

# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

---

Факультет физико-математических и естественных наук

## ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

---

Тема: Дискреционное разграничение прав в Linux. Основные атрибуты

дисциплина: Информационная безопасность

Студент: Койфман Кирилл Дмитриевич

Группа: НПИбд-01-21

### Введение.

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.

Задачи.

1. Проведём последовательность тестов над атрибутами файлов и каталогов.
2. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет.
3. На основании заполненной таблицы определим минимально необходимые права для выполнения операций внутри директории dir1 и заполним таблицу «Минимальные права для совершения операций».

### Ход работы

1 задание

---

Для начала в установленной ОС создадим учётную запись пользователя guest, зададим для неё пароль, после чего войдём в систему от имени этого пользователя (рис.1 - рис.3):

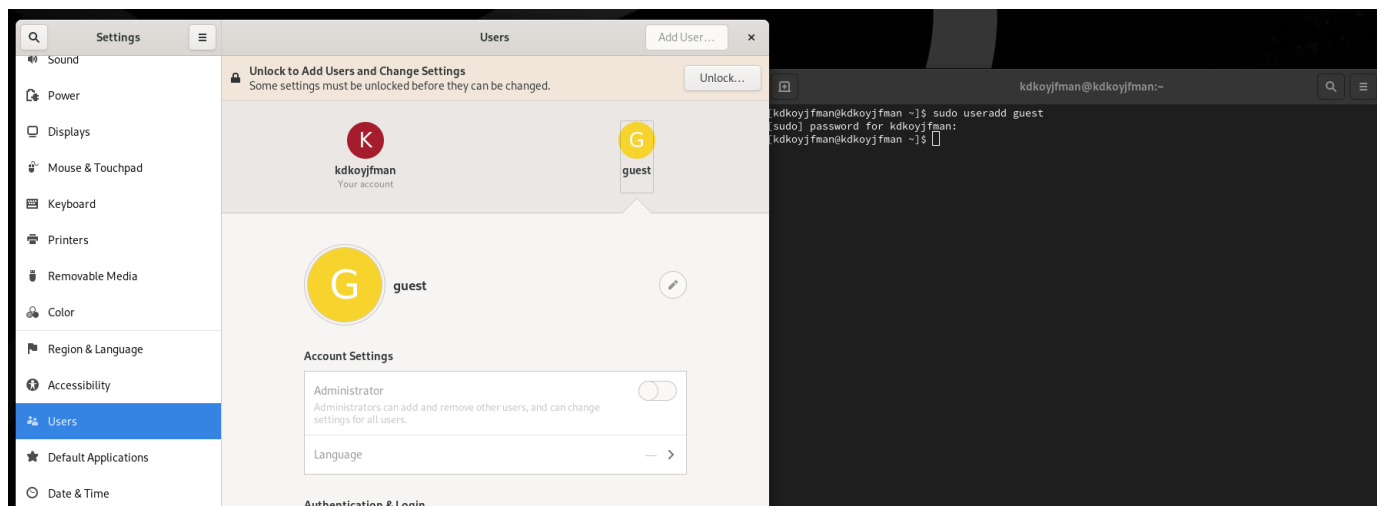


РИС.1(создание учётной записи)

```
[kdkoyjfman@kdkoyjfman ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[kdkoyjfman@kdkoyjfman ~]$
```

РИС.2(установка пароля для учётной записи)

```
[kdkoyjfman@kdkoyjfman ~]$ su guest
Password:
[guest@kdkoyjfman kdkoyjfman]$
```

РИС.3(вход в систему через новую учётную запись)

Далее определим директорию, в которой находимся (рис.4):

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

РИС.4(это не домашняя директория guest, поэтому переходим в другую)

Уточним имя пользователя, его группу, а также группы, куда входит пользователь, с помощью команд `id` и `groups` и сравним выведенные результаты (рис.5 - рис.7):

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

РИС.5(было установлено, что это пользователь guest)

```
[guest@kdkoyjfman ~]$ id guest
uid=1001(guest) gid=1001(guest) groups=1001(guest)
[guest@kdkoyjfman ~]$
```

РИС.6(вывод имени пользователя, его группы, а также групп, куда он входит, с помощью `id`)

```
[guest@kdkoyjfman ~]$ groups guest
guest : guest
[guest@kdkoyjfman ~]$
```

РИС.7(вывод группы пользователя, а также групп, куда он входит, с помощью `groups`)

Исходя из полученных данных (рис.6, рис.7), можно утверждать, что пользователь `guest` состоит только в своей группе `1001(guest)` и эта информация подтверждается результатом команды `groups`.

Также сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки (рис.8):

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

РИС.8(разницы в получаемых данных нет)

Просмотрим файл /etc/passwd командой **cat**, найдём данные о нашей учётной записи и сравним с теми данными, что получили ранее (рис.9):

```
[guest@kdkoyjfman ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@kdkoyjfman ~]$
```

РИС.9(данные uid и gid совпадают)

Определим существующие в системе директории (рис.10):

```
[guest@kdkoyjfman ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Sep 12 17:42 guest
drwx-----. 14 kdkoyjfman kdkoyjfman 4096 Sep 12 17:42 kdkoyjfman
[guest@kdkoyjfman ~]$
```

РИС.10(получили информацию о директориях *guest* и *kdkoyjfman* с правами на чтение, редактирование и выполнение для владельцев этих директорий)

А сейчас проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home (рис.11):

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

РИС.11(удалось получить информацию о расширенных атрибутах домашней директории *guest*, однако не удалось получить информацию о расширенных атрибутах других директорий)

Теперь попробуем создать в домашней директории поддиректорию *dir1* и определим командами **ls -l** и **lsattr**, какие права доступа и расширенные атрибуты были выставлены на эту директорию (рис.12):

```
[guest@kdkoyjfman ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 12 17:49 dir1
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Documents
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Music
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Public
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Templates
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Videos
[guest@kdkoyjfman ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@kdkoyjfman ~]$
```

РИС.12(владелец может считывать, редактировать и выполнять содержимое директории, пока члены группы и остальные только считывать и выполнять. Расширенные атрибуты не установлены)

Снимем с директории *dir1* все атрибуты (рис.13):

```
[guest@kdkoyjfman ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Desktop
d----- 2 guest guest 6 Sep 12 17:49 dir1
drwxr-xr-x. 2 guest guest 6 Sep 12 17:42 Documents
[guest@kdkoyjfman ~]$
```

РИС.13(все атрибуты директории были успешно сняты)

Наконец, попытаемся создать в директории файл file1 (рис.14):

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

РИС.14(создать файл не удалось, потому что ранее мы ограничили права доступа к директории)

2 задание

Заполним 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, занесём в таблицу знак «+», если не разрешена, знак «-» (таблица 1):

ТАБЛИЦА 1

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(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)	-	-	-	-	-	+	-	-

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(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)	+	+	+	+	+	+	+	+

3 задание

На основании заполненной таблицы 1 определим минимально необходимые права для выполнения операций внутри директории dir1 и заполним таблицу 2 (таблица 2):

ТАБЛИЦА 2

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)

Операция	Минимальные права на директорию	Минимальные права на файл
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)

Заключение

В ходе проделанной лабораторной работы мной были усвоены навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.