

# **Лабораторная работа №2**

**Дискреционное разграничение прав в Linux. Основные атрибуты**

Василий Александрович Селезнев

# Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	16

## Список иллюстраций

3.1	Создание учетной записи guest . . . . .	7
3.2	Задание пароля для учетной записи . . . . .	7
3.3	Вход в систему от имени пользователя guest . . . . .	8
3.4	Определение текущей директории. Переход в домашнюю директорию	8
3.5	Уточнение имени пользователя . . . . .	9
3.6	Уточнение имени, его группы . . . . .	9
3.7	Сравнение полученной информации . . . . .	9
3.8	Просмотр файла с помощью команды cat . . . . .	10
3.9	Определение существующих в системе директорий . . . . .	10
3.10	Создание директории dir1 . . . . .	11
3.11	Снятие всех атрибутов с директории dir1 . . . . .	11
3.12	Попытка создания файла file1 . . . . .	11

## Список таблиц

3.1	Установленные права и разрешённые действия . . . . .	12
3.2	Минимальные права для совершения операций . . . . .	15

# 1 Цель работы

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

## 2 Задание

1. Создать учетную запись пользователя guest.
2. Войти в терминал, используя созданную учетную запись, и выполнить ряд команд.
3. Заполнить таблицу “Установленные права и разрешенные действия”
4. Заполнить таблицу “Минимальные права для совершения операций”

### 3 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (использовал учётную запись администратора) (рис - @fig:001). Для этого использовал команду `user add guess`

```
[vaseleznev@vaseleznev ~]$ su
Пароль:
[root@vaseleznev vaseleznev]# useradd guest
[root@vaseleznev vaseleznev]# passwd guest
```

Рис. 3.1: Создание учетной записи guest

Задал пароль для пользователя guest (использовал учётную запись администратора) (рис - @fig:002). Для этого использовал команду `passwd guest`

```
[root@vaseleznev vaseleznev]# passwd guest
Смена пароля для пользователя guest.
Новый пароль :
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
```

Рис. 3.2: Задание пароля для учетной записи

Вошел в систему от имени пользователя guest (рис - @fig:003).

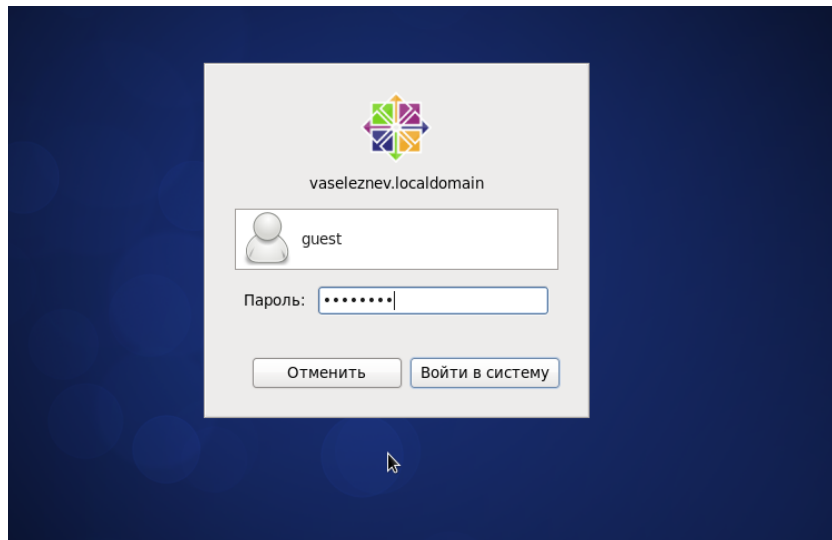


Рис. 3.3: Вход в систему от имени пользователя guest

2. Определил директорию, в которой я нахожусь, командой `pwd`. Она совпадает с приглашением командной строки. Определил, что она не является моей домашней директорией. Перешл в свою домашнюю директорию. (рис - @fig:004)

```
[guest@vaseleznev ~]$ pwd
/home/guest
[guest@vaseleznev ~]$ cd...
bash: cd...: команда не найдена
[guest@vaseleznev ~]$ cd..
bash: cd..: команда не найдена
[guest@vaseleznev ~]$ cd ..
[guest@vaseleznev home]$ pwd
/home
```

Рис. 3.4: Определение текущей директории. Переход в домашнюю директорию

Уточнил имя своего пользователя командой `whoami` (рис - @fig:005).



```
[guest@vaseleznev home]$ whoami  
guest
```

Рис. 3.5: Уточнение имени пользователя

Уточнил имя своего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомнил. Группы совпадают, однако вывод команды `id` объемнее (рис -@fig:006).

```
-----  
[guest@vaseleznev home]$ id  
uid=501(guest) gid=501(guest) группы=501(guest) контекст=unconfined_u:unconfined  
r:unconfined t:s0-s0:c0.c1023  
[guest@vaseleznev home]$ █
```

Рис. 3.6: Уточнение имени, его группы

Сравнил полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки (рис -@fig:007). Как видно из рисунка, информация об имени пользователя, полученная командой `id` (`gid=501(guest)`), совпадает с приглашением командной строки (`guest@rvivanov home`)

```
█ [guest@vaseleznev home]$ █
```

Рис. 3.7: Сравнение полученной информации

Просмотрел файл `/etc/passwd` командой `cat /etc/passwd` (рис -@fig:008, рис -@fig:009)

```
[guest@vaseleznev home]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:./:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
haldaemon:x:68:68:HAL daemon:./:/sbin/nologin
ntp:x:38:38:./etc/ntp:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
sasauth:x:497:76:Sasauthd user:/var/empty/sasauth:/sbin/nologin
postfix:x:89:89:./var/spool/postfix:/sbin/nologin
abrt:x:173:173:./etc/abrt:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
vaseleznev:x:500:500:vaseleznev:/home/vaseleznev:/bin/bash
guest:x:501:501:./home/guest:/bin/bash
[guest@vaseleznev home]$ █
```

Рис. 3.8: Просмотр файла с помощью команды cat

Определил существующие в системе директории командой `ls -l /home/`  
(рис -@fig:009)

```
[guest@vaseleznev home]$ ls -l /home/
итого 8
drwx-----. 26 guest      guest      4096 Окт  2 17:37 guest
drwx-----. 27 vaseleznev vaseleznev 4096 Окт  2 17:30 vaseleznev
[guest@vaseleznev home]$ █
```

Рис. 3.9: Определение существующих в системе директорий

Создал в домашней директории поддиректорию `dir1` командой `mkdir dir1`  
(рис. -@fig:013)

```
[guest@vaseleznev home]$ ls -l
итого 8
drwx-----. 2 guest      guest      4096 Окт  2 17:37 guest
drwx-----. 27 vaseleznev vaseleznev 4096 Окт  2 17:30 vaseleznev
[guest@vaseleznev home]$ cd guast
bash: cd: guast: Нет такого файла или каталога
[guest@vaseleznev home]$ cd guest
[guest@vaseleznev ~]$ mkdir dir1
[guest@vaseleznev ~]$
```

Рис. 3.10: Создание директории dir1

Также с помощью команд `ls -l` и `lsattr` просмотрел, какие атрибуты выставлены на директорию `dir1` (`drwxrwxr-x` и `-----e-` соответственно).

Снял с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверил правильность выполнения команды с помощью `ls -l` (рис. -@fig:014)

```
[guest@vaseleznev ~]$ chmod 000 dir1
[guest@vaseleznev ~]$ ls -l
итого 36
d------. 2 guest guest 4096 Окт  2 20:55 dir1
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Видео
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Документы
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Загрузки
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Картинки
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Музыка
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Общедоступные
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Рабочий стол
drwxr-xr-x. 2 guest guest 4096 Окт  2 17:37 Шаблоны
[guest@vaseleznev ~]$
```

Рис. 3.11: Снятие всех атрибутов с директории dir1

Попытался создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` (рис. -@fig:015). Я получил отказ, т.к. на предыдущем шаге для директории `dir` были сняты все атрибуты.

```
[guest@vaseleznev ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@vaseleznev ~]$ echo "test" > /home/guest/dir1/file1
```

Рис. 3.12: Попытка создания файла file1

С помощью команды `ls -l /home/guest/dir1` выяснил, что невозможно

получить доступ к директории `dir1`. Файл `file1` действительно не находится в директории

3. Заполнил таблицу “Установленные права и разрешенные действия”, выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет. “+” - операция разрешена, “-” - операция не разрешена (таб. 3.1)

Таблица 3.1: Установленные права и разрешённые действия

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись в файл	Чте- ние фай- ла	Сме- ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(000)	(000)	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	-	-	+
d(100)	(100)	-	-	-	-	-	-	+
d(100)	(200)	-	-	+	-	-	-	+
d(100)	(300)	-	-	+	-	-	-	+
d(100)	(400)	-	-	-	+	-	-	+
d(100)	(500)	-	-	-	+	-	-	+

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	Сме- на	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
ди- рек- то- рии	Пра- ва фай- ла	фай- ла	фай- ла	в файл	фай- ла	то- рии		
d(100)	(600)	-	-	+	+	-	-	+
d(100)	(700)	-	-	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	+	+
d(300)	(100)	+	+	-	-	+	+	+
d(300)	(200)	+	+	+	-	+	+	+
d(300)	(300)	+	+	+	-	+	+	+
d(300)	(400)	+	+	-	+	+	+	+
d(300)	(500)	+	+	-	+	+	+	+
d(300)	(600)	+	+	+	+	+	+	-
d(300)	(700)	+	+	+	+	+	+	-
d(400)	(000)	-	-	-	-	-	+	-
d(400)	(100)	-	-	-	-	-	+	-
d(400)	(200)	-	-	-	-	-	+	-
d(400)	(300)	-	-	-	-	-	+	-
d(400)	(400)	-	-	-	-	-	+	-

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	Сме- на	Просмотр	Пере- имено- вание	Смена
ди- рек- то- рии	Пра- ва фай- ла	фай- ла	фай- ла	в файл	фай- ла	рек- то- рии	файлов в директо- рии	атрибу- тов файла
d(400)	(500)	-	-	-	-	-	+	-
d(400)	(600)	-	-	-	-	-	+	-
d(400)	(700)	-	-	-	-	-	+	-
d(500)	(000)	+	-	-	-	-	+	+
d(500)	(100)	+	-	-	-	-	+	+
d(500)	(200)	+	-	+	-	-	+	+
d(500)	(300)	+	-	+	-	-	+	+
d(500)	(400)	+	-	-	+	-	+	+
d(500)	(500)	+	-	-	+	-	+	+
d(500)	(600)	+	-	+	+	-	+	+
d(500)	(700)	+	-	+	+	-	+	+
d(600)	(000)	-	-	-	-	-	+	-
d(600)	(100)	-	-	-	-	-	+	-
d(600)	(200)	-	-	-	-	-	+	-
d(600)	(300)	-	-	-	-	-	+	-
d(600)	(400)	-	-	-	-	-	+	-
d(600)	(500)	-	-	-	-	-	+	-
d(600)	(600)	-	-	-	-	-	+	-
d(600)	(700)	-	-	-	-	-	+	-
d(700)	(000)	+	+	-	-	+	+	+
d(700)	(100)	+	+	-	-	+	+	+
d(700)	(200)	+	+	+	-	+	+	+
d(700)	(300)	+	+	+	-	+	+	+

Пра-						Сме-			
ва	Со-		Уда-		на				
ди-	Пра-	зда-	ле-	За-	Чте-	ди-	Просмотр	Пере-	Смена
рек-	ва	ние	ние	пись	ние	рек-	файлов в	имено-	атрибу-
то-	фай-	фай-	фай-	в	фай-	то-	директо-	вание	тов
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

4. На основании заполненной выше таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполняя таблицу “Установленные права и разрешенные действия” (таб. 3.2).

Таблица 3.2: Минимальные права для совершения операций

Операция	min права на директорию	min права на файл
Создание файла	(-wx)(3)	(- - -)(0)
Удаление файла	(-wx)(3)	(- - -)(0)
Чтение файла	(- - x)(1)	(r - -)(4)
Запись в файл	(- - x)(1)	(-w-)(2)
Переименование файла	(-wx)(3)	(- - -)(0)
Создание поддиректории	(-wx)(3)	(- - -)(0)
Удаление поддиректории	(-wx)(3)	(- - -)(0)

## 4 Выводы

Получил практически навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.