

# **Отчет по лабораторной работе №3**

**Информационная безопасность**

Чекалова Лилия Руслановна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Выводы</b>	<b>14</b>
	<b>Список литературы</b>	<b>15</b>

## **Список таблиц**

## Список иллюстраций

4.1	Создание учетных записей . . . . .	8
4.2	Вход и информация о группах . . . . .	9
4.3	Содержимое файла etc/group . . . . .	10
4.4	Регистрация guest2 в группе guest . . . . .	10
4.5	Изменение прав доступа к /home/guest . . . . .	11
4.6	Изменение и просмотр прав доступа папки dir1 . . . . .	11
4.7	Снятие атрибутов с file1 . . . . .	11
4.8	Проверка доступных действий . . . . .	12
4.9	Установленные права и разрешенные действия, 1 . . . . .	12
4.10	Установленные права и разрешенные действия, 2 . . . . .	13
4.11	Установленные права и разрешенные действия, 3 . . . . .	13
4.12	Минимальные права для совершения операций . . . . .	13

# 1 Цель работы

- Приобретение практических навыков работы в консоли с атрибутами файлов для групп пользователей

## 2 Задание

- Создание двух учетных записей
- Объединение пользователей в одну группу
- Изменение прав доступа одним пользователем и проверка возможных в рамках заданных прав доступа действий другим пользователем
- Заполнение таблиц

## 3 Теоретическое введение

Файлы и директории имеют три вида прав доступа:

- Чтение — разрешает получать содержимое файла, но не изменять. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;
- Запись — разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;
- Выполнение — разрешает выполнять файл как программу и переходить в директорию.

Каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

- Владелец — набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права.
- Группа — любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу. Остальные — пользователи, не входящие в предыдущие категории.

Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является или к тем, доступ к которым ему разрешен. В данной лабораторной работе будет рассматриваться доступ к файлам через общую группу.

Более подробно о см. в [1,2].

## 4 Выполнение лабораторной работы

В качестве первого шага лабораторной работы мы перешли в режим `sudo`, дающий нам больше прав, создали учетные записи `guest` и `guest2` с помощью команды `useradd` и добавили пользователя `guest2` в группу `guest` (рис. 4.1).

```
[lrchekalova@lrchekalova ~]$ sudo su
[sudo] пароль для lrchekalova:
[root@lrchekalova lrchekalova]# useradd guest
[root@lrchekalova lrchekalova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@lrchekalova lrchekalova]# useradd guest2
[root@lrchekalova lrchekalova]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@lrchekalova lrchekalova]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@lrchekalova lrchekalova]#
```

Рис. 4.1: Создание учетных записей

Далее мы осуществили вход в систему от двух пользователей на разных терминалах, определили, в какой директории мы находимся, командой `pwd` и получили информацию о группах, в которые входит каждый пользователь, с помощью команд `id` и `groups` (рис. 4.2).



```

[root@lrchekalova lrchekalova]# su guest
[guest@lrchekalova lrchekalova]$ pwd
/home/lrchekalova
[guest@lrchekalova lrchekalova]$ id
uid=1001(guest) gid=1001(guest) rpytty=1001(guest) контекст=unconfined_u:unconf
ined_r:unconfined_t:s0-s0:c0.c1023
[guest@lrchekalova lrchekalova]$ groups guest
guest : guest
[guest@lrchekalova lrchekalova]$ id -Gn
guest
[guest@lrchekalova lrchekalova]$ id -G
1001
[guest@lrchekalova lrchekalova]$

[lrchekalova@lrchekalova ~]$ su guest2
[guest2@lrchekalova lrchekalova]$ pwd
/home/lrchekalova
[guest2@lrchekalova lrchekalova]$ id
uid=1002(guest2) gid=1002(guest2) rpytty=1002(guest2),1001(guest) контекст=unconf
ined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@lrchekalova lrchekalova]$ groups guest2
guest2 : guest2 guest
[guest2@lrchekalova lrchekalova]$ id -Gn
guest2 guest
[guest2@lrchekalova lrchekalova]$ id -G
1002 1001
[guest2@lrchekalova lrchekalova]$

```

Рис. 4.2: Вход и информация о группах

Посмотрели содержимое файла `etc/group` и увидели, что данные о группах пользователей совпадают с полученными ранее (рис. 4.3).

```
cockpit-ws:x:986:  
cockpit-wsinstance:x:985:  
flatpak:x:984:  
colord:x:983:  
clevis:x:982:  
setroubleshoot:x:981:  
gdm:x:42:  
stapusr:x:156:  
stapsys:x:157:  
stapdev:x:158:  
pesign:x:980:  
gnome-initial-setup:x:979:  
sshd:x:74:  
slocate:x:21:  
chrony:x:978:  
dnsmasq:x:977:  
tcpdump:x:72:  
lrchekalova:x:1000:  
vboxsf:x:976:  
vboxdrmipc:x:975:  
guest:x:1001:guest2  
guest2:x:1002:  
[guest@lrchekalova lrchekalova]$
```

Рис. 4.3: Содержимое файла etc/group

Зарегистрировали второго пользователя в группе guest командой newgrp (рис. 4.4).

```
[guest2@lrchekalova lrchekalova]$ newgrp guest  
[guest2@lrchekalova lrchekalova]$
```

Рис. 4.4: Регистрация guest2 в группе guest

Дали всем пользователям группы все права доступа к директории /home/guest (рис.

4.5).

```
[guest@lrchekalova lrchekalova]$ chmod g+rxw /home/guest
```

Рис. 4.5: Изменение прав доступа к /home/guest

Создали папку dir1 и сняли с нее все атрибуты командой `chmod 000`. Проверили успешность действий командой `ls -l` (рис. 4.6).

```
[guest@lrchekalova lrchekalova]$ cd /home/guest
[guest@lrchekalova ~]$ mkdir dir1
[guest@lrchekalova ~]$ ls -l home/guest
ls: невозможно получить доступ к 'home/guest': Нет такого файла или каталога
[guest@lrchekalova ~]$ ls -l home/guest/
ls: невозможно получить доступ к 'home/guest/': Нет такого файла или каталога
[guest@lrchekalova ~]$ ls -l /home/guest
итого 0
drwxr-xr-x. 2 guest guest 6 сен 21 12:15 dir1
[guest@lrchekalova ~]$ chmod 000 dir1
[guest@lrchekalova ~]$ ls -l /home/guest/
итого 0
d----- . 2 guest guest 6 сен 21 12:15 dir1
[guest@lrchekalova ~]$
```

Рис. 4.6: Изменение и просмотр прав доступа папки dir1

Сняли с ранее созданного файла `file1` все атрибуты (рис. 4.7).

```
[guest@lrchekalova ~]$ chmod 000 /home/guest/dir1/file1
```

Рис. 4.7: Снятие атрибутов с file1

Комбинируя разные права доступа к директории и к файлу от имени `guest`, проверили, какие действия доступны для разных прав доступа от имени `guest2` (рис. 4.8).

```

[guest2@lrchekalova lrchekalova]$ touch /home/guest/dir1/file2
touch: невозможно выполнить touch для '/home/guest/dir1/file2': Отказано в досту
[guest2@lrchekalova lrchekalova]$ rm /home/guest/dir1/file1
rm: невозможно удалить '/home/guest/dir1/file1': Отказано в доступе
[guest2@lrchekalova lrchekalova]$ echo "1" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest2@lrchekalova lrchekalova]$ cat /home/guest/dir1/file1
cat: /home/guest/dir1/file1: Отказано в доступе
[guest2@lrchekalova lrchekalova]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest2@lrchekalova lrchekalova]$ mv /home/guest/dir1/file1 /home/guest/fir1/fil
mv: не удалось выполнить stat для '/home/guest/dir1/file1': Отказано в доступе
[guest2@lrchekalova lrchekalova]$ chmod 010 /home/guest/dir1/file1
chmod: невозможно получить доступ к '/home/guest/dir1/file1': Отказано в доступе
[guest2@lrchekalova lrchekalova]$

```

Рис. 4.8: Проверка доступных действий

Заполнили таблицу полученной информацией (рис. 4.9, 4.10, 4.11).

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)	+	+	-	-	+	-	+	-
dr--(040)	(000)	-	-	-	-	-	+	-	-
dr-x(050)	(000)	-	-	-	-	+	+	-	-
drw-(060)	(000)	-	-	-	-	-	+	-	-
drwx(070)	(000)	+	+	-	-	+	+	+	-
d(000)	(010)	-	-	-	-	-	-	-	-
d--x(010)	(010)	-	-	-	-	+	-	-	-
d-w-(020)	(010)	-	-	-	-	-	-	-	-
d-wx(030)	(010)	+	+	-	-	+	-	+	-
dr--(040)	(010)	-	-	-	-	-	+	-	-
dr-x(050)	(010)	-	-	-	-	+	+	-	-
drw-(060)	(010)	-	-	-	-	-	+	-	-
drwx(070)	(010)	+	+	-	-	+	+	+	-
d(000)	(020)	-	-	-	-	-	-	-	-
d--x(010)	(020)	-	-	+	-	+	-	-	-
d-w-(020)	(020)	-	-	-	-	-	-	-	-
d-wx(030)	(020)	+	+	+	-	+	-	+	-
dr--(040)	(020)	-	-	-	-	-	+	-	-
dr-x(050)	(020)	-	-	+	-	+	+	-	-
drw-(060)	(020)	-	-	-	-	-	+	-	-
drwx(070)	(020)	+	+	+	-	+	+	+	-
d(000)	(030)	-	-	-	-	-	-	-	-
d--x(010)	(030)	-	-	+	-	+	-	-	-
d-w-(020)	(030)	-	-	-	-	-	-	-	-
d-wx(030)	(030)	+	+	+	-	+	-	+	-
dr--(040)	(030)	-	-	-	-	-	+	-	-
dr-x(050)	(030)	-	-	+	-	+	+	-	-
drw-(060)	(030)	-	-	-	-	-	+	-	-
drwx(070)	(030)	+	+	+	-	+	+	+	-

Рис. 4.9: Установленные права и разрешенные действия, 1

d(000)	(040)	-	-	-	-	-	-	-	-
d--x(010)	(040)	-	-	-	+	-	-	-	-
d-w(020)	(040)	-	-	-	-	-	-	-	-
d-wx(030)	(040)	+	+	-	+	+	-	+	-
dx--(040)	(040)	-	-	-	-	+	-	-	-
dx-x(050)	(040)	-	-	-	+	+	+	-	-
dxw(060)	(040)	-	-	-	-	-	+	-	-
dxwx(070)	(040)	+	+	-	+	+	+	+	-
d(000)	(050)	-	-	-	-	-	-	-	-
d--x(010)	(050)	-	-	-	+	+	-	-	-
d-w(020)	(050)	-	-	-	-	-	-	-	-
d-wx(030)	(050)	+	+	-	+	+	-	+	-
dx--(040)	(050)	-	-	-	-	-	+	-	-
dx-x(050)	(050)	-	-	-	+	+	+	-	-
dxw(060)	(050)	-	-	-	-	-	+	-	-
dxwx(070)	(050)	+	+	-	+	+	+	+	-

Рис. 4.10: Установленные права и разрешенные действия, 2

d(000)	(060)	-	-	-	-	-	-	-	-
d--x(010)	(060)	-	-	+	+	-	-	-	-
d-w(020)	(060)	-	-	-	-	-	-	-	-
d-wx(030)	(060)	+	+	+	+	+	-	+	-
dx--(040)	(060)	-	-	-	-	-	+	-	-
dx-x(050)	(060)	-	-	+	+	+	+	-	-
dxw(060)	(060)	-	-	-	-	-	+	-	-
dxwx(070)	(060)	+	+	+	+	+	+	+	-
d(000)	(070)	-	-	-	-	-	-	-	-
d--x(010)	(070)	-	-	+	+	+	-	-	-
d-w(020)	(070)	-	-	-	-	-	-	-	-
d-wx(030)	(070)	+	+	+	+	+	-	+	-
dx--(040)	(070)	-	-	-	-	-	+	-	-
dx-x(050)	(070)	-	-	+	+	+	+	-	-
dxw(060)	(070)	-	-	-	-	-	+	-	-
dxwx(070)	(070)	+	+	+	+	+	+	+	+

Рис. 4.11: Установленные права и разрешенные действия, 3

Проанализировали полученную таблицу и определили, какие минимальные права доступа на директорию и на файл необходимы для различных операций (рис. 4.12). Мы видим, что, например, создание, переименование и удаление файла не требует от файла прав доступа на чтение, запись или исполнение. У нас получилась таблица, аналогичная таблице, полученной при выполнении предыдущей лабораторной работы.

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

Рис. 4.12: Минимальные права для совершения операций

## **5 Выводы**

В результате лабораторной работы мной были получены навыки работы с атрибутами файлов, закреплены знания о правах доступа в системах на базе ОС Linux, а также были выявлены минимальные необходимые права доступа для выполнения операций над файлами и директориями. Также было замечено, что в большинстве случаев действия, доступные пользователям группы при определенных атрибутах, аналогичны действиям пользователя-владельца при тех же атрибутах.

## Список литературы

1. Дискреционное разграничение прав в Linux. Основные атрибуты [Электронный ресурс]. URL: <https://esystem.rudn.ru/mod/resource/view.php?id=1031371>.
2. Права доступа к файлам в Linux [Электронный ресурс]. URL: <https://losst.pro/prava-dostupa-k-fajlam-v-linux?ysclid=lmj6rdxo4478919330>.