

# Лабораторная работа № 2

## Дискреционное разграничение прав в Linux. Основные атрибуты

Соболевский Денис Андреевич

### Содержание

Цель работы .....	1
Задание .....	1
Теоретическое введение .....	1
Выполнение лабораторной работы.....	2
Выводы .....	7
Список литературы .....	7

### Цель работы

Целью данной работы является 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.

### Задание

1. Создать новую учетную запись guest.
2. Выполнить операции в новой учетной записи.
3. Сформировать таблицу “Установленные права и разрешенные действия”.
4. Сформировать таблицу “Минимальные права для совершения операций”.

### Теоретическое введение

- Операционная система — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.
- Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не

может поменять содержимое ваших документов или повредить системные файлы.

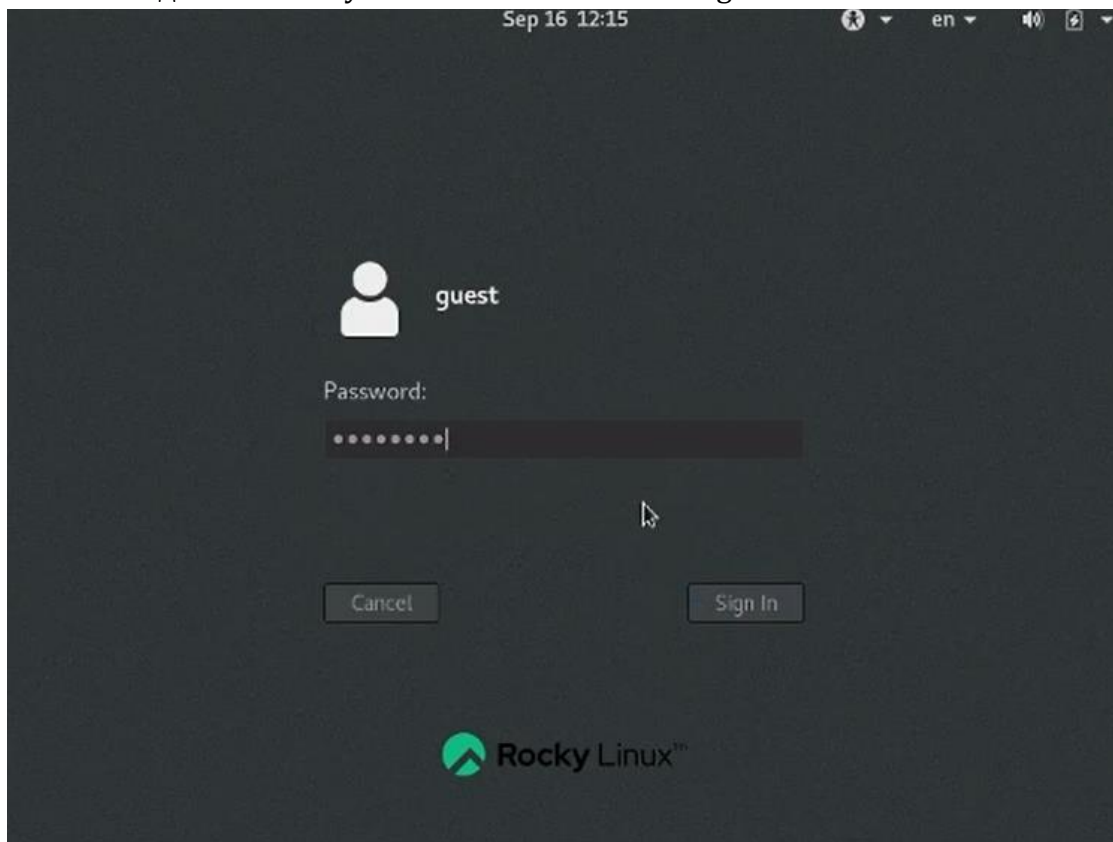
## Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора):

```
root@user:/home/dasobolevskiy
File Edit View Search Terminal Help
[dasobolevskiy@user ~]$ sudo su
[sudo] password for dasobolevskiy:
[root@user dasobolevskiy]# useradd guest
[root@user dasobolevskiy]#
```

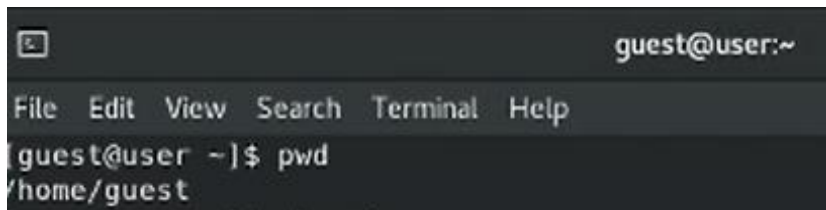
### *Создание и настройка новой учетной записи*

2. Войдем в систему от имени пользователя guest



### *Вход в систему*

3. Определим директорию, в которой мы находимся.

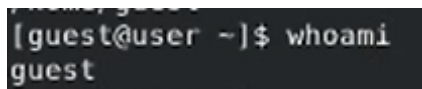
A terminal window with a dark background. The title bar shows a window icon and the text "guest@user:~". The menu bar contains "File", "Edit", "View", "Search", "Terminal", and "Help". The command prompt is "[guest@user ~]\$". The command "pwd" has been entered, and the output is "/home/guest".

```
guest@user:~  
File Edit View Search Terminal Help  
[guest@user ~]$ pwd  
/home/guest
```

### *Определение директории*

Мы находимся в домашней директории.

4. Уточним имя пользователя командой whoami.

A terminal window showing the command "whoami" and its output "guest".

```
[guest@user ~]$ whoami  
guest
```

### *Уточнение имени пользователя*

5. Уточним имя пользователя, его группу, а также группы, куда входит пользователь.

A terminal window showing the command "id" and its output, which lists user and group IDs, groups, and context information.

```
[guest@user ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@user ~]$
```

### *Уточнение информации о пользователе*

Имя пользователя совпадает с приглашением в командной строке.

6. Просмотрим файл /etc/passwd.

```
guest@user:~  
File Edit View Search Terminal Help  
setroubleshoot:x:991:984::/var/lib/setroubleshoot:/sbin/nologin  
saslauth:x:990:76:Saslauthd user:/run/saslauthd:/sbin/nologin  
dnsmasq:x:983:983:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
sssd:x:982:982:User for sssd:/:/sbin/nologin  
clevis:x:981:981:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin  
cockpit-ws:x:980:979:User for cockpit web service:/nonexisting:/sbin/nologin  
cockpit-wsinstance:x:979:978:User for cockpit-ws instances:/nonexisting:/sbin/nologin  
flatpak:x:978:977:User for flatpak system helper:/:/sbin/nologin  
colord:x:977:976:User for colord:/var/lib/colord:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:976:975::/run/gnome-initial-setup:/sbin/nologin  
pesign:x:975:974:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
rngd:x:974:973:Random Number Generator Daemon:/var/lib/rngd:/sbin/nologin  
tcpdump:x:72:72::/:/sbin/nologin  
dasobolevskiy:x:1000:1000:dasobolevskiy:/home/dasobolevskiy:/bin/bash  
vboxadd:x:973:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@user ~]$
```

### Содержимое файла

Найдем в нём свою учётную запись.

```
[guest@user ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001::/home/guest:/bin/bash
```

Учетная запись *guest* в файле */etc/passwd*

uid = 1001, gid = 1001. Совпадают со значениями, полученными в предыдущих пунктах.

7. Определим существующие в системе директории.

```
[guest@user ~]$ ls -l /home/  
total 8  
drwx-----. 18 dasobolevskiy dasobolevskiy 4096 Sep 16 11:06 dasobolevskiy  
drwx-----. 15 guest guest 4096 Sep 16 12:15 guest
```

Существующие в системе директории

Получили список поддиректорий директории */home*. На обеих директориях установлены права *drwx---*.

8. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории */home*.

```
[guest@user ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/dasobolevskiy
----- /home/guest
```

### *Расширенные атрибуты*

Удалось увидеть расширенные атрибуты директории текущего пользователя. Не удалось увидеть атрибуты директории другого пользователя.

9. Создадим в домашней директории поддиректорию dir1 и выведем права доступа и расширенные атрибуты.

```
[guest@user ~]$ mkdir dir1
[guest@user ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Desktop
drwxrwxr-x. 2 guest guest 6 Sep 16 12:21 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Music
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Videos
```

### *Создание поддиректории*

10. Снимем с директории dir1 все атрибуты командой `chmod 000 dir1`.

```
[guest@user ~]$ chmod 000 dir1
[guest@user ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Desktop
d------. 2 guest guest 6 Sep 16 12:21 dir1
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Music
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 12:15 Videos
```

### *Снятие всех атрибутов*

11. Попытаемся создать в директории dir1 файл file1.

```
[guest@user ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
```

### *Создание file1*

Мы получили отказ, так как у нас нет прав на создание. Из-за этого файл не был создан.

## 12. Заполним таблицу «Установленные права и разрешённые действия».

Права директории	Права файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Создание файла
(000)	(000)	-	-	-	-	-	-
(000)	(100)	-	-	-	-	-	-
(000)	(200)	-	-	-	-	-	-
(000)	(300)	-	-	-	-	-	-
(000)	(400)	-	-	-	-	-	-
(000)	(500)	-	-	-	-	-	-
(000)	(600)	-	-	-	-	-	-
(000)	(700)	-	-	-	-	-	-
(100)	(000)	-	-	-	+	-	-
(100)	(100)	-	-	-	+	-	-
(100)	(200)	-	+	-	+	-	-
(100)	(300)	-	+	-	+	-	-
(100)	(400)	-	-	+	+	-	-
(100)	(500)	-	+	+	+	-	-
(100)	(600)	-	+	+	+	-	-
(100)	(700)	-	-	-	+	-	-
(200)	(000)	-	-	-	-	-	-
(200)	(100)	-	-	-	-	-	-
(200)	(200)	-	-	-	-	-	-
(200)	(300)	-	-	-	-	-	-
(200)	(400)	-	-	-	-	-	-
(200)	(500)	-	-	-	-	-	-
(200)	(600)	-	-	-	-	-	-
(200)	(700)	-	-	-	-	-	-
(300)	(000)	+	-	-	+	-	+
(300)	(100)	+	-	-	+	-	+
(300)	(200)	+	+	-	+	-	+

Таблица 2.1

## 13. Заполним таблицу «Минимальные права для совершения операций».

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	(300)	(000)
Удаление файла	(300)	(000)
Чтение файла	(100)	(400)
Запись в файл	(100)	(200)
Переименование файла	(300)	(000)
Создание поддиректории	(300)	(000)
Удаление поддиректории	(300)	(000)

Таблица 2.2

## Выводы

В данной лабораторной работе были изучены средства ограничения прав для отдельных учетных записей.

## Список литературы

[1] <https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux>

[2] <https://wiki.astralinux.ru/kb/diskretnionnye-i-mandatnye-razgranicheniya-dostupa-k-resursu-samba-158603114.html>