

# Отчет по лабораторной работе №3

Основы информационной безопасности

Ничипорова Елена Дмитриевна

## Содержание

Цель работы .....	1
Задание .....	1
Теоретическое введение .....	1
Выполнение лабораторной работы .....	2
Заполнение таблицы 3.1 .....	5
Заполнение таблицы 3.2 .....	8
Выводы.....	9
Список литературы. Библиография .....	9

## Цель работы

Получить практические навыки работы в консоли с атрибутами файлов для групп пользователей.

## Задание

1. Создание пользователя `guest2`, добавление его в группу пользователей `guest`
2. Заполнение таблицы 3.1
3. Заполнение таблицы 3.2 на основе таблицы 3.1.

## Теоретическое введение

**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. [1]

**Группы пользователей Linux** кроме стандартных `root` и `users`, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого

пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен. [2]

- daemon - от имени этой группы и пользователя daemon запускаются сервисы, которым необходима возможность записи файлов на диск.
- sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
- sync - позволяет выполнять команду /bin/sync
- games - разрешает играм записывать свои файлы настроек и историю в определенную папку
- man - позволяет добавлять страницы в директорию /var/cache/man
- lp - позволяет использовать устройства параллельных портов
- mail - позволяет записывать данные в почтовые ящики /var/mail/
- proxy - используется прокси серверами, нет доступа записи файлов на диск
- www-data - с этой группой запускается веб-сервер, она дает доступ на запись /var/www, где находятся файлы веб-документов
- list - позволяет просматривать сообщения в /var/mail
- nogroup - используется для процессов, которые не могут создавать файлов на жестком диске, а только читать, обычно применяется вместе с пользователем nobody.
- adm - позволяет читать логи из директории /var/log
- tty - все устройства /dev/vsa разрешают доступ на чтение и запись пользователям из этой группы
- disk - открывает доступ к жестким дискам /dev/sd\* /dev/hd\*, можно сказать, что это аналог рут доступа.
- dialout - полный доступ к серийному порту
- cdrom - доступ к CD-ROM
- wheel - позволяет запускать утилиту sudo для повышения привилегий
- audio - управление аудиодрайвером
- src - полный доступ к исходникам в каталоге /usr/src/
- shadow - разрешает чтение файла /etc/shadow
- utmp - разрешает запись в файлы /var/log/utmp /var/log/wtmp
- video - позволяет работать с видеодрайвером
- plugdev - позволяет монтировать внешние устройства USB, CD и т д
- staff - разрешает запись в папку /usr/local

## Выполнение лабораторной работы

1. Пользователь guest был создан в лабораторной работе №2, поэтому в этой лабораторной работе его не создаем заново

2. Пароль для пользователя guest тоже был задан в лабораторной работе №2.
3. С правами администратора создаю пользователя guest с помощью команды `useradd`, далее с помощью команды `passwd` задаю пароль пользователю (рис. 1).

```

Rocky Linux 9.2 (Blue Onyx)
Kernel 5.14.0-284.11.1.el9_2.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: root
Password:
Last login: Wed Sep  4 12:16:18 on tty1
[root@localhost ~]# sudo useradd guest2
[root@localhost ~]# sudo passwd guest2
Changing password for user guest2.
New password:
Retype new password: _

```

### Создание пользователя

4. Добавляю пользователя guest2 в группу guest (рис. 2).

```

[root@localhost ~]# sudo gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@localhost ~]# _

```

### Добавление пользователя в группу

5. Зашла на двух разных консолях от имени двух разных пользователей с помощью команды `su <имя пользователя>`
6. Проверяю путь директории, в которой я нахожусь с помощью `pwd`.

Проверка для пользователя guest (рис. 3).

```

[root@localhost ~]# su guest2
[guest2@localhost root]$ pwd
/root
[guest2@localhost root]$

```

### Текущая директория для guest

Проверка для пользователя guest2 (рис. 4).

```

[guest2@localhost root]$ whoami
guest2
[guest2@localhost root]$ id
uid=1001(guest2) gid=1001(guest2) groups=1001(guest2),1000(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@localhost root]$ groups guest2
guest2 : guest2 guest
[guest2@localhost root]$ groups
guest2 guest
[guest2@localhost root]$ id -Gn
guest2 guest
[guest2@localhost root]$ id -G
1001 1000
[guest2@localhost root]$ _

```

### Текущая директория для guest2

Стоит отметить, что вход в терминал от имени пользователей был выполнен в домашней директории пользователя evdvorkina, которую команда `pwd` вывела. Домашней директорией пользователей она не является. Текущая директория с приглашением командной строки совпадает.

7. Проверяю имя пользователей с помощью команды `whoami`, с помощью команды `id` могу увидеть группы, к которым принадлежит пользователь и коды этих групп (gid), команда `groups` просто выведет список групп, в которые входит пользователь.

`id -Gn` - выведет названия групп, которым принадлежит пользователь

`id -G` - выведет только код групп, которым принадлежит пользователь.

Проверка для пользователя `guest2` (рис. 5).

```
[guest@localhost root]$ whoami
guest
[guest@localhost root]$ id
uid=1000(guest) gid=1000(guest) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:system_r:guest_t:guest
[guest@localhost root]$ groups guest
guest : guest
[guest@localhost root]$ groups guest2
guest2 : guest2 guest
[guest@localhost root]$ id -Gn
bash: id -Gn: command not found
[guest@localhost root]$ id -Gn
guest
[guest@localhost root]$ id -G
1000
[guest@localhost root]$ groups
guest
[guest@localhost root]$ _
```

*Информация о пользователе guest2*

Проверка для пользователя `guest` (рис. 5).

```
[guest@localhost root]$ whoami
guest
[guest@localhost root]$ id
uid=1000(guest) gid=1000(guest) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:system_r:guest_t:guest
[guest@localhost root]$ groups guest
guest : guest
[guest@localhost root]$ groups guest2
guest2 : guest2 guest
[guest@localhost root]$ id -Gn
bash: id -Gn: command not found
[guest@localhost root]$ id -Gn
guest
[guest@localhost root]$ id -G
1000
[guest@localhost root]$ groups
guest
[guest@localhost root]$ _
```

*Информация о пользователе guest*

Пользователь `guest2` входит в две группы пользователей: в группу `guest`, потому что я сама его туда добавила, и в группу `guest2`, которая создавалась автоматически при создании пользователя.

8. Вывела интересующее меня содержимое файла `etc/group`, видно, что в группе `guest` два пользователя, а в группе `guest2` один (рис. 7).

```
[guest@localhost root]$ cat /etc/group | grep 'guest'
guest:x:1000:guest2
guest2:x:1001:
[guest@localhost root]$
```

*Содержимое файла `etc/group`*

9. От имени пользователя guest2 регистрирую его в группе guest с помощью команды newgrp (рис. 6).

```
[guest2@localhost root]$ newgrp guest
[guest2@localhost root]$ _
```

#### *Регистрация пользователя в группе*

10. Добавляю права на чтение, запись и исполнение группе пользователей guest (guest, guest2) на директорию home/guest в которой находятся все файлы для последующей работы (рис. 8).

```
[guest@localhost root]$ cd
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ chmod g+rx /home/guest
[guest@localhost ~]$ _
```

#### *Изменение прав директории*

11. От имени пользователя guest снимаю все атрибуты с директории dir1, созданной в предыдущей лабораторной работе. Проверяю, что права действительно сняты (рис. 9).

```
[guest@localhost ~]$ chmod g+rx /home/guest
[guest@localhost ~]$ ls
dir dir1 test
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls
dir dir1 test
[guest@localhost ~]$ ls -l
total 8
-rw-r--r--. 1 guest guest 12 Sep  4 15:10 dir
d----- 2 guest guest 19 Sep  4 15:17 dir1
-rw-r--r--. 1 guest guest  5 Sep  4 15:07 test
[guest@localhost ~]$
```

#### *Изменение прав директории*

### Заполнение таблицы 3.1

Далее проверяю как пользователь guest2 будет взаимодействовать с файлами в этой директории (рис. 10).

```
[guest2@localhost guest]$ cd /home/guest
[guest2@localhost guest]$ ls
dir dir1 test
[guest2@localhost guest]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest2@localhost guest]$ rm dir1/a
rm: cannot remove 'dir1/a': Permission denied
[guest2@localhost guest]$ touch dir1/f1
touch: cannot touch 'dir1/f1': Permission denied
[guest2@localhost guest]$ echo 'test' > dir1/file1
bash: dir1/file1: Permission denied
[guest2@localhost guest]$ chmod 020 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest2@localhost guest]$ _
```

#### *Пример заполнения таблицы 3.1*

Права директории	Права файла	Со зд ан ие фа йл а	Уд ал ен ие фа йл а	За пи сь в фа йл	Чт ен ие фа йл а	См ен а ди ре кто ри и	Пр ос мо тр фа йл ов ди ре кто ри и	Пе ре им ен ов ан ие фа йл	См ен а три бу то в фа йл а
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d-----x-- (010)	----- (000)	-	-	-	-	-	-	-	+
d----w--- (020)	----- (000)	-	-	-	-	-	-	-	-
d----wx-- (030)	----- (000)	+	+	-	-	+	-	+	+
d---r---- (040)	----- (000)	-	-	-	-	-	+	-	-
d---r-x-- (050)	----- (000)	-	-	-	-	+	+	-	+
d---rw--- (060)	----- (000)	-	-	-	-	-	+	-	-
d---rwx-- (070)	----- (000)	+	+	-	-	+	+	+	+
d----- (000)	-----x-- (010)	-	-	-	-	-	-	-	-
d-----x-- (010)	-----x-- (010)	-	-	-	-	-	-	-	+
d----w--- (020)	-----x-- (010)	-	-	-	-	-	-	-	-
d----wx-- (030)	-----x-- (010)	+	+	-	-	+	-	+	+
d---r---- (040)	-----x-- (010)	-	-	-	-	-	+	-	-
d---r-x-- (050)	-----x-- (010)	-	-	-	-	+	+	-	+
d---rw--- (060)	-----x-- (010)	-	-	-	-	-	+	-	-
d---rwx-- (070)	-----x-- (010)	+	+	-	-	+	+	+	+
d----- (000)	-----w--- (020)	-	-	-	-	-	-	-	-
d-----x-- (010)	-----w--- (020)	-	-	+	-	-	-	-	+
d----w--- (020)	-----w--- (020)	-	-	-	-	-	-	-	-
d----wx-- (030)	-----w--- (020)	+	+	+	-	+	-	+	+
d---r---- (040)	-----w--- (020)	-	-	-	-	-	+	-	-
d---r-x-- (050)	-----w--- (020)	-	-	+	-	+	+	-	+
d---rw--- (060)	-----w--- (020)	-	-	-	-	-	+	-	-
d---rwx-- (070)	-----w--- (020)	+	+	+	-	+	+	+	+
d----- (000)	-----wx-- (030)	-	-	-	-	-	-	-	-
d-----x-- (010)	-----wx-- (030)	-	-	+	-	-	-	-	+

Права директории	Права файла	Со зд ан ие фа йл а	Уд ал ен ие фа йл а	За пи сь в фа йл	Чт ен ие фа йл а	См ен а ди ре кто ри и	Пр ос мо тр фа йл ов ди ре кто ри и	Пе ре им ен ов ан ие фа йл	См ен а три бу то в фа йл а
d----w--- (020)	-----wx-- (030)	-	-	-	-	-	-	-	-
d----wx-- (030)	-----wx-- (030)	+	+	+	-	+	-	+	+
d---r---- (040)	-----wx-- (030)	-	-	-	-	-	+	-	-
d---r-x-- (050)	-----wx-- (030)	-	-	+	-	+	+	-	+
d---rw--- (060)	-----wx-- (030)	-	-	-	-	-	+	-	-
d---rwx-- (070)	-----wx-- (030)	+	+	+	-	+	+	+	+
d----- (000)	----r---- (040)	-	-	-	-	-	-	-	-
d-----x-- (010)	----r---- (040)	-	-	-	+	+	-	-	+
d---w--- (020)	----r---- (040)	-	-	-	-	-	-	-	-
d---wx-- (030)	----r---- (040)	+	+	-	+	+	-	+	+
d---r---- (040)	----r---- (040)	-	-	-	-	-	+	-	-
d---r-x-- (050)	----r---- (040)	-	-	-	+	+	+	-	+
d---rw--- (060)	----r---- (040)	-	-	-	-	-	+	-	-
d---rwx-- (070)	----r---- (040)	+	+	-	+	+	+	+	+
d----- (000)	----r-x-- (050)	-	-	-	-	-	-	-	-
d-----x-- (010)	----r-x-- (050)	-	-	-	+	+	-	-	+
d---w--- (020)	----r-x-- (050)	-	-	-	-	-	-	-	-
d---wx-- (030)	----r-x-- (050)	+	+	-	+	+	-	+	+
d---r---- (040)	----r-x-- (050)	-	-	-	-	-	+	-	-
d---r-x-- (050)	----r-x-- (050)	-	-	-	+	+	+	-	+
d---rw--- (060)	----r-x-- (050)	-	-	-	-	-	+	-	-
d---rwx-- (070)	----r-x-- (050)	+	+	-	+	+	+	+	+
d----- (000)	----rw--- (060)	-	-	-	-	-	-	-	-
d-----x-- (010)	----rw--- (060)	-	-	+	+	-	-	-	+
d---w--- (020)	----rw--- (060)	-	-	-	-	-	-	-	-
d---wx-- (030)	----rw--- (060)	+	+	+	+	+	-	+	+

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

Таблица 3.1 «Установленные права и разрешённые действия для групп»

## Заполнение таблицы 3.2

На основе таблицы 3.1 заполняю таблицу 3.2.

Операция	Права на директорию	Права на файл
Создание файла	d----wx-- (030)	----- (000)
Удаление файла	d----wx-- (030)	----- (000)
Чтение файла	d-----x-- (010)	----r--- (040)
Запись в файл	d-----x-- (010)	----w--- (020)
Переименование файла	d----wx-- (030)	----- (000)
Создание поддиректории	d----wx-- (030)	----- (000)
Удаление	d----wx-- (030)	----- (000)



Операция  
поддиректории

Права на директорию

Права на файл

---

Таблица 3.2 «Минимальные права для совершения операций от имени пользователей входящих в группу»

## Выводы

Были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей

## Список литературы. Библиография

[0] Методические материалы курса

[1] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>

[2] Группы пользователей: [https://losst.pro/gruppy-polzovatelej-linux#Что\\_такое\\_группы](https://losst.pro/gruppy-polzovatelej-linux#Что_такое_группы)