

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

Дисциплина: Информационная безопасность

---

Доборщук Владимир Владимирович, НФИбд-01-18

2 октября 2021

# Цель работы

---

# 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.

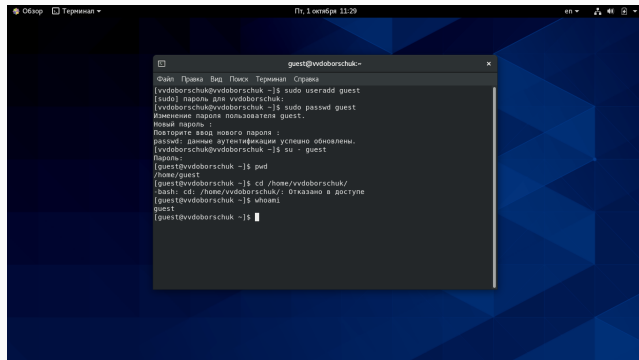
## Задачи:

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

# Выполнение лабораторной работы

---

# Выполнение лабораторной работы

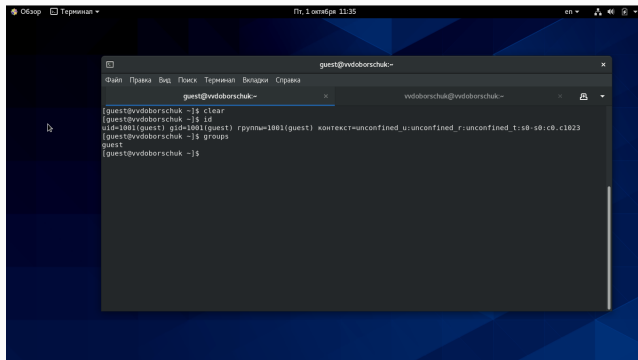


```
Обзор Терминал
Пн, 1 октября 11:29
en

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
Пароля:
[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

# Выполнение лабораторной работы

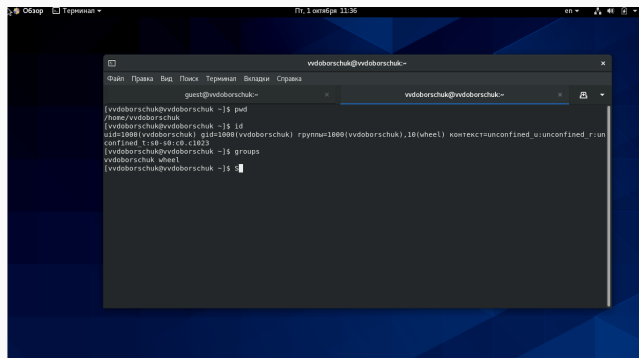


The screenshot shows a terminal window titled "guest@vvdoborschuk:-". The terminal output is as follows:

```
guest@vvdoborschuk ~]$ clear
(guest@vvdoborschuk ~)$ id
uid=1001(guest) gid=1001(guest) rpnpu=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
(guest@vvdoborschuk ~)$ groups
guest
(guest@vvdoborschuk ~)$
```

Рис. 2: Информация о пользователе guest

# Выполнение лабораторной работы

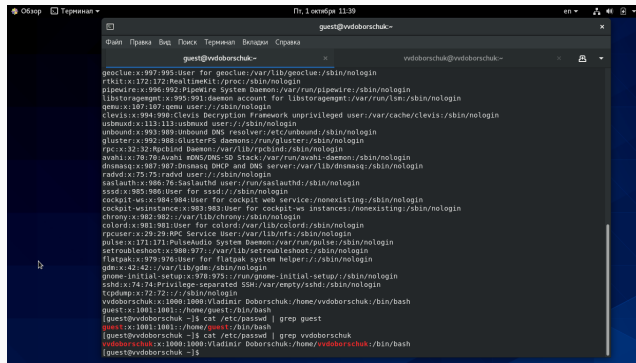


The screenshot shows a terminal window titled "vvdoborschuk@vvdoborschuk-". The terminal output is as follows:

```
[vvdoborschuk@vvdoborschuk ~]$ pwd
/home/vvdoborschuk
[vvdoborschuk@vvdoborschuk ~]$ id
uid=1000(vvdoborschuk) gid=1000(vvdoborschuk) rгруппы=1000(vvdoborschuk),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-c1023
[vvdoborschuk@vvdoborschuk ~]$ groups
vvdoborschuk wheel
[vvdoborschuk@vvdoborschuk ~]$
```

Рис. 3: Информация о пользователе vvdoborschuk

# Выполнение лабораторной работы

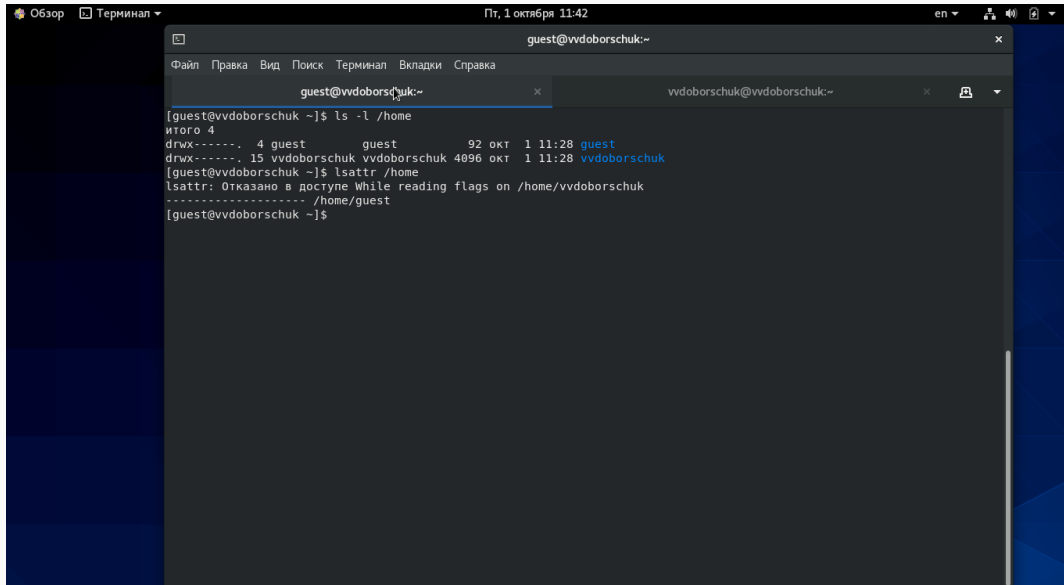


```
guest@vvdoborschuk-  
geoclue:x:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
pipewire:x:996:992:Pipewire System Daemon:/var/run/pipewire:/sbin/nologin  
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin  
qemu:x:107:107:qemu user:/sbin/nologin  
clevis:x:994:990:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin  
unbound:x:993:989:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
gluster:x:992:988:GlusterFS daemons:/run/gluster:/sbin/nologin  
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
dnsmasq:x:987:987:dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
radvd:x:75:75:radvd user:/sbin/nologin  
saslauth:x:986:76:Saslauthd user:/run/saslauthd:/sbin/nologin  
sssd:x:985:986:User for sssd:/sbin/nologin  
cockpit-ws:x:984:984:User for cockpit web service:/nonexistent:/sbin/nologin  
cockpit-wsinstance:x:983:983:User for cockpit-ws instances:/nonexistent:/sbin/nologin  
chrony:x:982:982:/var/lib/chrony:/sbin/nologin  
colord:x:981:981:User for colord:/var/lib/colord:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/dfs:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
setroubleshoot:x:980:977:/var/lib/setroubleshoot:/sbin/nologin  
flatpak:x:979:976:User for flatpak system helper:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:978:975:/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
tcpdump:x:72:72:/sbin/nologin  
vvdoborschuk:x:1000:1000:Vladimir Doborschuk:/home/vvdoborschuk:/bin/bash  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@vvdoborschuk ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@vvdoborschuk ~]$ cat /etc/passwd | grep vvdoborschuk  
vvdoborschuk:x:1000:1000:Vladimir Doborschuk:/home/vvdoborschuk:/bin/bash  
[guest@vvdoborschuk ~]$
```

Рис. 4: Файл /etc/passwd



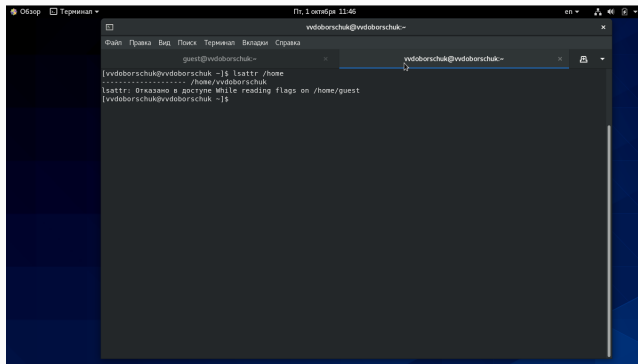
# Выполнение лабораторной работы



The screenshot shows a terminal window titled "guest@vvdoborschuk:~". The window has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", "Вкладки", and "Справка". Below the menu bar, there are two tabs: "guest@vvdoborschuk:~" (active) and "vvdoborschuk@vvdoborschuk:~". The terminal content shows the following commands and output:

```
[guest@vvdoborschuk ~]$ ls -l /home
итого 4
drwx-----.  4 guest      guest      92 окт  1 11:28 guest
drwx-----. 15 vvdoborschuk vvdoborschuk 4096 окт  1 11:28 vvdoborschuk
[guest@vvdoborschuk ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/vvdoborschuk
----- /home/guest
[guest@vvdoborschuk ~]$
```

# Выполнение лабораторной работы

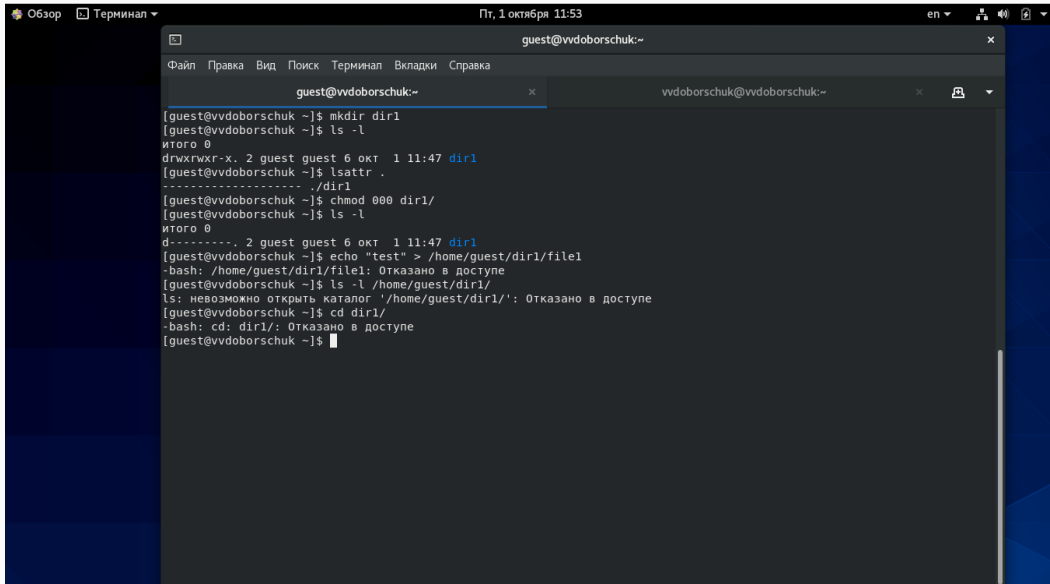


The screenshot shows a terminal window titled "Обзор Терминал" with a timestamp of "Пт, 1 октября 11:46". The terminal is running a command prompt for a user named "vvdoborschuk" on a host named "vvdoborschuk". The prompt is "vvdoborschuk@vvdoborschuk:". The user has entered the command "lsattr /home". The output of the command is displayed as follows:

```
[vvdoborschuk@vvdoborschuk ~]$ lsattr /home
----- /home/vvdoborschuk
lsattr: Отказано в доступе while reading flags on /home/guest
[vvdoborschuk@vvdoborschuk ~]$
```

Рис. 6: Вывод информации от vvdoborschuk

# Выполнение лабораторной работы



```
Обзор Терминал
Пт, 1 октября 11:53
en
guest@vvdoborschuk:~
Файл Правка Вид Поиск Терминал Вкладки Справка
guest@vvdoborschuk:~
vvdoborschuk@vvdoborschuk:~
[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 ~]$
```

# Выполнение лабораторной работы

```
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
```

# Выполнение лабораторной работы

```
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
```

# Выполнение лабораторной работы

```
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
```

# Выполнение лабораторной работы

```
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]$
```

# Выполнение лабораторной работы

```
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 ~]$
```



# Выполнение лабораторной работы

```
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 ~]$
```

# Выполнение лабораторной работы

```
guest@vvdoborschuk:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@vvdoborschuk ~]$ chmod 600 dir1/  
[guest@vvdoborschuk ~]$ ls -l dir1/  
ls: невозможно получить доступ к 'dir1/file2': Отказано в доступе  
ls: невозможно получить доступ к 'dir1/file3': Отказано в доступе  
итого 0  
-????????? ? ? ? ?      ? file2  
-????????? ? ? ? ?      ? file3  
[guest@vvdoborschuk ~]$ echo "test" > dir1/file4  
-bash: dir1/file4: Отказано в доступе  
[guest@vvdoborschuk ~]$ rm dir1/file3  
rm: невозможно удалить 'dir1/file3': Отказано в доступе  
[guest@vvdoborschuk ~]$ echo "test" > dir1/file3  
-bash: dir1/file3: Отказано в доступе  
[guest@vvdoborschuk ~]$ cat dir1/file2  
cat: dir1/file2: Отказано в доступе  
[guest@vvdoborschuk ~]$ cd dir1/  
-bash: cd: dir1/: Отказано в доступе  
[guest@vvdoborschuk ~]$ mv dir1/file2 dir1/file1  
mv: не удалось получить доступ к 'dir1/file1': Отказано в доступе  
[guest@vvdoborschuk ~]$ chmod 400 dir1/file2  
chmod: невозможно получить доступ к 'dir1/file2': Отказано в доступе  
[guest@vvdoborschuk ~]$
```

# Выполнение лабораторной работы

Таблица 1. Установленные права и разрешённые действия

| Права     |       |       |        |        |        | Смена  |     | Просмотр<br>фай-<br>лов в | Смена<br>атри-<br>бу- |
|-----------|-------|-------|--------|--------|--------|--------|-----|---------------------------|-----------------------|
| ди-       | рек-  | Прав  | Создан | Удален | Запись | Чтение | ди- | рек-                      | Перейти               |
| то-       | то-   | фай-  | фай-   | фай-   | в      | фай-   | то- | то-                       | фай-                  |
| рии       | рии   | ла    | ла     | ла     | файл   | ла     | рии | рии                       | ла                    |
| d-----    | (000) |       | -      | -      | -      | -      | -   | -                         | -                     |
| d--x----- | (100) | (000) | -      | -      | -      | +      | -   | -                         | +                     |

# Выполнение лабораторной работы

Таблица 2. Минимальные права для совершения операция

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

# Заключение

---

Мы приобрели практические навыки установки операционной системы на виртуальную машину, успешно настроили минимально необходимые для дальнейшей работы сервисы.