

# Лабораторная работа №2

## Дискреционное разграничение прав в Linux. Основные атрибуты

---

Кекишева А.Д.

16 сентябрь 2023

Российский университет дружбы народов, Москва, Россия

Докладчик

■ Кекишева Анастасия Дмитриевна

- Бизнес-информатика
- Кафедра теории вероятности и кибербезопасности
- Российский университет дружбы народов
- 1032201194@pfur.ru
- <https://github.com/adkekisheva>

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.

1. Создать учётную запись пользователя `guest` и задать пароль и проделать последовательность команд, описанных в лабораторной, которые направлены на изучения поведения прав директорий и файлов.
2. Заполнить таблицу «Установленные права и разрешённые действия»;
3. Заполнить таблицу «Минимально необходимые права для выполнения операций внутри директории».

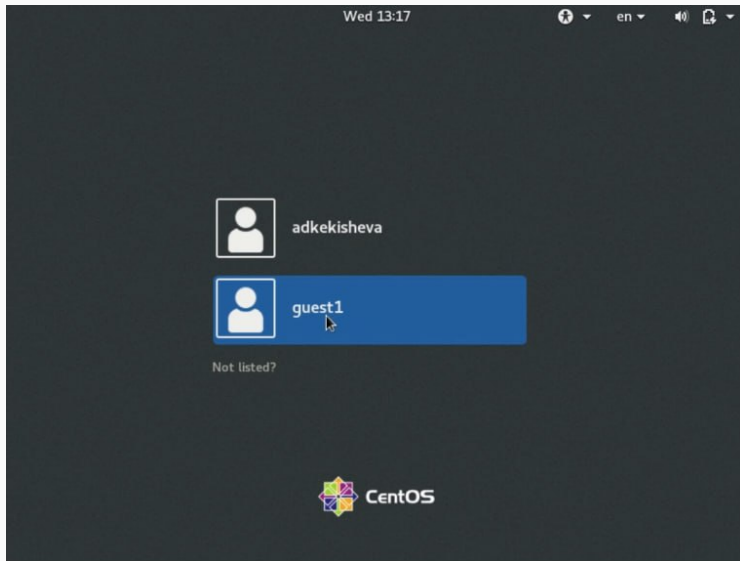


## Шаг 1 - Создание нового пользователя

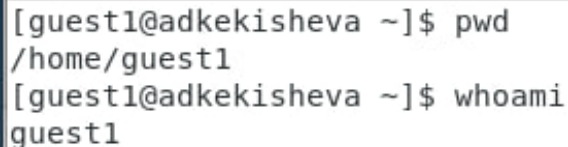
```
[root@adkekisheva ~]# useradd guest
useradd: user 'guest' already exists
[root@adkekisheva ~]# useradd guest1
[root@adkekisheva ~]# passwd guest1
Changing password for user guest1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Рис. 1: Создание нового пользователя

## Шаг 2 - Вход в систему



Определила директорию, в которой я нахожусь, командой pwd. Также уточнила имя пользователя командой whoami (рис. @fig:003).

A terminal window with a light gray background and a dark blue vertical bar on the left. The prompt is [guest1@adkekisheva ~]\$. The first command is pwd, followed by a newline and the output /home/guest1. The second command is whoami, followed by a newline and the output guest1.

```
[guest1@adkekisheva ~]$ pwd
/home/guest1
[guest1@adkekisheva ~]$ whoami
guest1
```



Уточнила имя моего пользователя, его группу, а также группы, куда входит пользователь, командой id.

```
[guest1@adkekisheva ~]$ id
uid=1002(guest1) gid=1002(guest1) groups=1002(guest1) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest1@adkekisheva ~]$ groups
guest1
```

## Шаг 5 - Просмотр файла /etc/passwd

```
[guest1@adkekisheva ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
polkitd:x:999:998:User for polkitd:./:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sane:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
saslauth:x:995:76:Saslauthd user:/run/saslauthd:/sbin/nologin
abrt:x:173:173:./etc/abrt:/sbin/nologin
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
```

Рис. 3: Содержание файл passwd

## Шаг 6 - Применение команды grep

```
[guest1@adkekisheva ~]$ cat /etc/passwd | grep guest1
guest1:x:1002:1002::/home/guest1:/bin/bash
[guest1@adkekisheva ~]$ cat /etc/passwd | grep uid
[guest1@adkekisheva ~]$ cat /etc/passwd | grep id
[guest1@adkekisheva ~]$ cat /etc/passwd | grep user
saned:x:996:994:SANE scanner daemon user:/usr/share/sane/sbin/nologin
sasauth:x:995:76:Sasauthd user:/run/sasauthd/sbin/nologin
radvd:x:75:75:radvd user:/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
rpcuser:x:29:29:RPC Service User:/var/lib/nfs/sbin/nologin
[guest1@adkekisheva ~]$ cat /etc/passwd | grep group
[guest1@adkekisheva ~]$ cat /etc/passwd | grep gid
```

Рис. 4: Применение команды grep

## Шаг 7 - Определение существующих директории

```
[guest1@adkekisheva ~]$ ls -l /home/
total 8
drwx-----. 21 adkekisheva adkekisheva 4096 Sep 13 13:16 adkekisheva
drwx-----.  3 guest      guest      78 Sep 13 13:06 guest
drwx-----. 15 guest1     guest1     4096 Sep 13 13:17 guest1
[guest1@adkekisheva ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/adkekisheva
lsattr: Permission denied While reading flags on /home/guest
----- /home/guest1 ..
```

Рис. 5: Просмотр прав и расширенных атрибутов директорий

```
[guest1@adkekisheva ~]$ mkdir dir1
[guest1@adkekisheva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Desktop
drwxrwxr-x. 2 guest1 guest1 6 Sep 13 13:36 dir1
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Documents
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Downloads
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Music
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Pictures
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Public
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Templates
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Videos
[guest1@adkekisheva ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
```

Рис. 6: Создание папки и просмотр её прав и расширенных атрибутов

## Шаг 9 - Применение команды chmod

```
[guest1@adkekisheva ~]$ chmod 000 dir1
[guest1@adkekisheva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Desktop
d------. 2 guest1 guest1 6 Sep 13 13:36 dir1
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Documents
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Downloads
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Music
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Pictures
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Public
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Templates
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Videos
[guest1@adkekisheva ~]$ echo "hello" > /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: Permission denied
[guest1@adkekisheva ~]$ ls -l /home/guest1/dir1
ls: cannot open directory /home/guest1/dir1: Permission denied
```

Рис. 7: Команда chmod

Таблицу лучше смотреть в файлах pdf и rd.

```
[adkekiheva@adkekiheva ~]$ chmod 100 dir3
[adkekiheva@adkekiheva ~]$ cd dir3
[adkekiheva@adkekiheva dir3]$ ls
ls: cannot open directory .: Permission denied
[adkekiheva@adkekiheva dir3]$ cat file1
nastya
[adkekiheva@adkekiheva dir3]$ ls
ls: cannot open directory .: Permission denied
[adkekiheva@adkekiheva dir3]$ touch f2
touch: cannot touch 'f2': Permission denied
[adkekiheva@adkekiheva dir3]$ mv file1 f4
mv: cannot move 'file1' to 'f4': Permission denied
[adkekiheva@adkekiheva dir3]$ cd
[adkekiheva@adkekiheva ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./gitflow-installer.sh
----- ./gitflow
----- ./work
----- ./biblatex-ms-4.0.tds.tgz
----- ./dir2
lsattr: Permission denied While reading flags on ./dir3
[adkekiheva@adkekiheva ~]$ chmod 300 dir3
[adkekiheva@adkekiheva ~]$ cd dir3
[adkekiheva@adkekiheva dir3]$ touch f2
[adkekiheva@adkekiheva dir3]$ mv f2 f3
[adkekiheva@adkekiheva dir3]$ rm f3
[adkekiheva@adkekiheva dir3]$ cat file1
nastya
[adkekiheva@adkekiheva dir3]$ touch f2
```



```

[adkekisheva@adkekisheva ~]$ chmod 200 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
bash: cd: dir3: Permission denied
[adkekisheva@adkekisheva ~]$ cat dir3/file1
cat: dir3/file1: Permission denied
[adkekisheva@adkekisheva ~]$ chmod 400 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
bash: cd: dir3: Permission denied
[adkekisheva@adkekisheva ~]$ echo "nastya_kekisheva" > dir3/file2
bash: dir3/file2: Permission denied
[adkekisheva@adkekisheva ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./gitflow-installer.sh
----- ./gitflow
----- ./work
----- ./biblatex-ms-4.0.tds.tgz
----- ./dir2
----- ./dir3
[adkekisheva@adkekisheva ~]$ chmod 500 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ ls
file1 file1A file2
[adkekisheva@adkekisheva dir3]$ cat file1
nastya
[adkekisheva@adkekisheva dir3]$ touch f3
touch: cannot touch 'f3': Permission denied
[adkekisheva@adkekisheva dir3]$ ls
file1 file1A file2
[adkekisheva@adkekisheva dir3]$ ls -l
total 12
-r-x----- 1 adkekisheva adkekisheva 7 Sep 16 11:18 file1

```

```
[adkekisheva@adkekisheva ~]$ chmod 600 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
2 bash: cd: dir3: Permission denied
[adkekisheva@adkekisheva ~]$ echo "nastya_kekisheva" > dir3/file:
bash: dir3/file1: Permission denied
4 [adkekisheva@adkekisheva ~]$ chmod 700 dir3
[adkekisheva@adkekisheva ~]$ echo "nastya_kekisheva" > dir3/file:
bash: dir3/file1: Permission denied
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ cat file1
nastya
[adkekisheva@adkekisheva dir3]$ touch f4
[adkekisheva@adkekisheva dir3]$ mv f4 f3
[adkekisheva@adkekisheva dir3]$ rm f3
5 [adkekisheva@adkekisheva dir3]$ cat >> file
fgnjsnk
6 ^C
[adkekisheva@adkekisheva dir3]$ cat >> file1
7 bash: file1: Permission denied
8 [adkekisheva@adkekisheva dir3]$ ls -l
total 16
-rw-rw-r--. 1 adkekisheva adkekisheva  8 Sep 16 12:44 file
9 -r-x-----. 1 adkekisheva adkekisheva  7 Sep 16 11:18 file1
-rw-rw-r--. 1 adkekisheva adkekisheva  7 Sep 16 11:44 file1A
-rw-rw-r--. 1 adkekisheva adkekisheva 17 Sep 16 12:31 file2
[adkekisheva@adkekisheva dir3]$ chmod 600 file1
[adkekisheva@adkekisheva dir3]$ ls -l
total 16
-rw-rw-r--. 1 adkekisheva adkekisheva  8 Sep 16 12:44 file
-rw-----. 1 adkekisheva adkekisheva  7 Sep 16 11:18 file1
-rw-rw-r--. 1 adkekisheva adkekisheva  7 Sep 16 11:44 file1A
-rw-rw-r--. 1 adkekisheva adkekisheva 17 Sep 16 12:31 file2
```

Рис. 10: Эксперимент на права доступа - часть 3

```
[adkekisheva@adkekisheva ~]$ chmod 700 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ ls -
ls: cannot access -: No such file or directory
[adkekisheva@adkekisheva dir3]$ ls -l
total 16
-rw-rw-r--. 1 adkekisheva adkekisheva  0 Sep 16 13:02 f3
-rw-rw-r--. 1 adkekisheva adkekisheva  8 Sep 16 12:44 file
-rwx-----. 1 adkekisheva adkekisheva  7 Sep 16 13:27 file1
-rw-rw-r--. 1 adkekisheva adkekisheva  7 Sep 16 11:44 file1A
-rw-rw-r--. 1 adkekisheva adkekisheva 17 Sep 16 12:31 file2
[adkekisheva@adkekisheva dir3]$ ls
f3 file file1 file1A file2
[adkekisheva@adkekisheva dir3]$ cat file1
yyyyyy
[adkekisheva@adkekisheva dir3]$ cd
[adkekisheva@adkekisheva ~]$ echo "yyyyyy---fffff" > dir3/file1
[adkekisheva@adkekisheva ~]$ cat dir3/file1
yyyyyy---fffff
[adkekisheva@adkekisheva ~]$ chmod 500 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ ls
f3 file file1 file1A file2
[adkekisheva@adkekisheva dir3]$ chmod 400 file1
[adkekisheva@adkekisheva dir3]$ cd
[adkekisheva@adkekisheva ~]$ chmod 100 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ cat file1
yyyyyy---fffff
[adkekisheva@adkekisheva dir3]$ echo "ffgg" > file1
bash: file1: Permission denied
[adkekisheva@adkekisheva dir3]$ chmod 500 file1
[adkekisheva@adkekisheva dir3]$ cd
[adkekisheva@adkekisheva ~]$ chmod 300 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ ls
ls: cannot open directory -: Permission denied
[adkekisheva@adkekisheva dir3]$
```

```
[adkekisheva@adkekisheva ~]$ chmod 300 dir3
[adkekisheva@adkekisheva ~]$ echo "nastya_kfgfgfgf" > dir3/file1
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ ls
ls: cannot open directory .: Permission denied
[adkekisheva@adkekisheva dir3]$ touch f2
[adkekisheva@adkekisheva dir3]$ rm f2
[adkekisheva@adkekisheva dir3]$ cat file1
nastya_kfgfgfgf
[adkekisheva@adkekisheva dir3]$ mv file1 f1
[adkekisheva@adkekisheva dir3]$ ls
ls: cannot open directory .: Permission denied
[adkekisheva@adkekisheva dir3]$ mv f1 file1
[adkekisheva@adkekisheva dir3]$ cd
[adkekisheva@adkekisheva ~]$ chmod 400 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
bash: cd: dir3: Permission denied
[adkekisheva@adkekisheva ~]$ echo "nastya_kfgfgfgf" > dir3/file1
bash: dir3/file1: Permission denied
[adkekisheva@adkekisheva ~]$ chmod 500 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ touch f5
touch: cannot touch 'f5': Permission denied
[adkekisheva@adkekisheva dir3]$ cat >> file1
oppp^C
[adkekisheva@adkekisheva dir3]$ cat file1
nastya_kfgfgfgf
[adkekisheva@adkekisheva dir3]$ cd
[adkekisheva@adkekisheva ~]$ echo "yyyyyy" > dir3/file1
[adkekisheva@adkekisheva ~]$ cat dir3/file1
```

Рис. 12: Эксперимент на права доступа - часть 5

## Шаг 11 - таблица «Минимальные права для совершения операций»

Операция	Права на директорию	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)

1. Выполнила лабораторную работу в необходимой последовательности;
2. Заполнила таблицу «Установленные права и разрешённые действия»;
3. Заполнила таблицу «Минимально необходимые права для выполнения операций внутри директории».