

Лабораторная работа №3

Дисциплина: Информационная безопасность

Боровикова Карина Владимировна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	22
	Список литературы	23

Список иллюстраций

4.1	Создание учетной записи guest	9
4.2	Добавление пользователя guest2 в группу guest	10
4.3	Проверка групп для пользователей guest и guest2	11
4.4	Файл /etc/group	11
4.5	регистрация пользователя guest2 в группе guest	12
4.6	Изменяем права директории разрешив все действия для пользова- телей группы	12

Список таблиц

4.1	Установленные права и разрешенные действия	14
4.2	Минимальные права для совершения операций	21

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Задание

- Произвести работу в консоли с атрибутами файлов для групп пользователей от имени пользователя *guest* и *guest2*;
- Составить опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

3 Теоретическое введение

В данной лабораторной работе нам предстоит поработать с правами доступа файлов и директорий. **Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами.

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

- **r** — read (чтение) — право просматривать содержимое файла;
- **w** — write (запись) — право изменять содержимое файла;
- **x** — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

- **owner** (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но владельцем можно сделать и кого-то другого.
- **group** (группа) — пользователи с общими заданными правами.
- **others** (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами.[01?]

Чтобы увидеть текущие назначения владельца, вы можете использовать команду `ls -l`. Эта команда показывает пользователя и группу-владельца.

С помощью команды `ls` вы можете отобразить владельца файлов в данном каталоге. Иногда может оказаться полезным получить список всех файлов в системе, в которых в качестве владельца указан данный пользователь или группа. Для этого вы можете использовать `find`. Аргумент `find -user` может быть использован для этой цели.

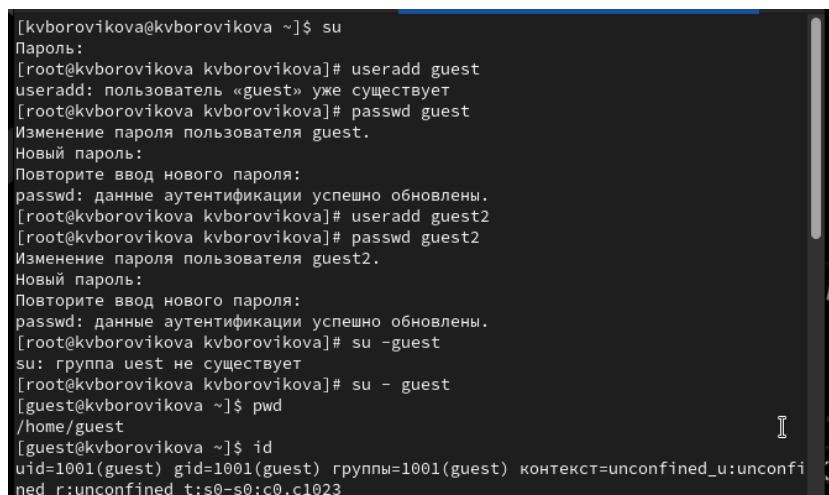
Чтобы применить соответствующие разрешения, первое, что нужно учитывать, это владение. Для этого есть команда `chown`.^[02?]

Для того, чтобы позволить обычным пользователям выполнять программы от имени суперпользователя без знания его пароля была придумана такая вещь, как SUID и SGID биты. Рассмотрим эти полномочия подробнее.

- **SUID** - если этот бит установлен, то при выполнении программы, `id` пользователя, от которого она запущена заменяется на `id` владельца файла. Фактически, это позволяет обычным пользователям запускать программы от имени суперпользователя;
- **SGID** - этот флаг работает аналогичным образом, только разница в том, что пользователь считается членом группы, с которой связан файл, а не групп, к которым он действительно принадлежит. Если SGID флаг установлен на каталог, все файлы, созданные в нем, будут связаны с группой каталога, а не пользователя. Такое поведение используется для организации общих папок;
- **Sticky-bit** - этот бит тоже используется для создания общих папок. Если он установлен, то пользователи могут только создавать, читать и выполнять файлы, но не могут удалять файлы, принадлежащие другим пользователям.

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора) (рис. 4.1): `useradd guest`.



```
[kvborovikova@kvborovikova ~]$ su
Пароль:
[root@kvborovikova kvborovikova]# useradd guest
useradd: пользователь «guest» уже существует
[root@kvborovikova kvborovikova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@kvborovikova kvborovikova]# useradd guest2
[root@kvborovikova kvborovikova]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@kvborovikova kvborovikova]# su - guest
su: группа uest не существует
[root@kvborovikova kvborovikova]# su - guest
[guest@kvborovikova ~]$ pwd
/home/guest
[guest@kvborovikova ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 4.1: Создание учетной записи guest

2. Зададим пароль для пользователя guest (используя учётную запись администратора) (рис. 4.1): `passwd guest`.
3. Аналогично создадим второго пользователя guest2. (рис. 4.1): `useradd guest2`, `passwd guest`
4. Добавим пользователя guest2 в группу guest: (рис. 4.2) `gpasswd -a guest2 guest`

```

gpasswd: доступ запрещен.
[guest2@kvborovikova ~]$ su
Пароль:
[root@kvborovikova guest2]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@kvborovikova guest2]# exit
exit
[guest2@kvborovikova ~]$ pwd
/home/guest2
[guest2@kvborovikova ~]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2) контекст=unconfined_u:unco
nfin_r:unconfined_t:s0-s0:c0.c1023
[guest2@kvborovikova ~]$ groups guest
guest : guest
[guest2@kvborovikova ~]$ groups guest2
guest2 : guest2 guest

```

Рис. 4.2: Добавление пользователя guest2 в группу guest

5. Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. (рис. 4.1 - 4.2) su - guest, su - guest2
6. Определим директорию, в которой находимся, командой pwd(рис. 4.1 - 4.2). Сравним её с приглашением командной строки. В командной строке видим символ ~, что свидетельствует о том, что **мы находимся в своей домашней директории.**
7. Уточним имя пользователя, его группу, а также группы, куда входит пользо- ватель, командой id (рис. 4.1 - 4.2).

Видим следующие данные для пользователя guest: uid = 1001(guest), gid = 1001(guest), groups = 1001(guest).

Видим следующие данные для пользователя guest2: uid = 1002(guest2), gid = 1002(guest2), groups = 1002(guest2).

Определите командами groups guest и groups guest2 (рис. 4.2), в какие груп- пы входят пользователи guest и guest2. Сравните вывод команды groups с выво- дом команд id -Gn и id -G.

Видим, что информация для groups guest и groups guest2 совпадает с дей- ствительностью, для пользователя guest группа guest, для пользователя guest2 группы guest и guest2, так как мы этого пользователя добавили в группу guest. Аналогично, совпадает и для команд id -Gn и id -G. (рис. 4.2 - 4.3)

```

guest2:x:1002:
[guest2@kvborovikova dir1]$ id -Gn guest2
guest2 guest
[guest2@kvborovikova dir1]$ id -Gn guest
guest
[guest2@kvborovikova dir1]$

```

Рис. 4.3: Проверка групп для пользователей guest и guest2

8. Сравним полученную информацию с содержимым файла /etc/group. Посмотрите файл командой

```
cat /etc/group
```

```

tcpdump:x:72:
kvborovikova:x:1000:
guest:x:1001:guest2
guest2:x:1002:
[guest2@kvborovikova dir1]$

```

Рис. 4.4: Файл /etc/group

Найдем в нем последние 2 записи - записи о пользователях guest и guest2. Данные строки показывают, что для guest gid = 1001 и guest2, что соответствует результатам предыдущих команд.

9. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой `newgrp guest` (рис. 4.5)

```
guest2@kvborovikova:/home/guest/dir1  x  guest@kvborovikova:~  x
[guest2@kvborovikova ~]$ newgrp guest
[guest2@kvborovikova ~]$ cd /home/guest
[guest2@kvborovikova guest]$ ls -l
итого 0
d----- 2 guest guest 19 сен 16 16:14 dir1
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Видео
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Документы
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Загрузки
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Изображения
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Музыка
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Общедоступные
drwxr-xr-x 2 guest guest 6 сен 16 15:19 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Шаблоны
[guest2@kvborovikova guest]$ cd dir1
bash: cd: dir1: Отказано в доступе
[guest2@kvborovikova guest]$ ls -l
итого 0
d----- 2 guest guest 19 сен 16 16:14 dir1
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Видео
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Документы
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Загрузки
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Изображения
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Музыка
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Общедоступные
drwxr-xr-x 2 guest guest 6 сен 16 15:19 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Шаблоны
[guest2@kvborovikova guest]$ cd dir1
[guest2@kvborovikova dir1]$ ls
```

Рис. 4.5: регистрация пользователя guest2 в группе guest

10. От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rwX /home/guest` (рис. 4.6)

```
[guest@kvborovikova ~]$ chmod g+rwX /home/guest
[guest@kvborovikova ~]$ cd /home/guest
[guest@kvborovikova ~]$ ls -l
итого 0
d----- 2 guest guest 19 сен 16 16:14 dir1
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Видео
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Документы
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Загрузки
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Изображения
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Музыка
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Общедоступные
drwxr-xr-x 2 guest guest 6 сен 16 15:19 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Шаблоны
[guest@kvborovikova ~]$ chmod 010 dir1
[guest@kvborovikova ~]$ ls -l
итого 0
d----- 2 guest guest 19 сен 16 16:14 dir1
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Видео
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Документы
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Загрузки
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Изображения
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Музыка
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Общедоступные
drwxr-xr-x 2 guest guest 6 сен 16 15:19 'Рабочий стол'
drwxr-xr-x 2 guest guest 6 сен 16 15:19 Шаблоны
[guest@kvborovikova ~]$
```

Рис. 4.6: Изменяем права директории разрешив все действия для пользователей группы

11. От имени пользователя `guest` снимем с директории `/home/guest/dir1` все атрибуты командой `chmod 000 dir1` и проверим правильность снятия атрибутов. (рис. 4.6)

Видим, что теперь на директорию `dir1` нет никаких прав.

12. Заполните таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Для определения опытным путем будем использовать следующие действия в соответствии со столбцами таблицы:

- `cd dir1` - смена директории;
- `touch <новый_файл>` - создание файла;
- `rm <новый_файл>` - удаление файла;
- `ls -l (dir1)` - просмотр файлов в директории;
- `echo "test" > <файл_с_установленными_правами>` - запись в файл;
- `cat <файл_с_установленными_правами>` - чтение файла;
- `mv <файл_с_установленными_правами> <переименование>` - переименование файла;
- `chattr <атрибуты> <файл_с_установленными_правами>` смена атрибутов файла.

Остальные действия можно найти в видеозаписи к лабораторной работе.

Заполненная табл. 4.1 краткого описания стандартных каталогов Unix.

Таблица 4.1: Установленные права и разрешенные действия

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
----- (000)	----- (000)	-	-	-	-	-	-	-	-
----- (000)	-- x----- (010)	-	-	-	-	-	-	-	-
----- (000)	- w----- (020)	-	-	-	-	-	-	-	-
----- (000)	- wx----- (030)	-	-	-	-	-	-	-	-
----- (000)	r----- (040)	-	-	-	-	-	-	-	-
----- (000)	r- x----- (050)	-	-	-	-	-	-	-	-
----- (000)	rw----- (060)	-	-	-	-	-	-	-	-
----- (000)	rw-x----- (070)	-	-	-	-	-	-	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
--x----- (010)	-- x----- (010)	-	-	-	-	+	-	-	-
--x----- (010)	- w----- (020)	-	-	+	-	+	-	-	-
--x----- (010)	- wx----- (030)	-	-	+	-	+	-	-	-
--x----- (010)	r----- (040)	-	-	-	+	+	-	-	+
--x----- (010)	r- x----- (050)	-	-	-	+	+	-	-	+
--x----- (010)	rw----- (060)	-	-	+	+	+	-	-	+
--x----- (010)	rwX----- (070)	-	-	+	+	+	-	-	+
--x----- (010)	----- (000)	-	-	-	-	+	-	-	-
-w----- (020)	----- (000)	-	-	-	-	-	-	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
-w----- (020)	-- x----- (010)	-	-	-	-	-	-	-	-
-w----- (020)	- w----- (020)	-	-	-	-	-	-	-	-
-w----- (020)	- wx----- (030)	-	-	-	-	-	-	-	-
-w----- (020)	r----- (040)	-	-	-	-	-	-	-	-
-w----- (020)	r- x----- (050)	-	-	-	-	-	-	-	-
-w----- (020)	rw----- (060)	-	-	-	-	-	-	-	-
-w----- (020)	rwX----- (070)	-	-	-	-	-	-	-	-
-wx----- (030)	-----+ (000)	+	+	-	-	+	-	+	-
-wx----- (030)	-- x----- (010)	+	+	-	-	+	-	+	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
-wx----- (030)	- w----- (020)	+	+	+	-	+	-	+	-
-wx----- (030)	- wx----- (030)	+	+	+	-	+	-	+	-
-wx----- (030)	r-----+ (040)	+	+	-	+	+	-	+	+
-wx----- (030)	r- x----- (050)	+	+	-	+	+	-	+	+
-wx----- (030)	rw-----+ (060)	+	+	+	+	+	-	+	+
-wx----- (030)	rwX-----+ (070)	+	+	+	+	+	-	+	+
r----- (040)	----- (000)	-	-	-	-	-	+	-	-
r----- (040)	-- x----- (010)	-	-	-	-	-	+	-	-
r----- (040)	- w----- (020)	-	-	-	-	-	+	-	-

Права ди- ректории	Права файла	Со- Уда- зда- ле- За- Чте- ние ние пись ние					Про- смотр фай- лов	Пере- име- нова- ние	Смена аттри- бутов файла
		фай- ла	фай- ла	в файл	фай- ла	Смена дирек- тории	дирек- тории	фай- ла	
r----- (040)	- wx----- (030)	-	-	-	-	-	+	-	-
r----- (040)	r----- (040)	-	-	-	-	-	+	-	-
r----- (040)	r- x----- (050)	-	-	-	-	-	+	-	-
r----- (040)	rw----- (060)	-	-	-	-	-	+	-	-
r----- (040)	rwX----- (070)	-	-	-	-	-	+	-	-
r-x----- (050)	----- (000)	-	-	-	-	+	+	-	-
r-x----- (050)	-- x----- (010)	-	-	-	-	+	+	-	-
r-x----- (050)	- w----- (020)	-	-	+	-	+	+	-	-
r-x----- (050)	- wx----- (030)	-	-	+	-	+	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
r-x----- (050)	r----- (040)	-	-	+	+	+	+	-	+
r-x----- (050)	r- x----- (050)	-	-	-	+	+	+	-	+
r-x----- (050)	rw----- (060)	-	+	+	+	+	+	-	+
r-x----- (050)	rwX----- (070)	-	+	+	+	+	+	-	+
rw----- (060)	----- (000)	-	-	-	-	-	+	-	-
rw----- (060)	-- x----- (010)	-	-	-	-	-	+	-	-
rw----- (060)	- w----- (020)	-	-	-	-	-	+	-	-
rw----- (060)	- wX----- (030)	-	-	-	-	-	+	-	-
rw----- (060)	r----- (040)	-	-	-	-	-	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
rw----- (060)	r- x----- (050)	-	-	-	-	-	+	-	-
rw----- (060)	rw----- (060)	-	-	-	-	-	+	-	-
rw----- (060)	rwX----- (070)	-	-	-	-	-	+	-	-
rwX----- (070)	-----+ (000)	+	+	-	-	+	+	+	-
rwX----- (070)	-- x----- (010)	+	+	-	-	+	+	+	-
rwX----- (070)	- w----- (020)	+	+	+	-	+	+	+	-
rwX----- (070)	- wx----- (030)	+	+	+	-	+	+	+	-
rwX----- (070)	r-----+ (040)	+	+	-	+	+	+	+	+
rwX----- (070)	r- x----- (050)	+	+	-	+	+	+	+	+

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
rwX----- (070)	rw-----+	+	+	+	+	+	+	+	+
rwX----- (070)	rwX-----+	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы 4.1 определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 4.2.

Таблица 4.2: Минимальные права для совершения операций

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)	-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)

5 Выводы

Получила практические навыки работы в консоли с атрибутами файлов для групп пользователей, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux. Заполнила опытным путем таблицы “Установленные права и разрешенные действия” и “Минимальные права для совершения операций”.

Список литературы