

# **Отчет по лабораторной работе №3**

**по предмету Информационная безопасность**

Алхимова Дарья Сергеевна

# Содержание

Цель работы	5
Задание	6
Теоретическое введение	8
Выполнение лабораторной работы	10
Выводы	22
Список литературы	23

## Список иллюстраций

1	Создание второго пользователя . . . . .	10
2	Добавление пользователя в группу . . . . .	11
3	Авторизация под разными пользователями . . . . .	11
4	Проверка текущей директории . . . . .	12
5	Данные групп пользователей . . . . .	12
6	Просмотр файла group . . . . .	13
7	Регистрация пользователя в группе . . . . .	13
8	Изменение прав на директорию для группы . . . . .	13
9	Редактирование и проверка прав на директорию . . . . .	14
10	Проверка доступа в директорию . . . . .	14

## Список таблиц

1	Установленные права и разрешённые действия для групп . . . . .	15
2	Минимальные права для совершения операций . . . . .	20

## Цель работы

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

# Задание

1. В установленной операционной системе создайте учётную запись пользователя `guest` (используя учётную запись администратора):  
`useradd guest`
2. Задайте пароль для пользователя `guest` (используя учётную запись администратора): `passwd guest`
3. Аналогично создайте второго пользователя `guest2`.
4. Добавьте пользователя `guest2` в группу `guest`: `gpasswd -a guest2 guest`
5. Осуществите вход в систему от двух пользователей на двух разных консолях: `guest` на первой консоли и `guest2` на второй консоли.
6. Для обоих пользователей командой `pwd` определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки.
7. Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравните вывод команды `groups` с выводом команд `id -Gn` и `id -G`.
8. Сравните полученную информацию с содержимым файла `/etc/group`. Просмотрите файл командой `cat /etc/group`
9. От имени пользователя `guest2` выполните регистрацию пользователя `guest2` в группе `guest` командой `newgrp guest`
10. От имени пользователя `guest` измените права директории `/home/guest`, разрешив все действия для пользователей группы: `chmod g+rx /home/guest`

11. От имени пользователя guest снимите с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1`

# Теоретическое введение

Для всех файлов и директорий Linux устанавливаются следующие права доступа:

- разрешение чтение содержимого файла;
- разрешение на изменение (запись) содержимого файла;
- разрешение на исполнение файла.

В свойствах каждого файла и директории эти три разрешения устанавливаются отдельно для:

- владельца файла
- группы владельцев файла, которой принадлежит этот файл
- всех остальных.

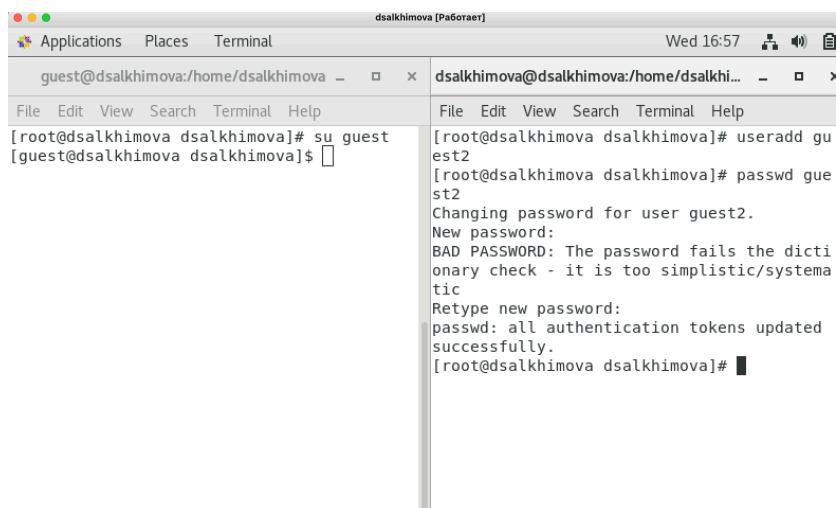
Просмотреть права доступа, а также владельца и группу, к которой относится файл, можно командой `ls` с опцией `-l`. Чтобы изменить режим (права доступа) файла или каталога, используется команда `chmod` с параметрами. Три цифры соответствуют трём параметрам режима доступа: чтение, запись, выполнение. Поэтому права доступа можно представить в виде трёх двоичных цифр, которые можно записать как одну восьмеричную цифру. Используя три восьмеричных цифры, мы можем установить режим файла для владельца, группы владельцев и всех остальных. Хотя запоминание восьмеричного бинарного отображения может показаться неудобным, обычно нужно использовать только несколько часто используемых: 7 (rwx), 6 (rw-), 5 (r-x), 4 (r-) и 0 (—). Либо можно запомнить значение одиночных прав доступа и складывать их значения для получения любых



комбинаций: 4 (r-), 2 (-w-), 1 (-x). После можно получить любую комбинацию, для прав чтения и записи это 6 (4+2) (rw-), для прав записи и выполнения это 3 (2+1) (-wx), для прав чтения и выполнения это 5 (4+1) (r-x)

# Выполнение лабораторной работы

1. Т.к. в рамках предыдущей лабораторной работы в установленной операционной системе я создала учетную запись пользователя guest и задала пароль для нее, то в данной работе я аналогично создала второго пользователя guest2, задала пароль и выполнила вход в эту учетную запись. (рис. 1)



The image shows two terminal windows side-by-side. The left window shows a root user switching to the 'guest' user. The right window shows the root user creating a new user 'guest2' and setting a password.

```
guest@dsalkhimova:/home/dsalkhimova - □ ×
File Edit View Search Terminal Help
[root@dsalkhimova dsalkhimova]# su guest
[guest@dsalkhimova dsalkhimova]$ □
```

```
dsalkhimova@dsalkhimova:/home/dsalkhi... - □ ×
File Edit View Search Terminal Help
[dsalkhimova@dsalkhimova dsalkhimova]# useradd gu
est2
[dsalkhimova@dsalkhimova dsalkhimova]# passwd gue
st2
Changing password for user guest2.
New password:
BAD PASSWORD: The password fails the dicti
onary check - it is too simplistic/systema
tic
Retype new password:
passwd: all authentication tokens updated
successfully.
[dsalkhimova@dsalkhimova dsalkhimova]# █
```

Рис. 1: Создание второго пользователя

2. Добавила пользователя guest2 в группу guest с помощью команды `gpasswd -a guest2 guest`. (рис. 2)

```

successfully.
[root@dsalkhimova dsalkhimova]# gpasswd -a
  guest2 guest
Adding user guest2 to group guest
[root@dsalkhimova dsalkhimova]# █

```

Рис. 2: Добавление пользователя в группу

3. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. (рис. 3)

<pre> [root@dsalkhimova dsalkhimova]# su guest [guest@dsalkhimova dsalkhimova]\$ █ </pre>	<pre> [root@dsalkhimova dsalkhimova]# useradd gu est2 [root@dsalkhimova dsalkhimova]# passwd gue st2 Changing password for user guest2. New password: BAD PASSWORD: The password fails the dicti onary check - it is too simplistic/systema tic Retype new password: passwd: all authentication tokens updated successfully. [root@dsalkhimova dsalkhimova]# gpasswd -a   guest2 guest Adding user guest2 to group guest [root@dsalkhimova dsalkhimova]# su guest2 [guest2@dsalkhimova dsalkhimova]\$ █ </pre>
---	--

Рис. 3: Авторизация под разными пользователями

4. Для обоих пользователей определила директорию, в которой я нахожусь, командой pwd - в домашней директории пользователя, под которым осуществлен вход в ОС. Для каждого пользователя перешла в домашнюю директорию с помощью команды cd и еще раз проверила текущую директорию. (рис. 4)

```

[root@dsalkhimova dsalkhimova]# su guest
[guest@dsalkhimova dsalkhimova]$ pwd
/home/dsalkhimova
[guest@dsalkhimova dsalkhimova]$ cd
[guest@dsalkhimova ~]$ pwd
/home/guest
[guest@dsalkhimova ~]$ █

[guest@dsalkhimova dsalkhimova]# passwd guest2
[guest@dsalkhimova dsalkhimova]# passwd guest2
Changing password for user guest2.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
[guest@dsalkhimova dsalkhimova]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[guest@dsalkhimova dsalkhimova]# su guest2
[guest2@dsalkhimova dsalkhimova]$ pwd
/home/dsalkhimova
[guest2@dsalkhimova dsalkhimova]$ cd
[guest2@dsalkhimova ~]$ pwd
/home/guest2
[guest2@dsalkhimova ~]$ █

```

Рис. 4: Проверка текущей директории

5. Уточнила имя каждого пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определила командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Информация, выводимая командами `groups` и `id -Gn` и `id -G` касательно групп пользователей совпадает. `id -G` выводит идентификаторы групп, куда входит пользователь, а `id -Gn` - имена этих групп. Пользователь `guest` входит только в группу `guest` (1001), а пользователь `guest2` - в `guest` (1001) и `guest2` (1002). (рис. 5)

```

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

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

```

Рис. 5: Данные групп пользователей

6. Просмотрела файл `group` командой `cat /etc/group`. (рис. 6)

```

[guest@dsalkhimova ~]$ 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:
nem:x:8:
kmem:x:9:
wheel:x:10:dsalkhimova
cdrom:x:11:
nail:x:12:postfix
nan:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
tss:x:59:
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
gluster:x:984:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
dsalkhimova:x:1000:dsalkhimova
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
[guest2@dsalkhimova ~]$

```

Рис. 6: Просмотр файла group

Информация, содержащаяся в файле, совпадает с той, что мы получили на предыдущем шаге (учетные записи созданных пользователей находятся в самом низу вывода).

- От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой `newgrp guest`. (рис. 7)

```

[guest2@dsalkhimova ~]$ newgrp guest
[guest2@dsalkhimova ~]$ █

```

Рис. 7: Регистрация пользователя в группе

- От имени пользователя guest изменила права директории `/home/guest`, разрешив все действия для пользователей группы владельца: `chmod g+rxw /home/guest`. (рис. 8)

```

[guest@dsalkhimova ~]$ chmod g+rxw /home/guest

```

Рис. 8: Изменение прав на директорию для группы

9. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` и проверила правильность выполнения команды через `ls -l` (рис. 9)

```
[guest@dsalkhimova ~]$ chmod 000 /home/guest/dir1
[guest@dsalkhimova ~]$ ls -l
total 0
d----- . 2 guest guest 6 Sep 21 17:05 dir1
[guest@dsalkhimova ~]$
```

Рис. 9: Редактирование и проверка прав на директорию

10. Проверила, что у пользователя guest2 есть доступ в домашнюю директорию пользователя guest как у члена группы владельца. (рис. 10)

```
guest2:x:1002:
[guest2@dsalkhimova ~]$ newgrp guest
[guest2@dsalkhimova ~]$ cd /home/guest
[guest2@dsalkhimova guest]$
```

Рис. 10: Проверка доступа в директорию

11. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнила таблицу “Установленные права и разрешенные действия для групп”, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

Обозначения в таблице:

- (1) Создание файла
- (2) Удаление файла

- (3) Запись в файл
- (4) Чтение файла
- (5) Смена директории
- (6) Просмотр файлов в директории
- (7) Переименование файл
- (8) Смена атрибутов файла

Таблица 1: Установленные права и разрешённые действия для групп

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
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)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d-----	-----x---	-	-	-	-	-	-	-	-
(000)	(010)								
d-----x---	-----x---	-	-	-	-	+	-	-	+
(010)	(010)								
d----w----	-----x---	-	-	-	-	-	-	-	-
(020)	(010)								
d----wx---	-----x---	+	+	-	-	+	-	+	+
(030)	(010)								
d---r-----	-----x---	-	-	-	-	-	+	-	-
(040)	(010)								
d---r-x---	-----x---	-	-	-	-	+	+	-	+
(050)	(010)								
d---rw----	-----x---	-	-	-	-	-	+	-	-
(060)	(010)								
d---rwx---	-----x---	+	+	-	-	+	+	+	+
(070)	(010)								
d-----	-----w----	-	-	-	-	-	-	-	-
(000)	(020)								
d-----x---	-----w----	-	-	+	-	+	-	-	+
(010)	(020)								
d----w----	-----w----	-	-	-	-	-	-	-	-
(020)	(020)								
d----wx---	-----w----	+	+	+	-	+	-	+	+
(030)	(020)								
d---r-----	-----w----	-	-	-	-	-	+	-	-
(040)	(020)								



Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d---r-x---	-----w----	-	-	+	-	+	+	-	+
(050)	(020)								
d---rw----	-----w----	-	-	-	-	-	+	-	-
(060)	(020)								
d---rwx---	-----w----	+	+	+	-	+	+	+	+
(070)	(020)								
d-----	-----wx---	-	-	-	-	-	-	-	-
(000)	(030)								
d-----x---	-----wx---	-	-	+	-	+	-	-	+
(010)	(030)								
d----w----	-----wx---	-	-	-	-	-	-	-	-
(020)	(030)								
d----wx---	-----wx---	+	+	+	-	+	-	+	+
(030)	(030)								
d---r-----	-----wx---	-	-	-	-	-	+	-	-
(040)	(030)								
d---r-x---	-----wx---	-	-	+	-	+	+	-	+
(050)	(030)								
d---rw----	-----wx---	-	-	-	-	-	+	-	-
(060)	(030)								
d---rwx---	-----wx---	+	+	+	-	+	+	+	+
(070)	(030)								
d-----	----r-----	-	-	-	-	-	-	-	-
(000)	(040)								
d-----x---	----r-----	-	-	-	+	+	-	-	+
(010)	(040)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d----w----	----r-----	-	-	-	-	-	-	-	-
(020)	(040)								
d---wx---	----r-----	+	+	-	+	+	-	+	+
(030)	(040)								
d---r-----	----r-----	-	-	-	-	-	+	-	-
(040)	(040)								
d---r-x---	----r-----	-	-	-	+	+	+	-	+
(050)	(040)								
d---rw----	----r-----	-	-	-	-	-	+	-	-
(060)	(040)								
d---rwx---	----r-----	+	+	-	+	+	+	+	+
(070)	(040)								
d-----	----r-x---	-	-	-	-	-	-	-	-
(000)	(050)								
d-----x---	----r-x---	-	-	-	+	+	-	-	+
(010)	(050)								
d----w----	----r-x---	-	-	-	-	-	-	-	-
(020)	(050)								
d---wx---	----r-x---	+	+	-	+	+	-	+	+
(030)	(050)								
d---r-----	----r-x---	-	-	-	-	-	+	-	-
(040)	(050)								
d---r-x---	----r-x---	-	-	-	+	+	+	-	+
(050)	(050)								
d---rw----	----r-x---	-	-	-	-	-	+	-	-
(060)	(050)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d---rwx---	----r-x---	+	+	-	+	+	+	+	+
(070)	(050)								
d-----	----rw----	-	-	-	-	-	-	-	-
(000)	(060)								
d-----x---	----rw----	-	-	+	+	+	-	-	+
(010)	(060)								
d---w----	----rw----	-	-	-	-	-	-	-	-
(020)	(060)								
d---wx---	----rw----	+	+	+	+	+	-	+	+
(030)	(060)								
d---r-----	----rw----	-	-	-	-	-	+	-	-
(040)	(060)								
d---r-x---	----rw----	-	-	+	+	+	+	-	+
(050)	(060)								
d---rw----	----rw----	-	-	-	-	-	+	-	-
(060)	(060)								
d---rwx---	----rw----	+	+	+	+	+	+	+	+
(070)	(060)								
d-----	----rwx---	-	-	-	-	-	-	-	-
(000)	(070)								
d-----x---	----rwx---	-	-	+	+	+	-	-	+
(010)	(070)								
d---w----	----rwx---	-	-	-	-	-	-	-	-
(020)	(070)								
d---wx---	----rwx---	+	+	+	+	+	-	+	+
(030)	(070)								

Права									
директории	Права файла	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
d---r----- (040)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---r-x--- (050)	----rwx--- (070)	-	-	+	+	+	+	-	+
d---rw---- (060)	----rwx--- (070)	-	-	-	-	-	+	-	-
d---rwx--- (070)	----rwx--- (070)	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы я определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила таблицу “Минимальные права для совершения операций” [-@tbl:min-rig]. Для заполнения последних двух строк опытным путем проверила минимальные права для создания и удаления поддиректории.

Таблица 2: Минимальные права для совершения операций

Операция	Мин. права на	
	директорию	Мин. 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)

Операция	Мин. права на директорию	Мин. права на файл
Удаление поддиректории	d----wx--- (030)	----- (000)

Сравнивая данную таблицу с такой же таблицей из предыдущей лабораторной работы, можно сделать вывод, что они идентичны. Единственное различие в том, что в предыдущей лабораторной работе права присваивались владельцу, а в этой - группе владельца.

## **Выводы**

В процессе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

## Список литературы

1. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
2. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
3. Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.