

# Отчёт по лабораторной работе №2

## Информационная безопасность

### Дискреционное разграничение прав в Linux. Основные атрибуты

Выполнила: Павлова Полина Алексеевна,  
НПИбд-02-21, 1032212967

#### Содержание

1	Цель работы .....	1
2	Теоретическое введение.....	1
3	Выполнение лабораторной работы.....	2
3.1	Атрибуты файлов .....	2
3.2	Заполнение таблицы 2.1 .....	4
3.3	Заполнение таблицы 2.2 .....	7
4	Вывод.....	8
5	Список литературы. Библиография .....	8

## 1 Цель работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

## 2 Теоретическое введение

**Операционная система** — то комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].

**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. [2].

## 3 Выполнение лабораторной работы

### 3.1 Атрибуты файлов

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

```
[root@papavlova12 ~]# useradd guest
```

(рис. 1. `useradd guest`)

2. Задайте пароль для пользователя guest (используя учётную запись администратора): `passwd guest`

```
[root@papavlova12 ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: 
```

(рис. 2. `passwd guest`)

3. Войдите в систему от имени пользователя guest.

```
[root@papavlova12 ~]# su - guest
```

(рис. 3. изменение пользователя)

```
[guest@papavlova12 ~]$
```

(рис. 4. `guest`)

4. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию.

```
[guest@papavlova12 ~]$ pwd
/home/guest
[guest@papavlova12 ~]$ cd
```

(рис. 5. `pwd`)

5. Уточните имя вашего пользователя командой `whoami`.

```
[guest@papavlova12 ~]$ whoami
guest
```

(рис. 6. `whoami`)

6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups`.

```
guest
[guest@papavlova12 ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@papavlova12 ~]$ groups
guest
```

(рис. 7. `id u groups`)

7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.

```
guest
[guest@papavlova12 ~]$
```

(рис. 8. Совпадение)

8. Просмотрите файл /etc/passwd командой `cat /etc/passwd`. Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах.

```
guest:x:1001:1001::/home/guest:/bin/bash
```

(рис. 9. `cat /etc/passwd`)

9. Определите существующие в системе директории командой `ls -l /home/`. Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?

```
[guest@papavlova12 ~]$ ls -l /home/
total 4
drwx-----.  4 guest      guest      133 Sep  4 11:08 guest
drwx-----. 14 papavlova12 papavlova12 4096 Sep  4 11:08 papavlova12
```

(рис. 10. `ls -l /home/`)

10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?

```
[guest@papavlova12 ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/papavlova12
----- /home/guest
```

(рис. 11. `lsattr /home`)

11. Создайте в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.

```
[guest@papavlova12 ~]$ mkdir dir1
[guest@papavlova12 ~]$ ls -l
total 0
drwxr-xr-x.  2 guest guest 6 Sep  4 11:17 dir1
[guest@papavlova12 ~]$ lsattr /dir1
lsattr: No such file or directory while trying to stat /dir1
[guest@papavlova12 ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/papavlova12
----- /home/guest
```

(рис. 12. `mkdir dir1`)

12. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l`

```
[guest@papavlova12 ~]$ chmod 000 dir1
[guest@papavlova12 ~]$ ls -l
total 0
d------.  2 guest guest 6 Sep  4 11:17 dir1
```

(рис. 13. `chmod 000 dir1`)

13. Попробуйте создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1 Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1.

```
[guest@papavloval2 ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@papavloval2 ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
```

(рис. 14. "test" > /home/guest/dir1/file1)

### 3.2 Заполнение таблицы 2.1

14. Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), 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 «-».

Права дирек тории	Права файла	Создан ие файла	Удале ние файла	Запись в файл	Чтени е файла	Смена дирек тории	Просм отр файло в в дирек тории	Переи мено- 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)	-	-	-	+	+	-	-	+
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)	-	-	-	-	-	+	-	-
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)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Таблица 2.1 «Установленные права и разрешённые действия»

Пример заполнения таблицы 2.1:

```
[guest@papavloval2 ~]$ mkdir dir1
[guest@papavloval2 ~]$ touch dir1/file1
[guest@papavloval2 ~]$ ls
dir1
[guest@papavloval2 ~]$ ls dir1/
file1
[guest@papavloval2 ~]$ chmod 000 dir1
[guest@papavloval2 ~]$ chmod 000 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@papavloval2 ~]$ chmod 111 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@papavloval2 ~]$ chmod 111 dir1
[guest@papavloval2 ~]$ chmod 000 dir1/file1
[guest@papavloval2 ~]$ chmod 000 dir1
[guest@papavloval2 ~]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest@papavloval2 ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@papavloval2 ~]$ echo "text" > dir1/file1
-bash: dir1/file1: Permission denied
[guest@papavloval2 ~]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest@papavloval2 ~]$ cd dir1
-bash: cd: dir1: Permission denied
[guest@papavloval2 ~]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest@papavloval2 ~]$ mv dir1/file1 dir1/file2
bash: mv: command not found...
[guest@papavloval2 ~]$ mv dir1/file1 dir1/file2
mv: failed to access 'dir1/file2': Permission denied
[guest@papavloval2 ~]$ chmod 700 file1
chmod: cannot access 'file1': No such file or directory
[guest@papavloval2 ~]$ chmod 700 dir/file1
chmod: cannot access 'dir/file1': No such file or directory
[guest@papavloval2 ~]$ chmod 700 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
```

(рис. 16. Проверка директории d(000) и d(100) с правами файла 000)

```
[guest@papavlova12 ~]$ chmod 100 dir1
[guest@papavlova12 ~]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest@papavlova12 ~]$ rm dir1/file1
rm: remove write-protected regular empty file 'dir1/file1'? y
rm: cannot remove 'dir1/file1': Permission denied
[guest@papavlova12 ~]$ echo "text" > dir1/file1
-bash: dir1/file1: Permission denied
[guest@papavlova12 ~]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest@papavlova12 ~]$ cd dir1
[guest@papavlova12 dir1]$ ls
ls: cannot open directory '.': Permission denied
[guest@papavlova12 dir1]$ cd
[guest@papavlova12 ~]$ ls dir1
ls: cannot open directory 'dir1': Permission denied
[guest@papavlova12 ~]$ mv dir1/file1 dir1/file2
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
[guest@papavlova12 ~]$ chmod 700 dir1/file1
[guest@papavlova12 ~]$ chmod 700 dir1
[guest@papavlova12 ~]$ touch dir1/file2
[guest@papavlova12 ~]$ rm dir1/file1
[guest@papavlova12 ~]$ echo "text" > dir1/file2
[guest@papavlova12 ~]$ cat dir1/file2
text
[guest@papavlova12 ~]$ cd dir1
[guest@papavlova12 dir1]$ cd
[guest@papavlova12 ~]$ ls dir1
file2
[guest@papavlova12 ~]$ mv dir1/file2 dir1/file1
[guest@papavlova12 ~]$ ls dir1/
file1
[guest@papavlova12 ~]$ chmod 000 dir1/file1
[guest@papavlova12 ~]$
```

(рис. 17. Проверка директории d(700) с правами файла 700)

3.3 Заполнение таблицы 2.2

15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2.

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Таблица 2.2 “Минимальные права для совершения операций”

## 4 Вывод

Были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

## 5 Список литературы. Библиография

- [1] Операционные системы: <https://blog.skillfactory.ru/glossary/operacziionnaya-sistema/>
- [2] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>