

# Отчет по лабораторной работе №3

Дискреционные разграничения прав в Linux. Два пользователя

Евсеева Дарья Олеговна

24 сентября, 2022

# Содержание

Цель работы	4
Задание	5
Теоретическое введение	6
Выполнение лабораторной работы	7
1. Создание и добавление пользователя в группу . . . . .	7
2. Заполнение таблиц прав доступа. . . . .	10
Выводы	14
Список литературы	15

## Список иллюстраций

1	Создание пользователя guest2 . . . . .	7
2	Добавление пользователя в группу . . . . .	7
3	Проверка текущей директории guest . . . . .	8
4	Проверка текущей директории guest2 . . . . .	8
5	Вывод информации о пользователе guest . . . . .	8
6	Вывод информации о пользователе guest2 . . . . .	8
7	Просмотр файла /etc/group (1) . . . . .	9
8	Просмотр файла /etc/group (2) . . . . .	9
9	Регистрация пользователя в группе . . . . .	9
10	Изменение атрибутов директорий . . . . .	9
11	Проверка прав и действий (1) . . . . .	10
12	Проверка прав и действий (2) . . . . .	10
13	Проверка прав и действий (3) . . . . .	10
14	Проверка прав и действий (4) . . . . .	11
15	Установленные права и действия (1) . . . . .	11
16	Установленные права и действия (2) . . . . .	12
17	Установленные права и действия (3) . . . . .	12
18	Установленные права и действия (4) . . . . .	13
19	Минимальные права для совершения операций . . . . .	13

## Цель работы

Целью данной работы является получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

## Задание

1. Создать второго гостевого пользователя и добавить его в группу.
2. Заполнить таблицы прав доступа для групп.

# Теоретическое введение

Дискреционное разграничение доступа — подход к разграничению доступа, предполагающий назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей.

# Выполнение лабораторной работы

Выполнять работу будем в операционной системе, установленной при выполнении первой лабораторной работы.

## 1. Создание и добавление пользователя в группу

Для начала, используя учетную запись администратора, создадим пользователя guest2 и установим для него пароль.

```
[doevseeva@doevseeva ~]$ su
Password:
[root@doevseeva doevseeva]# useradd guest2
[root@doevseeva doevseeva]# passwd guest2
Changing password for user guest2.
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@doevseeva doevseeva]#
```

Рис. 1: Создание пользователя guest2

Далее добавим созданного пользователя в группу guest.

```
[root@doevseeva doevseeva]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@doevseeva doevseeva]#
```

Рис. 2: Добавление пользователя в группу

Войдем в систему от имени пользователя guest на одной консоли, и от имени созданного пользователя guest2 на второй консоли. Также проверим текущие директории пользователей с помощью команды pwd.

```
[root@doevseeva doevseeva]# su - guest
[guest@doevseeva ~]$ pwd
/home/guest
[guest@doevseeva ~]$
```

Рис. 3: Проверка текущей директории guest

```
[doevseeva@doevseeva ~]$ su - guest2
Password:
[guest2@doevseeva ~]$ pwd
/home/guest2
[guest2@doevseeva ~]$
```

Рис. 4: Проверка текущей директории guest2

Мы видим, что для обоих пользователей результат выполнения команды совпадает с приглашением командной строки.

Далее выполним команду `id` для просмотра информации о пользователях. Также проверим вывод команд `groups`, `id -Gn` и `id -G`, сравнив результаты.

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

Рис. 5: Вывод информации о пользователе guest

```
[guest2@doevseeva ~]$ id
uid=1002(guest2) gid=1002(guest2) groups=1002(guest2),1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@doevseeva ~]$ groups guest2
guest2 : guest2 guest
[guest2@doevseeva ~]$ id -Gn
guest2 guest
[guest2@doevseeva ~]$ id -G
1002 1001
[guest2@doevseeva ~]$
```

Рис. 6: Вывод информации о пользователе guest2

Здесь мы видим, что для каждого из пользователей выводы команд соответствуют действительности и не противоречат друг другу. Также можно заметить, что пользователя `guest2` входит в две группы: `guest2` и `guest`.



Посмотрим содержимое файла /etc/group.

```
[guest@doevseeva ~]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
```

Рис. 7: Просмотр файла /etc/group (1)

```
doevseeva:x:1000:
vboxsf:x:976:
guest:x:1001:guest2
guest2:x:1002:
[guest@doevseeva ~]$
```

Рис. 8: Просмотр файла /etc/group (2)

Мы видим, что в последних двух строках вывода содержится информация о группах guest и guest2. Здесь мы также можем видеть, что пользователя guest2 дополнительно входит в группу guest.

Выполним регистрацию пользователя guest2 в группе guest.

```
[guest2@doevseeva ~]$ newgrp guest
[guest2@doevseeva ~]$
```

Рис. 9: Регистрация пользователя в группе

Теперь от имени пользователя guest изменим права его домашней директории, разрешив все действия для пользователей группы, а затем снимем все атрибуты с директории dir1.

```
[guest@doevseeva ~]$ chmod g+rwX /home/guest
[guest@doevseeva ~]$ ls -l dir1/
total 4
----- 1 guest guest 4 Sep 23 21:09 file1
[guest@doevseeva ~]$ chmod 000 dir1/
[guest@doevseeva ~]$ ls -l
total 0
d----- 2 guest guest 19 Sep 23 21:17 dir1
[guest@doevseeva ~]$
```

Рис. 10: Изменение атрибутов директорий

## 2. Заполнение таблиц прав доступа.

Заполним таблицу “Установленные права и разрешенные действия для групп”, меняя атрибуты от имени пользователя `guest` и делая проверку от имени пользователя `guest2`, определив опытным путем, какие операции разрешены, а какие нет.

```
[guest@doevseeva ~]$ chmod 070 dir1/
[guest@doevseeva ~]$ ls -l
total 0
d---rwx---. 2 guest guest 19 Sep 23 22:54 dir1
[guest@doevseeva ~]$
```

Рис. 11: Проверка прав и действий (1)

```
[guest2@doevseeva guest]$ touch dir1/file2
[guest2@doevseeva guest]$ rm dir1/file2
[guest2@doevseeva guest]$ echo "ssdsdd" > dir1/file1
bash: dir1/file1: Permission denied
[guest2@doevseeva guest]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest2@doevseeva guest]$ cd dir1/
[guest2@doevseeva dir1]$ ls
file1
[guest2@doevseeva dir1]$ cd ..
[guest2@doevseeva guest]$ mv dir1/file1 dir1/file2
[guest2@doevseeva guest]$ mv dir1/file2 dir1/file1
[guest2@doevseeva guest]$
[guest2@doevseeva guest]$ chmod 030 dir1/file1
chmod: changing permissions of 'dir1/file1': Operation not permitted
[guest2@doevseeva guest]$
```

Рис. 12: Проверка прав и действий (2)

```
[guest@doevseeva ~]$ chmod 050 dir1/file1
[guest@doevseeva ~]$
[guest@doevseeva ~]$ chmod 010 dir1/
[guest@doevseeva ~]$ ls -l
total 0
d-----x---. 2 guest guest 19 Sep 23 23:31 dir1
[guest@doevseeva ~]$
```

Рис. 13: Проверка прав и действий (3)

```
[guest2@doevseeva guest]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest2@doevseeva guest]$ rm dir1/file1
rm: remove write-protected regular file 'dir1/file1'? y
rm: cannot remove 'dir1/file1': Permission denied
[guest2@doevseeva guest]$ echo "gggg" > dir1/file1
bash: dir1/file1: Permission denied
[guest2@doevseeva guest]$ cat dir1/file1
gggg
[guest2@doevseeva guest]$ cd dir1/
[guest2@doevseeva dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest2@doevseeva dir1]$ cd ..
[guest2@doevseeva guest]$ mv dir1/file1 dir1/file2
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
[guest2@doevseeva guest]$
```

Рис. 14: Проверка прав и действий (4)

Итак, закончим заполнение таблицы “Установленные права и действия для групп”.

Установленные права и разрешенные действия для групп

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d----- (000)	- - - - - (000)	-	-	-	-	-	-	-	-
d---x--- (010)	(000)	-	-	-	-	+	-	-	-
d---w--- (020)	(000)	-	-	-	-	-	-	-	-
d---wx--- (030)	(000)	+	+	-	-	+	-	+	-
d---r--- (040)	(000)	-	-	-	-	-	+	-	-
d---x--- (050)	(000)	-	-	-	-	+	+	-	-
d---rw--- (060)	(000)	-	-	-	-	-	+	-	-
d---rwx--- (070)	(000)	+	+	-	-	+	+	+	-
- - - - -x--- (000)	(010)	-	-	-	-	-	-	-	-
(010)	(010)	-	-	-	-	+	-	-	-
(020)	(010)	-	-	-	-	-	-	-	-
(030)	(010)	+	+	-	-	+	-	+	-
(040)	(010)	-	-	-	-	-	+	-	-
(050)	(010)	-	-	-	-	+	+	-	-
(060)	(010)	-	-	-	-	-	+	-	-
(070)	(010)	+	+	-	-	+	+	+	-

Рис. 15: Установленные права и действия (1)

(000)	- - - - W - - - - (020)	-	-	-	-	-	-	-	-
(010)	(020)	-	-	+	-	+	-	-	-
(020)	(020)	-	-	-	-	-	-	-	-
(030)	(020)	+	+	+	-	+	-	+	-
(040)	(020)	-	-	-	-	-	+	-	-
(050)	(020)	-	-	+	-	+	+	-	-
(060)	(020)	-	-	-	-	-	+	-	-
(070)	(020)	+	+	+	-	+	+	+	-
(000)	- - - - W X - - - - (030)	-	-	-	-	-	-	-	-
(010)	(030)	-	-	+	-	+	-	-	-
(020)	(030)	-	-	-	-	-	-	-	-
(030)	(030)	+	+	+	-	+	-	+	-
(040)	(030)	-	-	-	-	-	+	-	-
(050)	(030)	-	-	+	-	+	+	-	-
(060)	(030)	-	-	-	-	-	+	-	-
(070)	(030)	+	+	+	-	+	+	+	-
(000)	- - - - T - - - - (040)	-	-	-	-	-	-	-	-
(010)	(040)	-	-	-	+	+	-	-	-

Рис. 16: Установленные права и действия (2)

(020)	(040)	-	-	-	-	-	-	-	-
(030)	(040)	+	+	-	+	+	-	+	-
(040)	(040)	-	-	-	-	-	+	-	-
(050)	(040)	-	-	-	+	+	+	-	-
(060)	(040)	-	-	-	-	-	+	-	-
(070)	(040)	+	+	-	+	+	+	+	-
(000)	- - - - T X - - - - (050)	-	-	-	-	-	-	-	-
(010)	(050)	-	-	-	+	+	-	-	-
(020)	(050)	-	-	-	-	-	-	-	-
(030)	(050)	+	+	-	+	+	-	+	-
(040)	(050)	-	-	-	-	-	+	-	-
(050)	(050)	-	-	-	+	+	+	-	-
(060)	(050)	-	-	-	-	-	+	-	-
(070)	(050)	+	+	-	+	+	+	+	-
(000)	- - - - T W - - - - (060)	-	-	-	-	-	-	-	-
(010)	(060)	-	-	+	+	+	-	-	-
(020)	(060)	-	-	-	-	-	-	-	-
(030)	(060)	+	+	+	+	+	-	+	-

Рис. 17: Установленные права и действия (3)

(040)	(060)	-	-	-	-	-	+	-	-
(050)	(060)	-	-	+	+	+	+	-	-
(060)	(060)	-	-	-	-	-	+	-	-
(070)	(060)	+	+	+	+	+	+	+	-
(000)	---ГВХ---	-	-	-	-	-	-	-	-
(010)	(070)	-	-	+	+	+	-	-	-
(020)	(070)	-	-	-	-	-	-	-	-
(030)	(070)	+	+	+	+	+	-	+	-
(040)	(070)	-	-	-	-	-	+	-	-
(050)	(070)	-	-	+	+	+	+	-	-
(060)	(070)	-	-	-	-	-	+	-	-
(070)	(070)	+	+	+	+	+	+	+	-

Рис. 18: Установленные права и действия (4)

Теперь, на основании заполненной таблицы определим те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполним таблицу “Минимальные права для совершения операций от имени пользователей, входящих в группу”.

**Минимальные права для совершения операций от имени пользователей входящих в группу**

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	000
Удаление поддиректории	030	000

Рис. 19: Минимальные права для совершения операций

## Выводы

В результате проделанной работы мы приобрели практические навыки работы в консоли с атрибутами файлов для групп пользователей.

## Список литературы

- Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” <https://esystem.rudn.ru/>