

# Отчет по лабораторной работе №3

## Основы информационной безопасности

Швецов Михаил, НКАбд-01-23

### Содержание

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

### 1 Цель работы

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

### 2 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.

### 3 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/
- проху - 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

## 4 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).

```

[mrshvecov@mrshvecov ~]$ sudo useradd guest2
[sudo] пароль для mrshvecov:
Попробуйте ещё раз.
[sudo] пароль для mrshvecov:
[mrshvecov@mrshvecov ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - на основе слова из словаря
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[mrshvecov@mrshvecov ~]$

```

### *Создание пользователя*

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

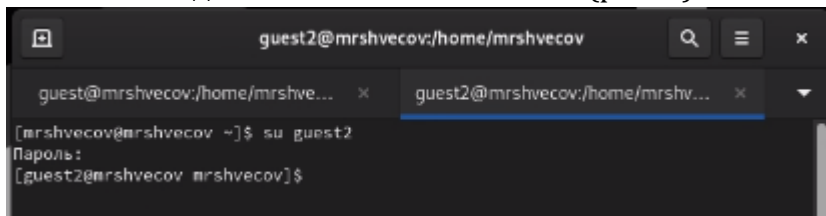
```

[mrshvecov@mrshvecov ~]$ sudo groupadd -a guest2 guest
Добавление пользователя guest2 в группу guest
[mrshvecov@mrshvecov ~]$

```

### *Добавление пользователя в группу*

5. Зашла на двух разных консолях от имени двух разных пользователей с помощью команды `su <имя пользователя>` (рис. 3).



```

guest2@mrshvecov:/home/mrshvecov
guest@mrshvecov:/home/mrshvecov x guest2@mrshvecov:/home/mrshvecov x
[mrshvecov@mrshvecov ~]$ su guest2
Пароль:
[guest2@mrshvecov mrshvecov]$

```

### *Вход в терминал от имени другого пользователя*

6. Проверяю путь директории, в которой я нахожусь с помощью `pwd`.

Проверка для пользователя guest (рис. 4).

```

Пароль:
[guest@mrshvecov mrshvecov]$ pwd
/home/mrshvecov
[guest@mrshvecov mrshvecov]$

```

### *Текущая директория для guest*

Проверка для пользователя guest2 (рис. 5).

```

Пароль:
[guest2@mrshvecov mrshvecov]$ pwd
/home/mrshvecov
[guest2@mrshvecov mrshvecov]$

```

### *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. 6).

```
[guest2@mrshvecov mrshvecov]$ whoami
guest2
[guest2@mrshvecov mrshvecov]$ id
uid=1002(guest2) gid=1002(guest2) rгруппы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@mrshvecov mrshvecov]$ groups guest2
guest2 : guest2 guest
[guest2@mrshvecov mrshvecov]$ dgroups
bash: dgroups: команда не найдена...
[guest2@mrshvecov mrshvecov]$ groups
guest2 guest
[guest2@mrshvecov mrshvecov]$ id -Gn
guest2 guest
[guest2@mrshvecov mrshvecov]$ id -G
1002 1001
[guest2@mrshvecov mrshvecov]$ groups
guest2 guest
[guest2@mrshvecov mrshvecov]$
```

*Информация о пользователе guest2*

Проверка для пользователя guest (рис. 7).

```
[guest@mrshvecov mrshvecov]$ whoami
guest
[guest@mrshvecov mrshvecov]$ id
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@mrshvecov mrshvecov]$ groups guest
guest : guest
[guest@mrshvecov mrshvecov]$ groups guest2
guest2 : guest2 guest
[guest@mrshvecov mrshvecov]$ id -Gn
guest
[guest@mrshvecov mrshvecov]$ id -G
1001
[guest@mrshvecov mrshvecov]$ groups
guest
[guest@mrshvecov mrshvecov]$ cat /etc/
```

*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 интересное меня содержимое файла etc/group, видно, что в группе guest два пользователя, а в группе guest2 один (рис. 8).

```
[guest@mrshvecov mrshvecov]$ cat /etc/group | grep 'guest'
guest:x:1001:guest2
guest2:x:1002:
[guest@mrshvecov mrshvecov]$
```

*Содержимое файла etc/group*

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

```
[guest2@mrshvecov mrshvecov]$ id -u
1002 1001
[guest2@mrshvecov mrshvecov]$ groups
guest2 guest
[guest2@mrshvecov mrshvecov]$ newgrp guest
```

### Регистрация пользователя в группе

- 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. 10).

```
[guest@evdvorkina evdvorkina]$ cd
[guest@evdvorkina ~]$ pwd
/home/guest
[guest@evdvorkina ~]$ chmod g+rxw /home/guest
```

### Изменение прав директории

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

```
[guest2@mrshvecov mrshvecov]$ newgrp guest
[guest2@mrshvecov mrshvecov]$ cd /home/guest
[guest2@mrshvecov guest]$ ls
dir1 Видео Загрузки Музыка Рабочий стол
test Документы Изображения Общедоступные Шаблоны
[guest2@mrshvecov guest]$ ls dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
[guest2@mrshvecov guest]$ rm dir1/a
rm: невозможно удалить 'dir1/a': Отказано в доступе
[guest2@mrshvecov guest]$ touch dir1/f1
touch: невозможно выполнить touch для 'dir1/f1': Отказано в доступе
[guest2@mrshvecov guest]$ echo 'test' > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@mrshvecov guest]$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
[guest2@mrshvecov guest]$ chmod 020 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest2@mrshvecov guest]$
```

### Изменение прав директории

## 4.1 Заполнение таблицы 3.1

Далее проверяю как пользователь guest2 будет взаимодействовать с файлами в этой директории (рис. 12).

```
[guest2@mrshvecov mrshvecov]$ newgrp guest
[guest2@mrshvecov mrshvecov]$ cd /home/guest
[guest2@mrshvecov guest]$ ls
dir1 Видео Загрузки Музыка Рабочий стол
test Документы Изображения Общедоступные Шаблоны
[guest2@mrshvecov guest]$ ls dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
[guest2@mrshvecov guest]$ rm dir1/a
rm: невозможно удалить 'dir1/a': Отказано в доступе
[guest2@mrshvecov guest]$ touch dir1/f1
touch: невозможно выполнить touch для 'dir1/f1': Отказано в доступе
[guest2@mrshvecov guest]$ echo 'test' > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@mrshvecov guest]$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
[guest2@mrshvecov guest]$ chmod 020 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest2@mrshvecov 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 а	Чт ен ие фа йл а	См ен а ди ре кт ор ии	Пр ос мо тр фа йл ов ди ре кт ор ии	Пе ре им ен ов ан ие фа йл а	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)	-	-	+	-	-	-	-	+
d----w--- (020)	-----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 кт ор ии	Пр ос мо тр фа йл	Пе ре им ен ов ан ие фа йл	См ен а три бу то в фа йл а
							ов ди ре кт ор ии		
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)	+	+	+	+	+	-	+	+
d---r---- (040)	----rw--- (060)	-	-	-	-	-	+	-	-
d---r-x-- (050)	----rw--- (060)	-	-	+	+	+	+	-	+

		Права							
		Права директории				Права файла			
		Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена имени	Промежуточные файлы	Переименование файла	Смена атрибутов файла
Права директории	Права файла								
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»

## 4.2 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 поддиректории	d----wx-- (030)	----- (000)

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



## 5 Выводы

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

## 6 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)