

Лабораторная работа № 3

Дискреционное разграничение прав в Linux. Два пользователя.

Алибаева Данагуль НБибд-01-18

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	8
4	Выполнение лабораторной работы	10
5	Выводы	23
6	Список литературы	24

List of Tables

4.1	Установленные права и разрешённые действия для групп	16
4.2	Минимальные права для совершения операций от имени пользо- вателя входящих в группу	22

List of Figures

4.1	Переход под учетную запись root	10
4.2	Создание учетной записи пользователя guest2	11
4.3	Задание пароля для пользователя guest2	11
4.4	Добавление пользователя guest2 в группу guest	11
4.5	Вход в систему от двух пользователей на двух разных консолях . .	12
4.6	Определение директории	12
4.7	Уточнение групп пользователей	13
4.8	Просмотр файла /etc/passwd	13
4.9	Регистрация пользователя guest2 в группе guest	14
4.10	Изменение прав директории	15
4.11	Изменение атрибутов	15

1 Цель работы

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

2 Задание

1. В установленной операционной системе создать учётную запись пользователя `guest` (используя учётную запись администратора)
2. Задать пароль для пользователя `guest` (используя учётную запись администратора)
3. Аналогично создать второго пользователя `guest2`
4. Добавить пользователя `guest2` в группу `guest`
5. Осуществить вход в систему от двух пользователей на двух разных консолях
6. Для обоих пользователей определить директорию, в которой находимся. Сравните её с приглашениями командной строки.
7. Уточнить имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определить в какие группы входят пользователи `guest` и `guest2`. Сравнить вывод команды `groups` с выводом команд `id -Gn` и `id -G`.
8. Сравнить полученную информацию с содержимым файла `/etc/group`
9. От имени пользователя `guest2` выполнить регистрацию пользователя `guest2` в группе `guest`
10. От имени пользователя `guest` изменить права директории `/home/guest`, разрешив все действия для пользователей группы

11. От имени пользователя guest снять с директории /home/guest/dir1 все атрибуты и проверить правильность снятия атрибутов. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнить табл. 3.1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Сравнить табл. 2.1 (из лабораторной работы № 2) и табл. 3.1. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. 3.2.

3 Теоретическое введение

Атрибуты файла - это набор из девяти основных битов. Определяющих какие из пользователей обладают правами на чтение, запись, а также запуск файлов для выполнения. Данный набор формирует код, называемый режимом доступа к файлу/каталогу. Первые три бита определяют права доступа для владельца. Следующие — для группы пользователей, к которой относится файл и последние три бита — права доступа для всех остальных пользователей в системе. [1]

Существует также ещё четыре дополнительных бита. Которые определяют тип самого файла и задаются непосредственно при создании файла. С помощью команды `chmod` можно менять основные (и некоторые дополнительные) биты режима доступа. Сделать это может только владелец файла или суперпользователь. Просматривать атрибуты (в том числе и режимы доступа) позволяет команда `ls`. Таким образом, характер поведения ФС, а также распределение доступа и управление им полностью определяется атрибутами файлов. Которые хранит сама ФС — это самодостаточный и универсальный подход. [1]

Для записи кода режима доступа используется восьмеричная запись чисел. Как уже было отмечено, код доступа содержит три «триады» битов — для пользователя, группы и всех остальных, именно в таком порядке. Битам из первой триады соответствуют значения в восьмеричной записи 400, 200 и 100. Для второй триады (т. е. для группы) — 40, 20 и 10. Наконец, для третьей (все остальные) — 4, 2 и 1. В свою очередь, первому биту в каждой триаде соответствует доступ на чтение (r — «read»). Второму — на запись (w — «write») и третьему — на выполнение, т. е. x — «execute». [1]

Установка бита чтения (r) в одной из триад (или во всех) задаёт право открывать данный файл для чтения соответствующим категориям пользователей. Наличие бита записи (w) позволяет изменять файл. При этом возможно его удаление и/или переименование файла, но только в том случае, если заданы соответствующие биты для его родительского каталога, поскольку именно в его записях хранятся имена файлов. [1]

4 Выполнение лабораторной работы

1. Лабораторная работа выполнялась дома со следующими характеристиками техники:

- Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz, 2304 МГц, ядер: 4, логических процессоров: 8
- ОС Майкрософт Windows 10 Pro
- VirtualBox верс. 6.1.26

2. В установленной при выполнении предыдущей лабораторной работы операционной системе запустила терминал и перешла под учетную запись root с помощью команды su (рис. 4.1)

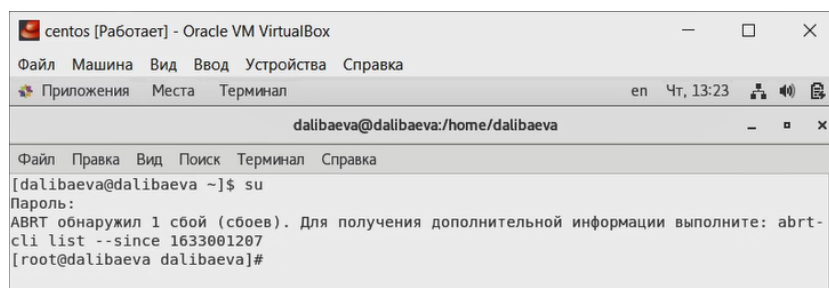
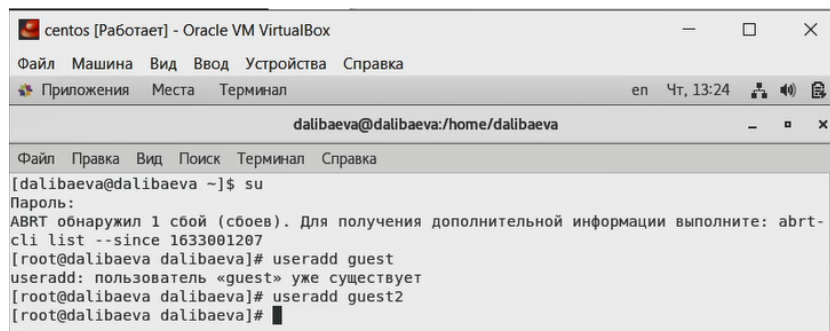


Figure 4.1: Переход под учетную запись root

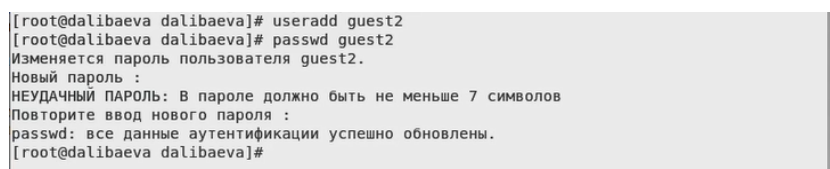
3. Создала учётную запись пользователя guest2 (используя учётную запись администратора): с помощью команды useradd guest2 (рис. 4.2)



```
centos [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Приложения Места Терминал en Чт, 13:24
dalibaeva@dalibaeva:/home/dalibaeva
Файл Правка Вид Поиск Терминал Справка
[dalibaeva@dalibaeva ~]$ su
Пароль:
ABRT обнаружил 1 сбой (сбоев). Для получения дополнительной информации выполните: abrt-
cli list --since 1633001207
[root@dalibaeva dalibaeva]# useradd guest
useradd: пользователь «guest» уже существует
[root@dalibaeva dalibaeva]# useradd guest2
[root@dalibaeva dalibaeva]#
```

Figure 4.2: Создание учетной записи пользователя guest2

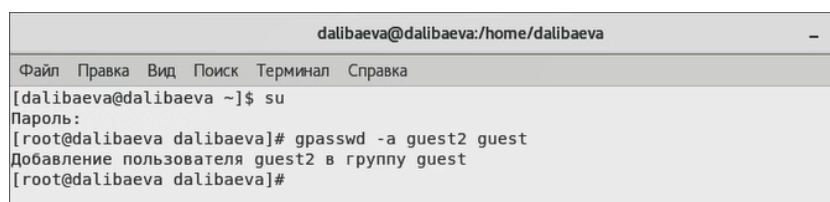
4. Задала пароль для пользователя guest2 (используя учётную запись администратора): `passwd guest2` (рис. 4.3)



```
[root@dalibaeva dalibaeva]# useradd guest2
[root@dalibaeva dalibaeva]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 7 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@dalibaeva dalibaeva]#
```

Figure 4.3: Задание пароля для пользователя guest2

5. Добавила пользователя guest2 в группу guest: `gpasswd -a guest2 guest` (рис. 4.4)



```
dalibaeva@dalibaeva:/home/dalibaeva
Файл Правка Вид Поиск Терминал Справка
[dalibaeva@dalibaeva ~]$ su
Пароль:
[root@dalibaeva dalibaeva]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@dalibaeva dalibaeva]#
```

Figure 4.4: Добавление пользователя guest2 в группу guest

6. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. (рис. 4.5)

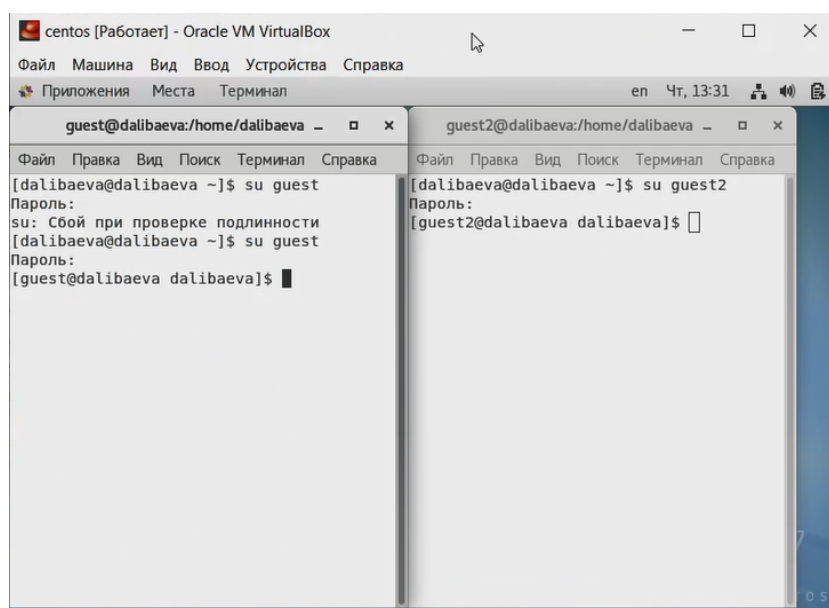


Figure 4.5: Вход в систему от двух пользователей на двух разных консолях

7. Для обоих пользователей командой `pwd` определила директорию, в которой я нахожусь. В обоих случаях я нахожусь в домашней директории пользователя `dalibaeva`. (рис. 4.6)

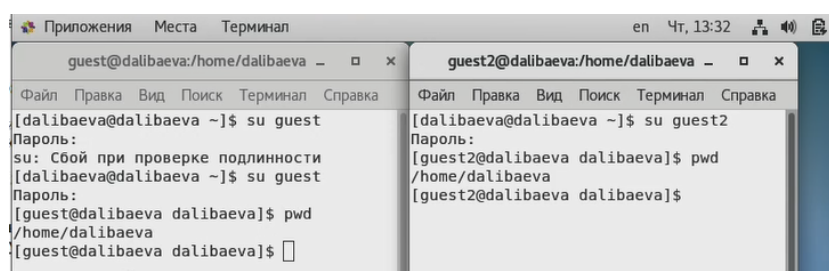


Figure 4.6: Определение директории

8. Уточнила имя пользователя, группу, кто входит в неё и к каким группам принадлежит он сам. Определила командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. В группу `guest` входят пользователи `guest` и `guest2`, а в группу `guest2` – пользователь `guest2`. Сравнила вывод команды `groups` с выводом команд `id -Gn` и `id -G`. Команда `id -Gn` показывает в каких группах состоит пользователь, а команда `id -G` – `id` этих групп (рис. 4.7)

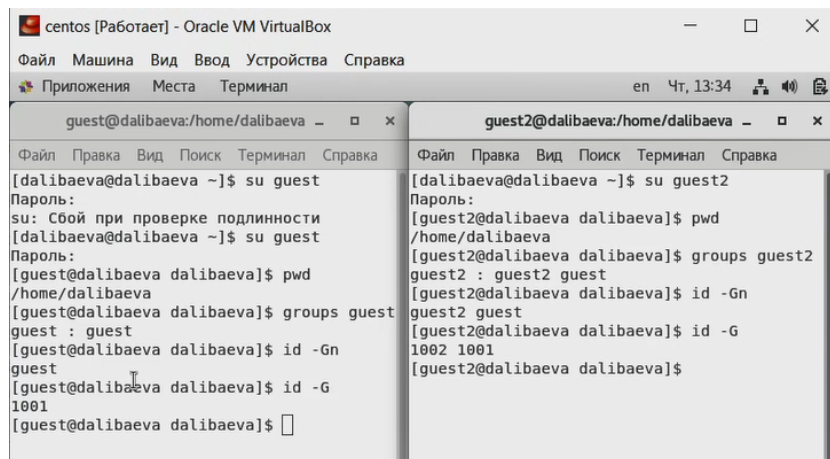


Figure 4.7: Уточнение групп пользователей

9. Сравнила полученную информацию с содержимым файла /etc/group. Просмотрела файл командой cat /etc/group (рис. 4.8)

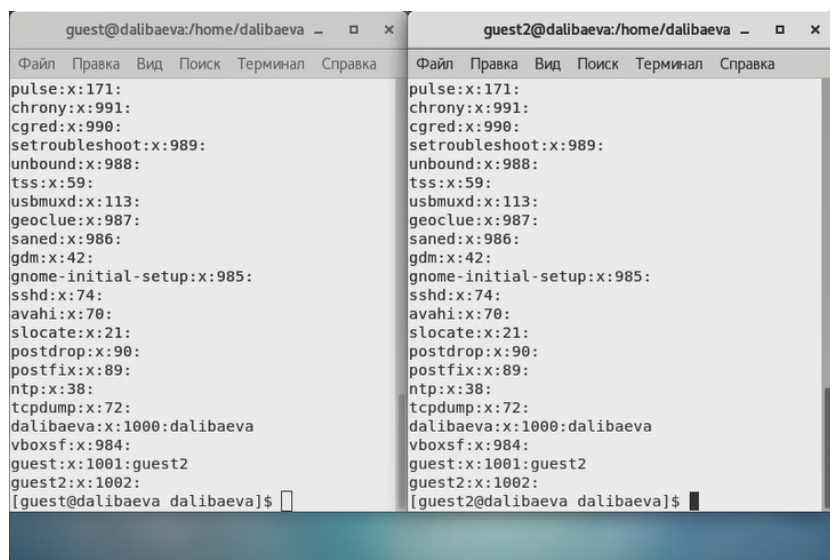
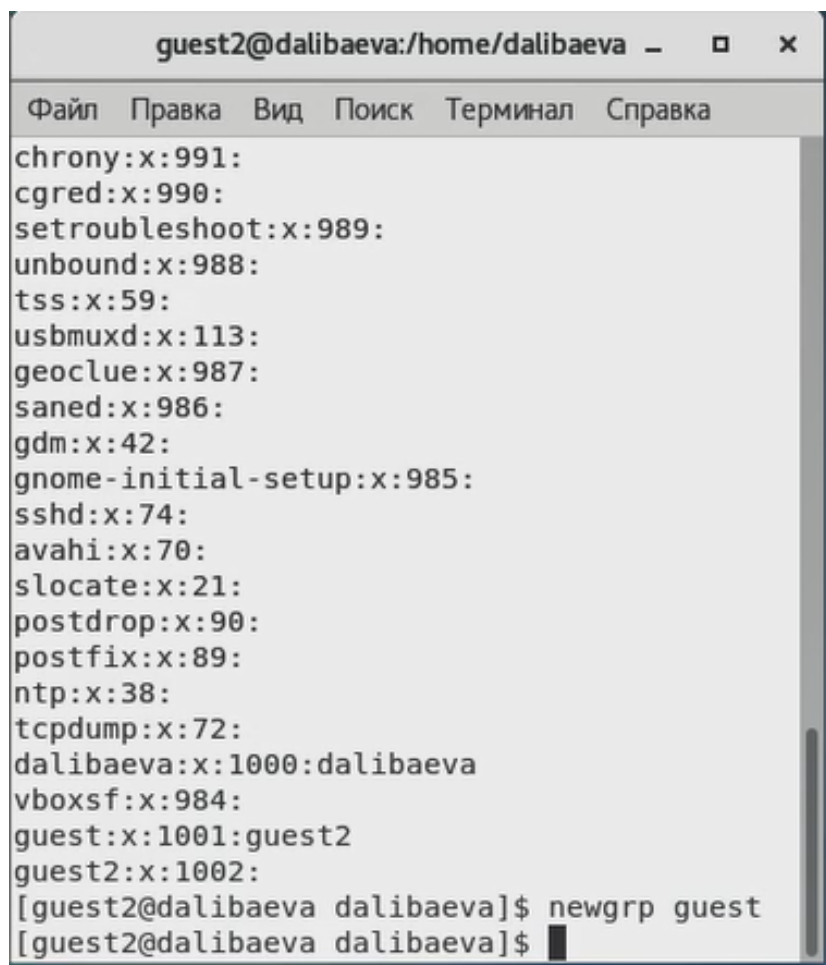


Figure 4.8: Просмотр файла /etc/passwd

10. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой newgrp guest (рис. 4.9).



```
guest2@dalibaeva:/home/dalibaeva — □ ×
Файл Правка Вид Поиск Терминал Справка
chrony:x:991:
cgred:x:990:
setroubleshoot:x:989:
unbound:x:988:
tss:x:59:
usbmuxd:x:113:
geoclue:x:987:
saned:x:986:
gdm:x:42:
gnome-initial-setup:x:985:
sshd:x:74:
avahi:x:70:
slocate:x:21:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
dalibaeva:x:1000:dalibaeva
vboxsf:x:984:
guest:x:1001:guest2
guest2:x:1002:
[guest2@dalibaeva dalibaeva]$ newgrp guest
[guest2@dalibaeva dalibaeva]$
```

Figure 4.9: Регистрация пользователя guest2 в группе guest

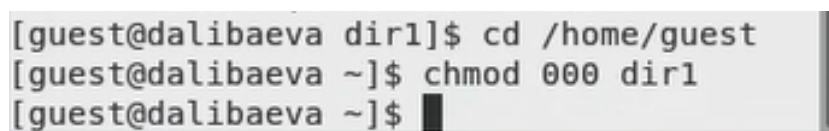
11. От имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rwX /home/guest` (рис. 4.10).

A terminal window titled 'guest@dalibaeva:/home/dalibaeva' with standard window controls. The menu bar includes 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal output lists system users and their IDs, followed by the user 'dalibaeva'. Then, it shows the user 'guest' and 'guest2'. Finally, it shows the command 'chmod g+rw /home/guest' being executed, changing the permissions of the directory /home/guest.

```
guest@dalibaeva:/home/dalibaeva
Файл  Правка  Вид  Поиск  Терминал  Справка
cgred:x:990:
setroubleshoot:x:989:
unbound:x:988:
tss:x:59:
usbmuxd:x:113:
geoclue:x:987:
saned:x:986:
gdm:x:42:
gnome-initial-setup:x:985:
sshd:x:74:
avahi:x:70:
slocate:x:21:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
dalibaeva:x:1000:dalibaeva
vboxsf:x:984:
guest:x:1001:guest2
guest2:x:1002:
[guest@dalibaeva dalibaeva]$ chmod g+rw
/home/guest
[guest@dalibaeva dalibaeva]$
```

Figure 4.10: Изменение прав директории

12. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` (рис. 4.11).

A terminal window showing the execution of two commands. First, the user changes the directory to /home/guest. Then, they run 'chmod 000 dir1' to remove all permissions from the directory /home/guest/dir1.

```
[guest@dalibaeva dir1]$ cd /home/guest
[guest@dalibaeva ~]$ chmod 000 dir1
[guest@dalibaeva ~]$
```

Figure 4.11: Изменение атрибутов

13. Заполнила таблицу «Установленные права и разрешённые действия для групп» (см. табл. 4.1), меняя атрибуты у директории `dir1` и файла `file1` от име-

ни пользователя guest и делая проверку от пользователя guest2, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

14. На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. 3.2. (см. табл. 4.2).

Table 4.1: Установленные права и разрешённые действия для групп

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d— (000)	— (000)	-	-	-	-	-	-	-	-
d— (000)	-x (010)	-	-	-	-	-	-	-	-
d— (000)	-w- (020)	-	-	-	-	-	-	-	-
d— (000)	-wx (030)	-	-	-	-	-	-	-	-
d— (000)	r— (040)	-	-	-	-	-	-	-	-
d— (000)	r-x (050)	-	-	-	-	-	-	-	-
d— (000)	rw- (060)	-	-	-	-	-	-	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d— (000)	rwX (070)	-	-	-	-	-	-	-	-
d-x (010)	— (000)	-	-	-	-	+	-	-	+
d-x (010)	-x (010)	-	-	-	-	+	-	-	+
d-x (010)	-w- (020)	-	-	+	-	+	-	-	+
d-x (010)	-wx (030)	-	-	+	-	+	-	-	+
d-x (010)	r— (040)	-	-	-	+	+	-	-	+
d-x (010)	r-x (050)	-	-	-	+	+	-	-	+
d-x (010)	rw- (060)	-	-	+	+	+	-	-	+
d-x (010)	rwX (070)	-	-	+	+	+	-	-	+
d-w- (020)	— (000)	-	-	-	-	-	-	-	-
d-w- (020)	-x (010)	-	-	-	-	-	-	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-w- (020)	-w- (020)	-	-	-	-	-	-	-	-
d-w- (020)	-wx (030)	-	-	-	-	-	-	-	-
d-w- (020)	r- (040)	-	-	-	-	-	-	-	-
d-w- (020)	r-x (050)	-	-	-	-	-	-	-	-
d-w- (020)	rw- (060)	-	-	-	-	-	-	-	-
d-w- (020)	rwX (070)	-	-	-	-	-	-	-	-
d-wX (030)	— (000)	+	+	-	-	+	-	+	+
d-wX (030)	-X (010)	+	+	-	-	+	-	+	+
d-wX (030)	-w- (020)	+	+	+	-	+	-	+	+
d-wX (030)	-wX (030)	+	+	+	-	+	-	+	+
d-wX (030)	r- (040)	+	+	-	+	+	-	+	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-wx (030)	r-x (050)	+	+	-	+	+	-	+	+
d-wx (030)	rw- (060)	+	+	+	+	+	-	+	+
d-wx (030)	rwX (070)	+	+	+	+	+	-	+	+
dr- (040)	— (000)	-	-	-	-	-	+	-	-
dr- (040)	-x (010)	-	-	-	-	-	+	-	-
dr- (040)	-w- (020)	-	-	-	-	-	+	-	-
dr- (040)	-wx (030)	-	-	-	-	-	+	-	-
dr- (040)	r- (040)	-	-	-	-	-	+	-	-
dr- (040)	r-x (050)	-	-	-	-	-	+	-	-
dr- (040)	rw- (060)	-	-	-	-	-	+	-	-
dr- (040)	rwX (070)	-	-	-	-	-	+	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
dr-x (050)	— (000)	-	-	-	-	+	+	-	+
dr-x (050)	-x (010)	-	-	-	-	+	+	-	+
dr-x (050)	-w- (020)	-	-	+	-	+	+	-	+
dr-x (050)	-wx (030)	-	-	+	-	+	+	-	+
dr-x (050)	r- (040)	-	-	-	+	+	+	-	+
dr-x (050)	r-x (050)	-	-	-	+	+	+	-	+
dr-x (050)	rw- (060)	-	-	+	+	+	+	-	+
dr-x (050)	rwX (070)	-	-	+	+	+	+	-	+
drw- (060)	— (000)	-	-	-	-	-	+	-	-
drw- (060)	-x (010)	-	-	-	-	-	+	-	-
drw- (060)	-w- (020)	-	-	-	-	-	+	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
drw- (060)	-wx (030)	-	-	-	-	-	+	-	-
drw- (060)	r- (040)	-	-	-	-	-	+	-	-
drw- (060)	r-x (050)	-	-	-	-	-	+	-	-
drw- (060)	rw- (060)	-	-	-	-	-	+	-	-
drw- (060)	rwX (070)	-	-	-	-	-	+	-	-
drwx (070)	— (000)	+	+	-	-	+	+	+	+
drwx (070)	-x (010)	+	+	-	-	+	+	+	+
drwx (070)	-w- (020)	+	+	+	-	+	+	+	+
drwx (070)	-wx (030)	+	+	+	-	+	+	+	+
drwx (070)	r- (040)	+	+	-	+	+	+	+	+
drwx (070)	r-x (050)	+	+	-	+	+	+	+	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
drwx (070)	rw- (060)	+	+	+	+	+	+	+	+
drwx (070)	rwX (070)	+	+	+	+	+	+	+	+

Table 4.2: Минимальные права для совершения операций от имени пользователя входящих в группу

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	(030)	(000)
Удаление файла	(030)	(000)
Чтение файла	(010)	(040)
Запись в файл	(010)	(020)
Переименование файла	(030)	(000)
Создание поддиректории	(030)	(000)
Удаление поддиректории	(030)	(000)

5 Выводы

Получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

6 Список литературы

1. Атрибуты файлов в Linux // URL: <https://itproffi.ru/atributy-fajlov-v-linux/>
(дата обращения: 01.10.2021).