guest@vvdoborschuk ~]$ chmod 300 dir1/
[guest@vvdoborschuk ~]$ ls
dir1
[guest@vvdoborschuk ~]$ echo "test" > dir1/file1
[guest@vvdoborschuk ~]$ ls -l dir1/
ls: невозможно открыть каталог 'dir1/': Отказано в доступе
[guest@vvdoborschuk ~]$ ls -l dir1/file1
-rw-rw-r--. 1 guest guest 5 окт  1 12:24 dir1/file1
[guest@vvdoborschuk ~]$ chmod 200 dir1
[guest@vvdoborschuk ~]$ ls -l dir1/file1
ls: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@vvdoborschuk ~]$ cd dir1/
-bash: cd: dir1/: Отказано в доступе
[guest@vvdoborschuk ~]$ mv dir1/file1 dir1/file2
mv: не удалось получить доступ к 'dir1/file2': Отказано в доступе
[guest@vvdoborschuk ~]$ ls -l
итого 0
d-w-----. 2 guest guest 19 окт  1 12:24 dir1
[guest@vvdoborschuk ~]$ chmod 300 dir1/
[guest@vvdoborschuk ~]$ cd dir1/
[guest@vvdoborschuk dir1]$ ls -l
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@vvdoborschuk dir1]$ mv file1 file2
[guest@vvdoborschuk dir1]$ chmod 600 file2
[guest@vvdoborschuk dir1]$ ls -l
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@vvdoborschuk dir1]$ ls -l file2
-rw-----. 1 guest guest 5 окт  1 12:24 file2
[guest@vvdoborschuk dir1]$

```

Рис. 11: Атрибуты 300. Часть 2

```

guest@vvdoborschuk:~
Файл Правка Вид Поиск Терминал Справка
[guest@vvdoborschuk ~]$ chmod 400 dir1/
[guest@vvdoborschuk ~]$ touch dir1/file1
touch: невозможно выполнить touch для 'dir1/file1': Отказано в доступе
[guest@vvdoborschuk ~]$ lsattr dir1/
dir1/..: Отказано в доступе
dir1/...: Отказано в доступе
dir1/file2: Отказано в доступе
[guest@vvdoborschuk ~]$ cat dir1/file2
cat: dir1/file2: Отказано в доступе
[guest@vvdoborschuk ~]$ ls -l
итого 0
dr----- . 2 guest guest 19 окт  1 12:28 dir1
[guest@vvdoborschuk ~]$ echo "test" > dir1/file2
-bash: dir1/file2: Отказано в доступе
[guest@vvdoborschuk ~]$ rm dir1/file2
rm: невозможно удалить 'dir1/file2': Отказано в доступе
[guest@vvdoborschuk ~]$ cd dir1/
-bash: cd: dir1/: Отказано в доступе
[guest@vvdoborschuk ~]$ ls -l dir1/
ls: невозможно получить доступ к 'dir1/file2': Отказано в доступе
итого 0
-???????? ? ? ? ? ? file2
[guest@vvdoborschuk ~]$ mv dir1/file2 dir1/file1
mv: не удалось получить доступ к 'dir1/file1': Отказано в доступе
[guest@vvdoborschuk ~]$ chmod 700 dir1/file2
chmod: невозможно получить доступ к 'dir1/file2': Отказано в доступе
[guest@vvdoborschuk ~]$

```

Рис. 12: Атрибуты 400


```

guest@vvdoborschuk:~
Файл Правка Вид Поиск Терминал Справка
[guest@vvdoborschuk ~]$ chmod 500 dir1
[guest@vvdoborschuk ~]$ ls -l
итого 0
dr-x-----. 2 guest guest 19 окт  1 12:28 dir1
[guest@vvdoborschuk ~]$ touch dir1/fileN
touch: невозможно выполнить touch для 'dir1/fileN': Отказано в доступе
[guest@vvdoborschuk ~]$ echo "test" > dir1/file2
[guest@vvdoborschuk ~]$ cat dir1/file2
test
[guest@vvdoborschuk ~]$ touch dir1/file1
touch: невозможно выполнить touch для 'dir1/file1': Отказано в доступе
[guest@vvdoborschuk ~]$ ls -l dir1/
итого 4
-rw-----. 1 guest guest 5 окт  1 12:35 file2
[guest@vvdoborschuk ~]$ chmod 400 dir1/file2
[guest@vvdoborschuk ~]$ ls -l dir1/
итого 4
-r-----. 1 guest guest 5 окт  1 12:35 file2
[guest@vvdoborschuk ~]$ chmod 777 dir1/file2
[guest@vvdoborschuk ~]$ ls -l dir1/
итого 4
-rwxrwxrwx. 1 guest guest 5 окт  1 12:35 file2
[guest@vvdoborschuk ~]$ echo "test" > dir1/file3
-bash: dir1/file3: Отказано в доступе
[guest@vvdoborschuk ~]$ mv dir1/file2 dir1/file3
mv: невозможно переместить 'dir1/file2' в 'dir1/file3': Отказано в доступе
[guest@vvdoborschuk ~]$ rm dir1/file2
rm: невозможно удалить 'dir1/file2': Отказано в доступе
[guest@vvdoborschuk ~]$

```

Рис. 13: Атрибуты 500

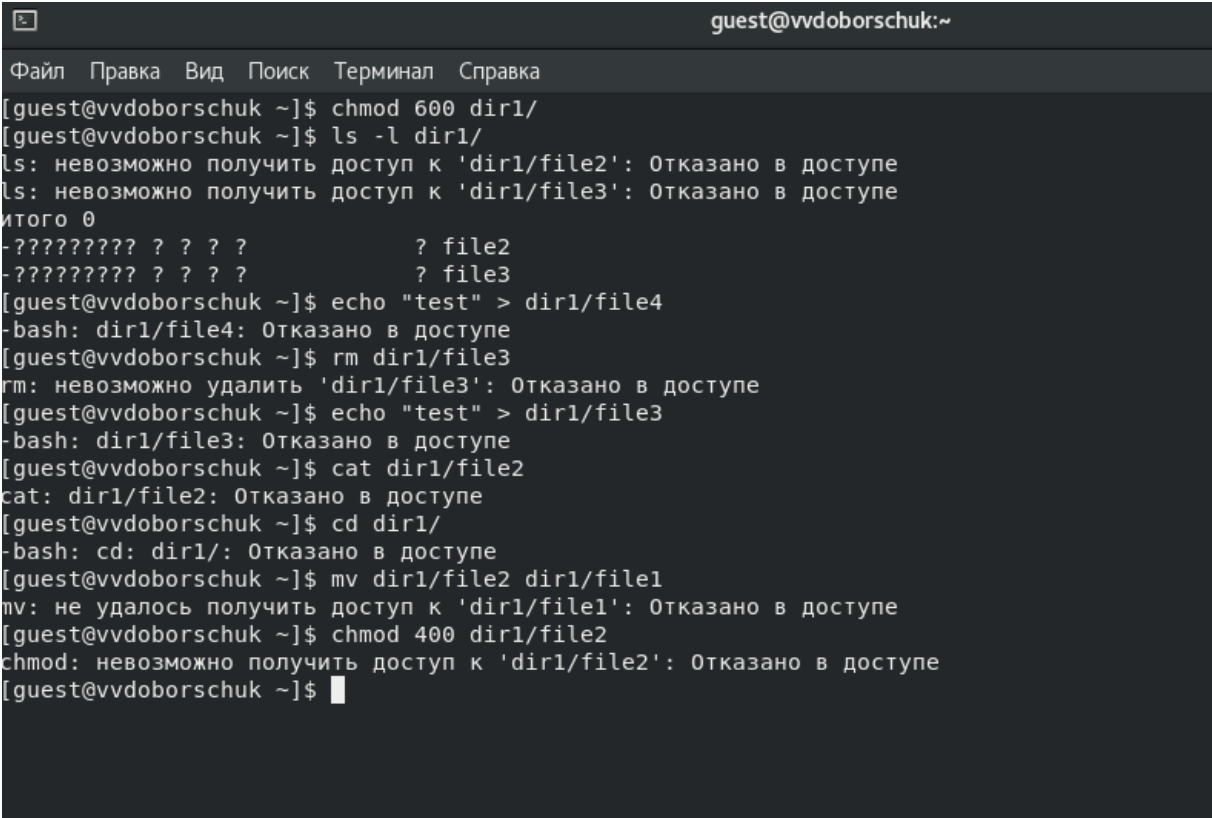


Рис. 14: Атрибуты 600

Для случая с правами (700) все достаточно очевидно, поэтому его мы не стали индивидуально рассматривать.

Таблица 1. Установленные права и разрешённые действия

Права		Запись		Смена		Просмотр		Смена	
ди-ректории	Права файла	Создание файла	Удаление файла	Чтение файла	ди-ректории	ди-ректории	ди-ректории	атри-бутов	атри-бутов
d-----	(000)	-	-	-	-	-	-	-	-
d--x-----	(000)	-	-	-	+	-	-	-	+

Права	Просмотр	Смена	Смена	Смена	Смена	Смена	Смена	Смена	Смена
ди-ректо-рии	Прав	Создани	Удалени	Запись	Чтение	ди-ректо-рии	лов в	ди-ректо-рии	атри-бутов
Прав	файла	файла	файла	файл	файла	Прав	файла	Прав	файла
d-w----- (200)	(000)	-	-	-	-	-	-	-	-
d-wx---- (300)	-wx---	+	+	+	+	-	+	+	+
dr----- (400)	(000)	-	-	-	-	+	-	-	-
dr-x---- (500)	-wx---	-	+	+	+	+	-	+	+
drw----- (600)	(000)	-	-	-	-	+	-	-	-
drwx---- (700)	-wx---	+	+	+	+	+	+	+	+

Таблица 2. Минимальные права для совершения операция

Операции	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx----- (300)	--wx----- (300)
Удаление файла	d-wx----- (300)	---x----- (100)
Чтение файла	d-wx----- (300)	-r----- (400)
Запись в файл	d-wx----- (300)	-rw----- (500)
Переименование файла	d-wx----- (300)	-rw----- (500)
Создание поддиректории	drwx----- (700)	---x----- (100)
Удаление поддиректории	drwx----- (700)	---x----- (100)

Заключение

Мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.