

# **Дискреционное разграничение прав в Linux. Два пользователя**

**Основы информационной безопасности**

Симонова Полина Игоревна

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Задание</b>	<b>6</b>
<b>3 Теоретическое введение</b>	<b>7</b>
<b>4 Выполнение лабораторной работы</b>	<b>9</b>
4.1 Заполнение таблицы 3.1 . . . . .	13
4.2 Заполнение таблицы 3.2 . . . . .	19
<b>5 Выводы</b>	<b>20</b>
<b>6 Список литературы</b>	<b>21</b>

# Список иллюстраций

4.1	Создание пользователя . . . . .	9
4.2	Добавление пользователя в группу . . . . .	9
4.3	Вход в терминал от имени другого пользователя . . . . .	10
4.4	Текущая директория для guest . . . . .	10
4.5	Текущая директория для guest2 . . . . .	10
4.6	Информация о пользователе guest2 . . . . .	11
4.7	Информация о пользователе guest . . . . .	11
4.8	Содержимое файла etc/group . . . . .	11
4.9	Регистрация пользователя в группе . . . . .	12
4.10	Изменение прав директории . . . . .	12
4.11	Изменение прав директории . . . . .	12
4.12	Пример заполнения таблицы 3.1 . . . . .	13

# **Список таблиц**

# **1 Цель работы**

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

## **2 Задание**

1. Создание пользователя guest2, добавление его в группу пользователей guest
2. Заполнение таблицы 3.1
3. Заполнение таблицы 3.2 на основе таблицы 3.1.

## 3 Теоретическое введение

**Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [1]

**Группы пользователей Linux** кроме стандартных root и users, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен. [2]

- daemon - от имени этой группы и пользователя daemon запускаются сервисы, которым необходима возможность записи файлов на диск.
- sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
- sync - позволяет выполнять команду /bin/sync
- games - разрешает играм записывать свои файлы настроек и историю в определенную папку
- man - позволяет добавлять страницы в директорию /var/cache/man
- lp - позволяет использовать устройства параллельных портов
- mail - позволяет записывать данные в почтовые ящики /var/mail/

- proxy - используется прокси серверами, нет доступа записи файлов на диск
- www-data - с этой группой запускается веб-сервер, она дает доступ на запись /var/www, где находятся файлы веб-документов
- list - позволяет просматривать сообщения в /var/mail
- nogroup - используется для процессов, которые не могут создавать файлов на жестком диске, а только читать, обычно применяется вместе с пользователем nobody.
- adm - позволяет читать логи из директории /var/log
- tty - все устройства /dev/vca разрешают доступ на чтение и запись пользователям из этой группы
- disk - открывает доступ к жестким дискам /dev/sd\* /dev/hd\*, можно сказать, что это аналог рут доступа.
- dialout - полный доступ к серийному порту
- cdrom - доступ к CD-ROM
- wheel - позволяет запускать утилиту sudo для повышения привилегий
- audio - управление аудиодрайвером
- src - полный доступ к исходникам в каталоге /usr/src/
- shadow - разрешает чтение файла /etc/shadow
- utmp - разрешает запись в файлы /var/log/utmp /var/log/wtmp
- video - позволяет работать с видеодрайвером
- plugdev - позволяет монтировать внешние устройства USB, CD и т д
- staff - разрешает запись в папку /usr/local

## 4 Выполнение лабораторной работы

1. Пользователь guest был создан в лабораторной работе №2, поэтому в этой лабораторной работе его не создаем заново
2. Пароль для пользователя guest тоже был задан в лабораторной работе №2.
3. С правами администратора создаю пользователя guest с помощью команды useradd, далее с помощью команды passwd задаю пароль пользователю (рис. 1).

```
pisimonova@pisimonova:~$ sudo useradd guest2
[sudo] пароль для pisimonova:
pisimonova@pisimonova:~$ sudo passwd guest2
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
```

Рисунок 4.1: Создание пользователя

4. Добавляю пользователя guest2 в группу guest (рис. 2).

```
pisimonova@pisimonova:~$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
pisimonova@pisimonova:~$ su guest
```

Рисунок 4.2: Добавление пользователя в группу

5. Зашла на двух разных консолях от имени двух разных пользователей с помощью команды su (рис. 3).

```
pisimonova@pisimonova:~$ su guest2
Пароль:
guest2@pisimonova: /home/pisimonova$ pwd
```

Рисунок 4.3: Вход в терминал от имени другого пользователя

6. Проверяю путь директории, в которой я нахожусь с помощью pwd.

Проверка для пользователя guest (рис. 4).

```
guest@pisimonova:/home/pisimonova$ pwd
/home/pisimonova
```

Рисунок 4.4: Текущая директория для guest

Проверка для пользователя guest2 (рис. 5).

```
guest2@pisimonova:/home/pisimonova$ pwd
/home/pisimonova
```

Рисунок 4.5: Текущая директория для guest2

Стоит отметить, что вход в терминал от имени пользователей был выполнен в домашней директории пользователя pisimonova, которую команда pwd вывела. Домашней директорией пользователей она не является. Текущая директория с приглашением командной строки совпадает.

7. Проверяю имя пользователей с помощью команды whoami, с помощью команды id могу увидеть группы, к которым принадлежит пользователь и коды этих групп (gid), команда groups просто выведет список групп, в которые входит пользователь.

id -Gn - выведет названия групп, которым принадлежит пользователь  
id -G - выведет только код групп, которым принадлежит пользователь.

Проверка для пользователя guest2 (рис. 6).

```

/home/pisimonova
guest2@pisimonova:/home/pisimonova$ whoami
guest2
guest2@pisimonova:/home/pisimonova$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=uncon
fined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
guest2@pisimonova:/home/pisimonova$ groups guest2
guest2 : guest2 guest
guest2@pisimonova:/home/pisimonova$ id -Gn
guest2 guest
guest2@pisimonova:/home/pisimonova$ id -G
1002 1001

```

Рисунок 4.6: Информация о пользователе guest2

Проверка для пользователя guest (рис. 7).

```

guest@pisimonova:/home/pisimonova$ whoami
guest
guest@pisimonova:/home/pisimonova$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
guest@pisimonova:/home/pisimonova$ groups guest
guest : guest
guest@pisimonova:/home/pisimonova$ id -Gn
guest
guest@pisimonova:/home/pisimonova$ id -G
1001

```

Рисунок 4.7: Информация о пользователе guest

Пользователь guest2 входит в две группы пользователей: в группу guest, потому что я сама его туда добавила, и в группу guest2, которая создалась автоматически при создании пользователя.

8. Вывела интересующее меня содержимое файла etc/group, видно, что в группе guest два пользователя, а в группе guest2 один (рис. 8).

```

pisimonova:x:1000:
guest:x:1001:guest2
wireshark:x:981:
usbmon:x:980:
guest2:x:1002:

```

Рисунок 4.8: Содержимое файла etc/group

9. От имени пользователя guest2 регистрирую его в группе guest с помощью команды newgrp (рис. 9).

```
guest2@pisimonova:/home/pisimonova$ newgrp guest
guest2@pisimonova:/home/pisimonova$ cd /home/guest
```

Рисунок 4.9: Регистрация пользователя в группе

10. Добавляю права на чтение, запись и исполнение группе пользователей guest (guest, guest2) на директорию home/guest в которой находятся все файлы для последующей работы (рис. 10).

```
guest@pisimonova:/home/pisimonova$ cd
guest@pisimonova:~$ chmod g+rwx /home/guest
guest@pisimonova:~$ ls
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка      'Рабочий стол'
```

Рисунок 4.10: Изменение прав директории

11. От имени пользователя guest снимаю все атрибуты с директории dir1, созданной в предыдущей лабораторной работе. Проверяю, что права действительно сняты (рис. 11).

```
guest@pisimonova:~$ chmod 000 dir1
guest@pisimonova:~$ ls
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка      'Рабочий стол'
guest@pisimonova:~$ ls -l
итого 0
d----- 2 guest guest 19 фев 13 21:59  dir1
drwxr-xr-x 2 guest guest  6 фев 13 21:34  Видео
drwxr-xr-x 2 guest guest  6 фев 13 21:34  Документы
drwxr-xr-x 2 guest guest  6 фев 13 21:34  Загрузки
drwxr-xr-x 2 guest guest  6 фев 13 21:34  Изображения
drwxr-xr-x 2 guest guest  6 фев 13 21:34  Музыка
drwxr-xr-x 2 guest guest  6 фев 13 21:34  Общедоступные
drwxr-xr-x 2 guest guest  6 фев 13 21:34  'Рабочий стол'
drwxr-xr-x 2 guest guest  6 фев 13 21:34  Шаблоны
guest@pisimonova:~$ cd /home/guest
```

Рисунок 4.11: Изменение прав директории

## 4.1 Заполнение таблицы 3.1

Далее проверяю как пользователь guest2 будет взаимодействовать с файлами в этой директории (рис. 12).

```
guest2@pisimonova:/home/pisimonova$ cd /home/guest
guest2@pisimonova:/home/guest$ ls
dir1 Документы Изображения Общедоступные Шаблоны
Видео Загрузки Музыка 'Рабочий стол'
guest2@pisimonova:/home/guest$ ls dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
guest2@pisimonova:/home/guest$ rm dir1
rm: невозможно удалить 'dir1': Это каталог
guest2@pisimonova:/home/guest$ rm dir1/a
rm: невозможно удалить 'dir1/a': Отказано в доступе
guest2@pisimonova:/home/guest$ touch dir1/file1
touch: невозможно выполнить touch для 'dir1/file1': Отказано в доступе
guest2@pisimonova:/home/guest$ echo 'test' > dir1/file1
bash: dir1/file1: Отказано в доступе
guest2@pisimonova:/home/guest$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
guest2@pisimonova:/home/guest$ chmod 020 dir1/fille1
chmod: невозможно получить доступ к 'dir1/fille1': Отказано в доступе
guest2@pisimonova:/home/guest$ ls
```

Рисунок 4.12: Пример заполнения таблицы 3.1

Права директории	Права файла	Просмотр						
		Создание	Удаление	Чтение	Изменение	Переименование	Смена	Манипуляции
d-----	-----	-	-	-	-	-	-	-
(000)	(000)							
d----x--	-----	-	-	-	-	-	-	+
(010)	(000)							
d---w---	-----	-	-	-	-	-	-	-
(020)	(000)							
d---wx--	-----	+	+	-	-	+	-	+
(030)	(000)							
d---r---	-----	-	-	-	-	-	+	-
(040)	(000)							

Права		Просмотр									
директории	Права файла	Созда	Удаление	Чтени	Смена	файлов	Смена	Переименование	Изменение	Перемещение	
		файла	файла	файла	файла	директории	директории	файла	файла	директории	
d---r-x--	-----	-	-	-	-	+	+	-	-	+	
(050)	(000)										
d---rw---	-----	-	-	-	-	-	+	-	-	-	
(060)	(000)										
d---rwx--	-----	+	+	-	-	+	+	+	+	+	
(070)	(000)										
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)										

---

Просмотр

Права директории	Права файла	Создание	Удаление	Чтение	Смена файлов	Переименование	Изменение атрибутов
директории	файла	файла	файла	файла	файлам директории	файла	атрибутов
d-----x--	-----w---	-	-	+	-	-	-
(010)	(020)						
d----w---	-----w---	-	-	-	-	-	-
(020)	(020)						
d----wx--	-----w---	+	+	+	-	+	+
(030)	(020)						
d---r----	-----w---	-	-	-	-	+	-
(040)	(020)						
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)						

Права		Просмотр									
директории	Права файла	Созда	Удаление	Чтени	Смена	файлов	Смена	Переименование	Изменение	Права	
		файла	файла	файла	файла	директории	директории	файла	директории	файла	
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)										
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)										

---

		Просмотр									
		Запись					файлов			Смена	
Права		Созда		Удаление		Чтени		Смена		Переименование	
директории	Права файла	файла	файла	файл	директ	файл	директо	файла	директо	файла	
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)										
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)										

Права		Просмотр									
директории	Права файла	Созда	Удаление	Чтени	Смена	файлов	Смена	Переименование	Изменение	Атрибутов	
		файла	файла	файла	файла	директории	директории	файла	директории	файла	
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)										
d---r----	-----rwx--	-	-	-	-	-	-	+	-	-	
(040)	(070)										
d---r-x--	-----rwx--	-	-	+	+	+	+	+	-	+	
(050)	(070)										
d---rw---	-----rwx--	-	-	-	-	-	-	+	-	-	
(060)	(070)										
d---rwx--	-----rwx--	+	+	+	+	+	+	+	+	+	
(070)	(070)										

Таблица 3.1 «Установленные права и разрешённые действия для групп»

## 4.2 Заполнение таблицы 3.2

На основе таблицы 3.1 заполняю таблицу 3.2.

Операция	Права на директорию	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)

Таблица 3.2 «Минимальные права для совершения операций от имени пользователей входящих в группу»

## **5 Выводы**

Были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей

## **6 Список литературы**

- [0] Методические материалы курса
- [1] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>