

# **Лабораторная работа № 3**

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

Усов Александр Александрович НБибд-02-18

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
<b>5</b>	<b>Выводы</b>	<b>24</b>

## Список иллюстраций

4.1	создал учётную запись пользователя guest . . . . .	9
4.2	Вошел в систему . . . . .	9
4.3	Уточнил имя пользователя, его группу, а также группы, куда входит пользователь . . . . .	10
4.4	cat /etc/group . . . . .	10
4.5	Сравнение . . . . .	10
4.6	newgrp guest . . . . .	11
4.7	chmod g+rwx /home/guest . . . . .	11

## Список таблиц

4.1	Установленные права и разрешённые действия . . . . .	12
4.2	Минимально необходимые права для выполнения операций . . .	23

# 1 Цель работы

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

## 2 Задание

1. Добавить пользователя guest2
2. Создать пароль для пользователя guest2
3. Добавить guest2 в группу guest
4. Опытным путём заполнить таблицу “Установленные права и разрешённые действия”
5. На основании заполненной таблицы определить те или иные минимально необходимые права для выполнения операций внутри директории

### 3 Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

И это очень важно, потому что локальный доступ к файлам для всех программ и всех пользователей позволил бы вирусам без проблем уничтожить систему. Но новым пользователям могут показаться очень сложными новые права на файлы в linux, которые очень сильно отличаются от того, что мы привыкли видеть в Windows. В этой статье мы попытаемся разобраться в том как работают права файлов в linux, а также как их изменять и устанавливать.

Изначально каждый файл имел три параметра доступа. Вот они:

Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;

Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;

Выполнение - вы не можете выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу.

Но все эти права были бы бессмысленными, если бы применялись сразу для всех пользователей. Поэтому каждый файл имеет три категории пользователей,

для которых можно устанавливать различные сочетания прав доступа:

Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение. Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу. Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла. Именно с помощью этих наборов полномочий устанавливаются права файлов в linux. Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является или к тем, доступ к которым ему разрешен. Только пользователь Root может работать со всеми файлами независимо от их набора их полномочий.

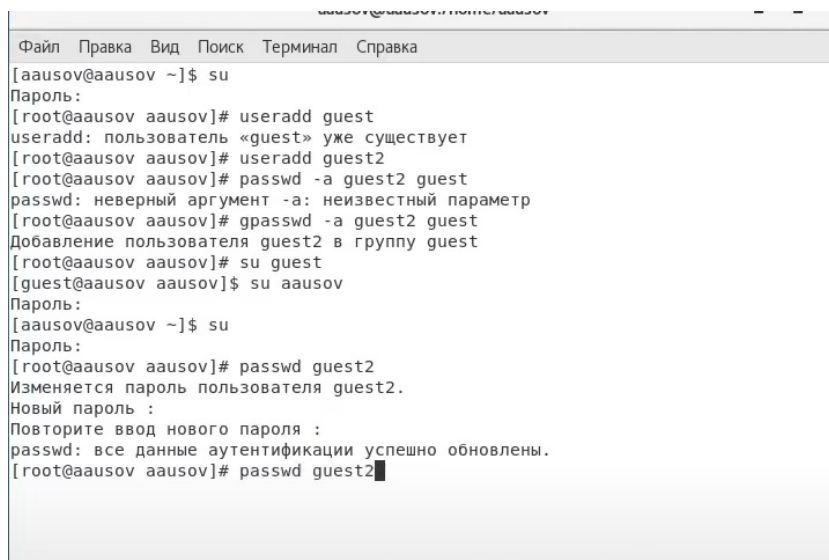
Но со временем такой системы стало не хватать и было добавлено еще несколько флагов, которые позволяют делать файлы не изменяемыми или же выполнять от имени суперпользователя

Более подробно о правах см. в [1].



## 4 Выполнение лабораторной работы

1. В установленной операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора) Задал пароль для пользователя guest (используя учётную запись администратора) (рис. 4.2): passwd guest (рис. 4.1): useradd guest



```
Файл Правка Вид Поиск Терминал Справка
[aausov@aausov ~]$ su
Пароль:
[root@aausov aausov]# useradd guest
useradd: пользователь «guest» уже существует
[root@aausov aausov]# useradd guest2
[root@aausov aausov]# passwd -a guest2 guest
passwd: неверный аргумент -a: неизвестный параметр
[root@aausov aausov]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@aausov aausov]# su guest
[guest@aausov aausov]$ su aausov
Пароль:
[aausov@aausov ~]$ su
Пароль:
[root@aausov aausov]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@aausov aausov]# passwd guest2
```

Рис. 4.1: создал учётную запись пользователя guest

2. Осуществите вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. (рис. 4.2).



```
[guest@aausov aausov]$ ls
ls: невозможно открыть каталог .: отказано в доступе
[guest@aausov aausov]$ pwd
/home/aausov
[guest@aausov aausov]$ cd ..
[guest@aausov home]$ cd guest
[guest@aausov ~]$ whoami
guest
[guest@aausov ~]$

[guest2@aausov aausov]$ groups guest2
guest2 : guest2 guest
[guest2@aausov aausov]$ pwd
/home/aausov
[guest2@aausov aausov]$ cd ..
[guest2@aausov home]$ cd guest2
[guest2@aausov ~]$ whoami
guest2
[guest2@aausov ~]$
```

Рис. 4.2: Вошел в систему

- Для обоих пользователей командой `pwd` определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки. (рис. 4.2).
- Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравните вывод команды `groups` с выводом команд `id -Gn` и `id -G`. (рис. 4.3).

```

[guest@aasov ~]$ id
uid=1001(guest) gid=1001(guest) groups=guest
[guest2@aasov ~]$ id
uid=1002(guest2) gid=1002(guest2) groups=guest2

```

Рис. 4.3: Уточнил имя пользователя, его группу, а также группы, куда входит пользователь

- Сравните полученную информацию с содержимым файла `/etc/group`. Просмотрите файл командой `cat /etc/group` (рис. 4.4) и (рис. 4.5)

```

[guest@aasov ~]$ cat /etc/group
guest:x:1001:1001:guest:/home/guest:/bin/bash
guest2:x:1002:1002:guest2:/home/guest2:/bin/bash

```

Рис. 4.4: cat /etc/group

```

[guest@aasov ~]$ cat /etc/group
guest:x:1001:1001:guest:/home/guest:/bin/bash
guest2:x:1002:1002:guest2:/home/guest2:/bin/bash

```

Рис. 4.5: Сравнение

- От имени пользователя `guest2` выполните регистрацию пользователя `guest2` в группе `guest` командой `newgrp guest` (рис. 4.6)

```
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
aasov:x:1000:aasov
guest:x:1001:guest2
guest2:x:1002:
[guest@aasov ~]$

[guest2@aasov ~]$ id -Gn
[guest2@aasov ~]$ id -G
1002 1001
[guest2@aasov ~]$ newgrp guest
[guest2@aasov ~]$
```

Рис. 4.6: newgrp guest

8. От имени пользователя guest измените права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rwX /home/guest` (рис. 4.7)

```
aasov:x:1000:aasov
guest:x:1001:guest2
guest2:x:1002:
[guest@aasov ~]$ chmod g+rwX /home/guest
[guest@aasov ~]$ ls -l
итого 4
drwxr-xr-x. 2 guest guest 34 сен 27 14:00 dir1
-rw-rw-r--. 1 guest guest 6 сен 27 13:55 file
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Видео
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Документы
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Изображения
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Музыка
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 27 12:58 Шаблоны
[guest@aasov ~]$

[guest2@aasov ~]$ group guest2
bash: group: команда не найдена...
[guest2@aasov ~]$ groups guest2
guest2 : guest2 guest
[guest2@aasov ~]$ pwd
/home/aasov
[guest2@aasov ~]$ cd ..
[guest2@aasov ~]$ cd guest2
[guest2@aasov ~]$ whoami
guest2
[guest2@aasov ~]$ groups guest2
guest2 : guest2 guest
[guest2@aasov ~]$ id -Gn
guest2 guest
[guest2@aasov ~]$ id -G
1002 1001
[guest2@aasov ~]$ newgrp guest
[guest2@aasov ~]$
```

Рис. 4.7: chmod g+rwX /home/guest

10. От имени пользователя guest снимите с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` (рис. 4.7) и проверьте правильность снятия атрибутов. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнил 4.1 На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории 4.2 dir1

Таблица 4.1: Установленные права и разрешённые действия

Права		Смена							
ди- ре- кто рии	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	рек- то- рии	Просмотр файлов в дирек- тории	Переименование фай- ла	Смена имени бутов файла
d---	---	-	-	-	-	-	-	-	-
-	-								
(000)	(000)								
d--	---	-	-	-	-	+	-	-	+
x-	-								
(010)	(000)								
d--	---	-	-	-	-	-	-	-	-
w-	-								
(020)	(000)								
d--	---	+	+	-	-	+	-	+	+
wx-	-								
(030)	(000)								
d-	---	-	-	-	-	-	+	-	-
r--	-								
(040)	(000)								

Права	Смена								
ди- ре- кто рии	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переименование фай- ла	Смена имени бутов файла
d-r- x- (050)	— — — (000)	-	-	-	-	+	+	-	+
d— rw— (060)	— — — (000)	-	-	-	-	-	+	-	-
d— rwx- (070)	— — — (000)	+	+	-	-	+	+	+	+
d— — — x— (000)	— — x— (010)	-	-	-	-	-	-	-	-
d— — x- x— (010)	— — x— (010)	-	-	-	-	+	-	-	+
d— — w— x— (020)	— — x— (010)	-	-	-	-	-	-	-	-

Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переимено- вание фай- ла	Смена имени бутов файла
d-- wx- (030)	-- x-	+	+	-	-	+	-	+	+
d-- r-- (040)	-- x-	-	-	-	-	-	+	-	-
d-r- x- (050)	-- x-	-	-	-	-	+	+	-	+
d-- rw- (050)	-- x-	-	-	-	-	-	+	-	-
d-- rwx- (050)	-- x-	+	+	-	-	+	+	+	+
d-- - (000)	-- w-- (020)	-	-	-	-	-	-	-	-

Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переименование фай- ла	Смена имени бутов файла
d-- x- (010)	-- w-- (020)	-	-	+	-	+	-	-	+
d-- w- (020)	-- w-- (020)	-	-	-	-	-	-	-	-
d-- wx- (030)	-- w-- (020)	+	+	+	-	+	-	+	+
d- r-- (040)	-- w-- (020)	-	-	-	-	-	+	-	-
d-r- x- (050)	-- w-- (020)	-	-	+	-	+	+	-	+
d- rw- (060)	-- w-- (020)	-	-	-	-	-	+	-	-

Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переименование фай- ла	Смена имени бутов файла
d— rwx— (070)	-- w-- (020)	+	+	+	-	+	+	+	+
d— — (000)	-- wx— (030)	-	-	-	-	-	-	-	-
d— x— (010)	-- wx— (030)	-	-	+	-	+	-	-	+
d— w— (020)	-- wx— (030)	-	-	-	-	-	-	-	-
d— wx— (030)	-- wx— (030)	+	+	+	-	+	-	+	+
d— r— (040)	-- wx— (030)	-	-	-	-	-	+	-	-



Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переименование фай- ла	Смена имени бутов файла
d-r- x- (050)	-- wx- (030)	-	-	+	-	+	+	-	+
d- rw- (050)	-- wx- (030)	-	-	-	-	-	+	-	-
d- rwx- (050)	-- wx- (030)	+	+	+	-	+	+	+	+
d-- - (000)	-r- - (030)	-	-	-	-	-	-	-	-
d-- x- (010)	-r- - (030)	-	-	-	+	+	-	-	+
d-- w- (020)	-r- - (030)	-	-	-	-	-	-	-	-

Права				Смена					
ди-	Права	Создание	Удаление	Запись	Чтение	Редактирование	Просмотр	Переименование	Смена
ре-	фай-	фай-	фай-	в	фай-	то-	файлов	фай-	имен
кто	ла	ла	ла	файл	ла	рии	в дирек-	ла	бутов
рии	ла	ла	ла	файл	ла	рии	тории	ла	файла
d--	--r--	+	+	-	+	+	-	+	+
wx-	-								
(030)	(030)								
d--	--r--	-	-	-	-	-	+	-	-
r--	-								
(040)	(030)								
d-r-	--r--	-	-	-	+	+	+	-	+
x-	-								
(050)	(030)								
d--	--r--	-	-	-	-	-	+	-	-
rw-	-								
(050)	(030)								
d--	--r--	+	+	-	+	+	+	+	+
rw-	-								
(050)	(030)								
d--	--r-	-	-	-	-	-	-	-	-
-	x-								
(000)	(050)								

Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переимено- вание фай- ла	Смена имени бутов файла
d-- x- (010)	--r- x- (050)	-	-	-	+	+	-	-	+
d-- w- (020)	--r- x- (050)	-	-	-	-	-	-	-	-
d-- wx- (030)	--r- x- (050)	+	+	-	+	+	-	+	+
d- r-- (040)	-r- x- (050)	-	-	-	-	-	+	-	-
d-r- x- (050)	-r- x- (050)	-	-	-	+	+	+	-	+
d- rw- (050)	-r- x- (050)	-	-	-	-	-	+	-	-

Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переимено- вание фай- ла	Смена имени бутов файла
d— rwx— (050)	—r- x— (050)	+	+	-	+	+	+	+	+
d— — (000)	— rw— (060)	-	-	-	-	-	-	-	-
d— x— (010)	— rw— (060)	-	-	+	+	+	-	-	+
d— w— (020)	— rw— (060)	-	-	-	-	-	-	-	-
d— wx— (030)	— rw— (060)	+	+	+	+	+	-	+	+
d— r— (040)	— rw— (060)	-	-	-	-	-	+	-	-

Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переимено- вание фай- ла	Смена имени бутов файла
d-r- x- (050)	— rw-- (060)	-	-	+	+	+	+	-	+
d— rw— (050)	— rw-- (060)	-	-	-	-	-	+	-	-
d— rwx- (050)	— rw-- (060)	+	+	+	+	+	+	+	+
d— — (000)	— rwx— (070)	-	-	-	-	-	-	-	-
d— x- (010)	— rwx— (070)	-	-	+	+	+	-	-	+

Права	Смена								
ди- ре- кто рии	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Рек- то- рии	Просмотр файлов в дирек- тории	Переименование фай- ла	Смена имени бутов файла
d-- w-- (020)	— rwx— (070)	-	-	-	-	-	-	-	-
d-- wx-- (030)	— rwx— (070)	+	+	+	+	+	-	+	+
d-- r-- (040)	— rwx— (070)	-	-	-	-	-	+	-	-
d-r- x-- (050)	— rwx— (070)	-	-	+	+	+	+	-	+
d-- rw-- (050)	— rwx— (070)	-	-	-	-	-	+	-	-

Права	Смена								
ди- ре- кто рии	Права фай- ла	Созда- ние фай- ла	Удале- ние фай- ла	Запис- ь в файл	Чтени- е фай- ла	рек- то- рии	Просмотр файлов в дирек- тории	Переимено- вание фай- ла	Смена имени бутов файла
d— rwx— (050)	—	+	+	+	+	+	+	+	+
	(070)								

Таблица 4.2: Минимально необходимые права для выполнения 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

Выполняя данную лабораторную работу, я получил практические навыки работы в консоли с атрибутами файлов для групп пользователей. # Список литературы{unnumbered}

1. ПРАВА ДОСТУПА К ФАЙЛАМ В LINUX [Электронный ресурс]. Сайт, 2021.  
URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux>.