

Лабораторная работа №3

Информационная безопасность

Леонтьева Ксения Андреевна | НПМбд-01-19

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Выводы	19
	Список литературы	20

Список иллюстраций

3.1	Создание пользователя и добавление его в группу	7
3.2	Проверка, в какие группы входят пользователи	8
3.3	Просмотр файла /etc/group	9
3.4	Изменение атрибутов	10

1 Цель работы

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

2 Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. 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 - невозможно 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

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

Команды, которые могут понадобиться при работе с правами доступа:

- “ls -l” - для просмотра прав доступа к файлам и каталогам
- “chmod категория действие флаг файл или каталог” - для изменения прав доступа к файлам и каталогам (категорию действие и флаг можно заменить на набор из трех цифр от 0 до 7)

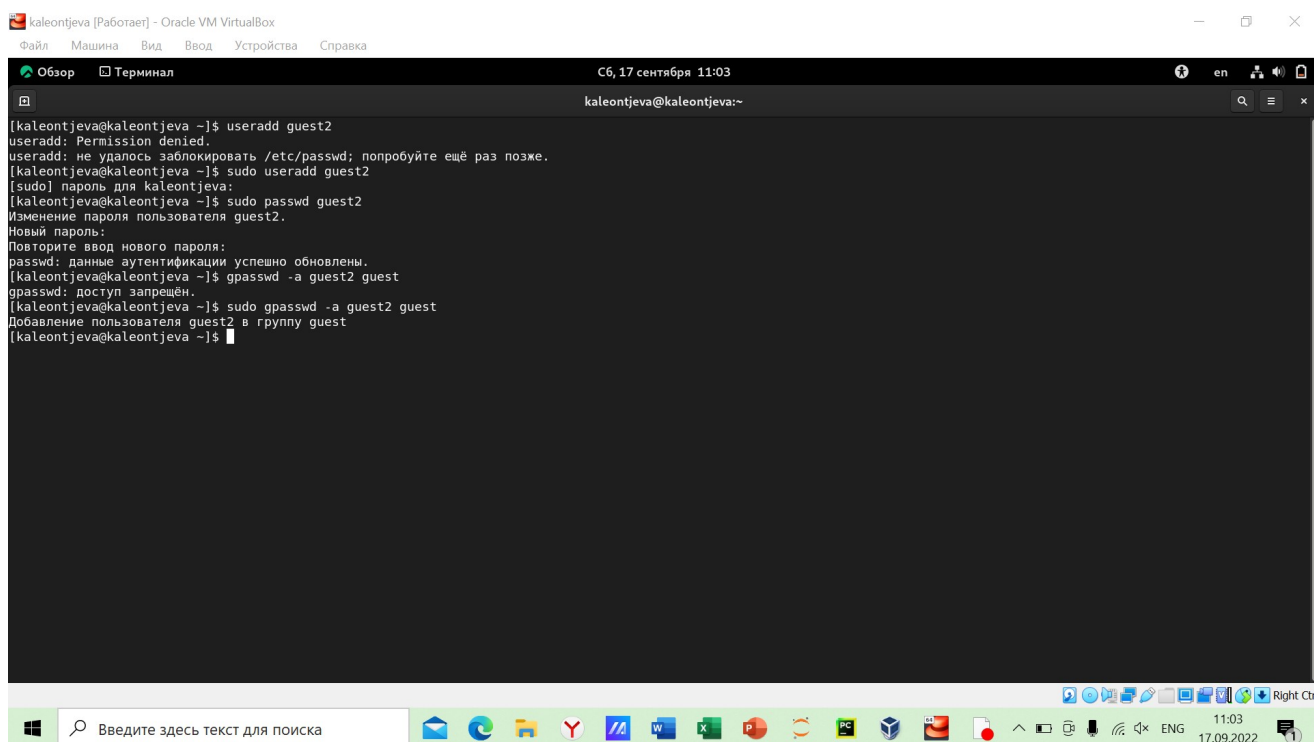
Значения флагов прав:

- — - нет никаких прав
- -x - разрешено только выполнение файла, как программы, но не изменение и не чтение
- -w- - разрешена только запись и изменение файла
- -wx - разрешено изменение и выполнение, но в случае с каталогом, невозможно посмотреть его содержимое
- r- - права только на чтение
- r-x - только чтение и выполнение, без права на запись
- rw- - права на чтение и запись, но без выполнения
- rwx - все права

Более подробно см. в [1]

3 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы ОС создана учётную запись пользователя guest2 (т.к. пользователь guest уже был создан в прошлой лабораторной работе) с помощью команды “sudo useradd guest2” и задала пароль для этого пользователя командой “sudo passwd guest2”. Добавила пользователя guest2 в группу guest с помощью команды “sudo gpasswd -a guest2 guest” (рис. 3.1).

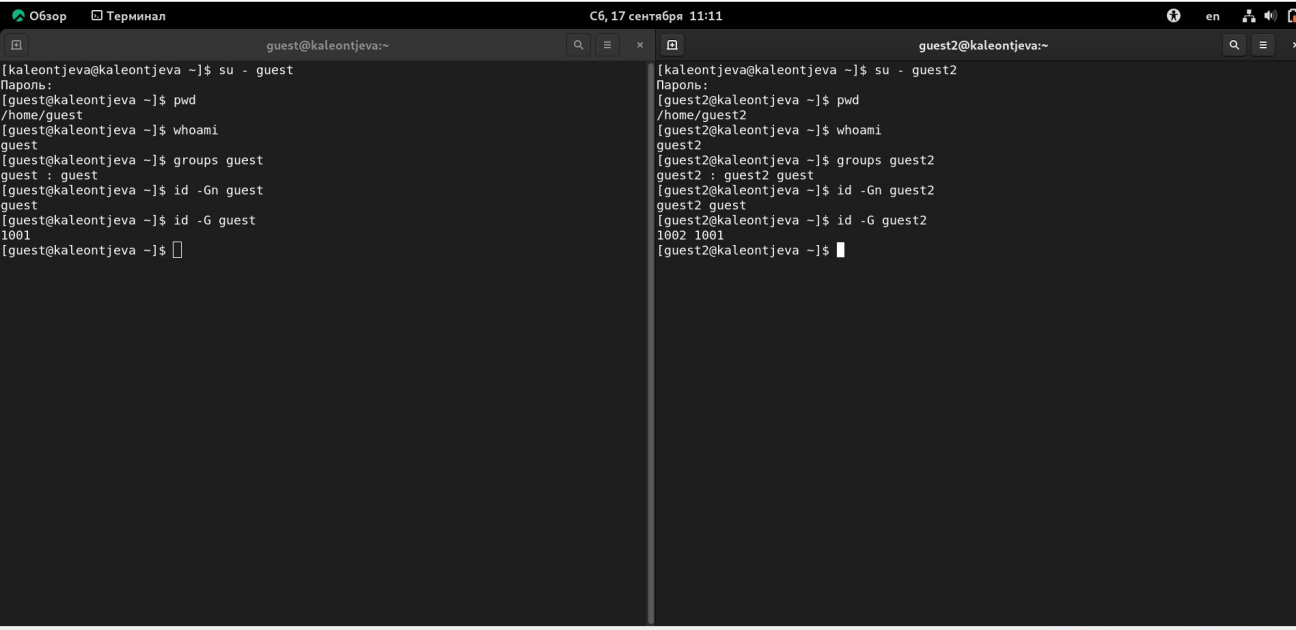


```
[kaleontjeva@kaleontjeva ~]$ useradd guest2
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[kaleontjeva@kaleontjeva ~]$ sudo useradd guest2
[sudo] пароль для kaleontjeva:
[kaleontjeva@kaleontjeva ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[kaleontjeva@kaleontjeva ~]$ gpasswd -a guest2 guest
gpasswd: доступ запрещён.
[kaleontjeva@kaleontjeva ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[kaleontjeva@kaleontjeva ~]$
```

Рис. 3.1: Создание пользователя и добавление его в группу

Затем осуществила вход в систему от двух пользователей на двух разных консо-

лях при помощи команд “su - guest” и “su - guest2”. Определила командой “pwd”, что оба пользователя находятся в своих домашних директориях, что совпадает с приглашениями командной строки. Уточнила имена пользователей командой “whoami”, соответственно получила: guest и guest2. С помощью команд “groups guest” и “groups guest2” определила, что пользователь guest входит в группу guest, а пользователь guest2 в группы guest и guest2. Сравнила полученную информацию с выводом команд “id -Gn guest”, “id -Gn guest2”, “id -G guest” и “id -G guest2”: данные совпали, за исключением второй команды “id -G”, которая вывела номера групп 1001 и 1002, что также является верным (рис. 3.2).

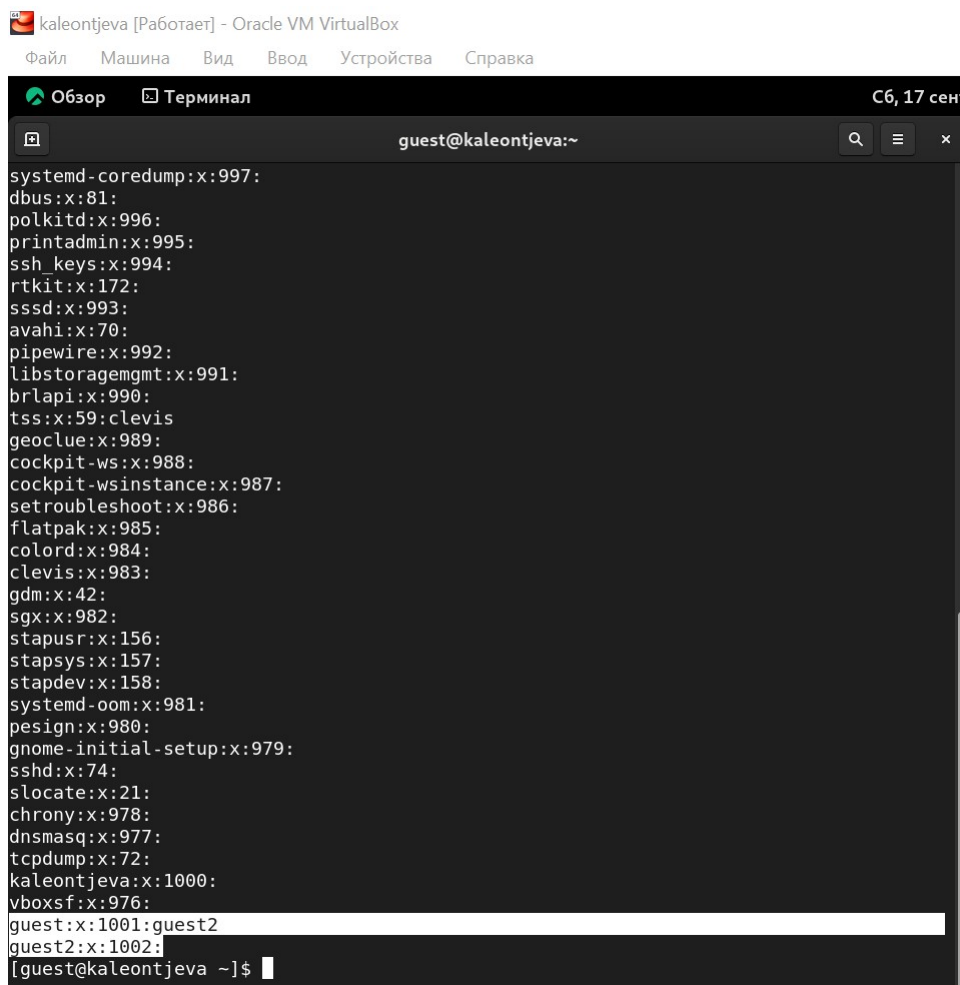


```
[kaleontjeva@kaleontjeva ~]$ su - guest
Пароль:
[guest@kaleontjeva ~]$ pwd
/home/guest
[guest@kaleontjeva ~]$ whoami
guest
[guest@kaleontjeva ~]$ groups guest
guest : guest
[guest@kaleontjeva ~]$ id -Gn guest
guest
[guest@kaleontjeva ~]$ id -G guest
1001
[guest@kaleontjeva ~]$

[kaleontjeva@kaleontjeva ~]$ su - guest2
Пароль:
[guest2@kaleontjeva ~]$ pwd
/home/guest2
[guest2@kaleontjeva ~]$ whoami
guest2
[guest2@kaleontjeva ~]$ groups guest2
guest2 : guest2 guest
[guest2@kaleontjeva ~]$ id -Gn guest2
guest2 guest
[guest2@kaleontjeva ~]$ id -G guest2
1002 1001
[guest2@kaleontjeva ~]$
```

Рис. 3.2: Проверка, в какие группы входят пользователи

Просмотрела файл /etc/group командой “cat /etc/group”, данные этого файла совпадают с полученными ранее (рис. 3.3).



The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar, there are tabs for "Обзор" and "Терминал". The terminal window shows the command prompt "guest@kaleontjeva:~" and the output of the command "cat /etc/group". The output lists various system users and their group memberships, including systemd-coredump, dbus, polkitd, printadmin, ssh_keys, rtkit, sssd, avahi, pipewire, libstoragemgmt, brlapi, tss, geoclue, cockpit-ws, cockpit-wsinstance, setroubleshoot, flatpak, colord, clemis, gdm, sgx, stapusr, stapys, stapdev, systemd-oom, pesign, gnome-initial-setup, sshd, slocate, chrony, dnsmasq, tcpdump, kaleontjeva, vboxsf, guest, and guest2. The terminal window also shows the command prompt "[guest@kaleontjeva ~]\$".

```
systemd-coredump:x:997:
dbus:x:81:
polkitd:x:996:
printadmin:x:995:
ssh_keys:x:994:
rtkit:x:172:
sssd:x:993:
avahi:x:70:
pipewire:x:992:
libstoragemgmt:x:991:
brlapi:x:990:
tss:x:59:clemis
geoclue:x:989:
cockpit-ws:x:988:
cockpit-wsinstance:x:987:
setroubleshoot:x:986:
flatpak:x:985:
colord:x:984:
clemis:x:983:
gdm:x:42:
sgx:x:982:
stapusr:x:156:
stapys:x:157:
stapdev:x:158:
systemd-oom:x:981:
pesign:x:980:
gnome-initial-setup:x:979:
sshd:x:74:
slocate:x:21:
chrony:x:978:
dnsmasq:x:977:
tcpdump:x:72:
kaleontjeva:x:1000:
vboxsf:x:976:
guest:x:1001:guest2
guest2:x:1002:
[guest@kaleontjeva ~]$
```

Рис. 3.3: Просмотр файла /etc/group

От имени пользователя guest2 зарегистрировала этого пользователя в группе guest командой “newgrp guest”. Далее от имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы командой “chmod g+rwX /home/guest”. От имени этого же пользователя сняла с директории /home/guest/dir1 все атрибуты командой “chmod 000 dir1” и проверила правильность снятия атрибутов командой “ls -l” (рис. 3.4).

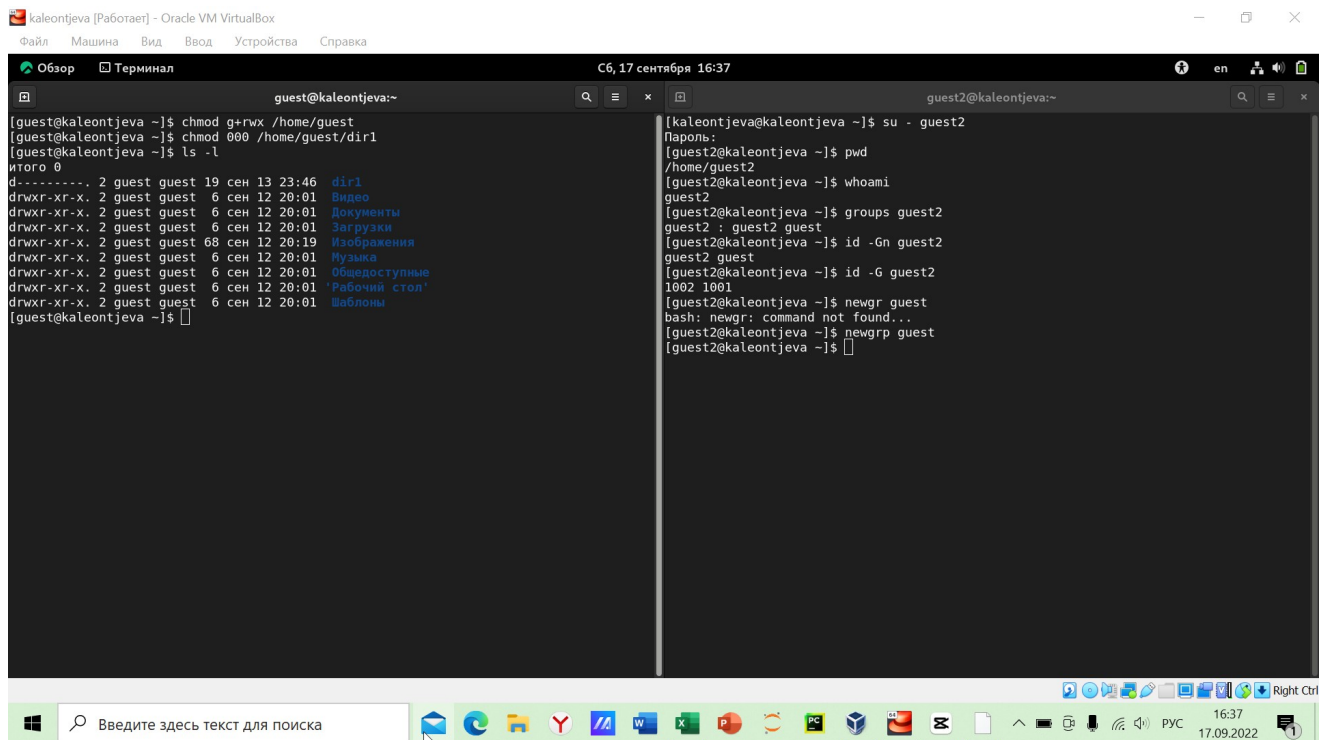


Рис. 3.4: Изменение атрибутов

Теперь заполним таблицу «Установленные права и разрешённые действия» 3.1, меняя атрибуты у директории и файла от имени пользователя guest и делая проверку от пользователя guest2.

Создание файла: “echo”text” > /home/guest/dir1/file2”

Удаление файла: “rm -r /home/guest/dir1/file1”

Запись в файл: “echo”textnew” > /home/guest/dir1/file1”

Чтение файла: “cat /home/guest/dir1/file1”

Смена директории: “cd /home/guest/dir1”

Просмотр файлов в директории: “ls /home/guest/dir1”

Переименование файла: “mv /home/guest/dir1/file1 filenew”

Смена атрибутов файла: “chattr -a /home/guest/dir1/file1”

Таблица 3.1: Установленные права и разрешённые действия

Права	Соз-	Уда-	на	Сме-					
				ди-	Просмотр	Пере-	Смена		
ди-	Пра-	да-	ле-	За-	Чте-	ди-	Просмотр	Пере-	Смена
рек-	ва	ние	ние	пись	ние	рек-	файлов в	имено-	атрибу-
то-	фай-	фай-	фай-	в	фай-	то-	директо-	вание	тов
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
d	(000)	-	-	-	-	-	-	-	-
(000)									
d -x	(000)	-	-	-	-	+	-	-	-
(010)									
d -w-	(000)	-	-	-	-	-	-	-	-
(020)									
d -wx	(000)	+	+	-	-	+	-	+	-
(030)									
d r-	(000)	-	-	-	-	-	+	-	-
(040)									
d r-x	(000)	-	-	-	-	+	+	-	-
(050)									
d rw-	(000)	-	-	-	-	-	+	-	-
(060)									
d rwx	(000)	+	+	-	-	+	+	+	-
(070)									

d	(010)	-	-	-	-	-	-	-	-
(000)									
d -x	(010)	-	-	-	-	+	-	-	-
(010)									

Сме-									
Права	Соз-	Уда-	на						
ди- рек- то- рии	Пра- ва фай- ла	да- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d -w- (020)	(010)	-	-	-	-	-	-	-	-
d -wx (030)	(010)	+	+	-	-	+	-	+	-
d r- (040)	(010)	-	-	-	-	-	+	-	-
d r-x (050)	(010)	-	-	-	-	+	+	-	-
d rw- (060)	(010)	-	-	-	-	-	+	-	-
d rwx (070)	(010)	+	+	-	-	+	+	+	-

d (000)	(020)	-	-	-	-	-	-	-	-
d -x (010)	(020)	-	-	+	-	+	-	-	-
d -w- (020)	(020)	-	-	-	-	-	-	-	-
d -wx (030)	(020)	+	+	+	-	+	-	+	-
d r- (040)	(020)	-	-	-	-	-	+	-	-

Сме-									
Права	Соз-	Уда-	на						
ди- рек- то- рии	Пра- ва фай- ла	да- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d r-x (050)	(020)	-	-	+	-	+	+	-	-
d rw- (060)	(020)	-	-	-	-	-	+	-	-
d rwx (070)	(020)	+	+	+	-	+	+	+	-

d (000)	(030)	-	-	-	-	-	-	-	-
d -x (010)	(030)	-	-	+	-	+	-	-	-
d -w- (020)	(030)	-	-	-	-	-	-	-	-
d -wx (030)	(030)	+	+	-	+	+	-	+	-
d r- (040)	(030)	-	-	-	-	-	+	-	-
d r-x (050)	(030)	-	-	+	-	+	+	-	-
d rw- (060)	(030)	-	-	-	-	-	+	-	-
d rwx (070)	(030)	+	+	+	-	+	+	+	-

Сме-									
Права	Соз-	Уда-	на						
ди- рек- то- рии	Пра- ва фай- ла	да- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла

d (000)	(040)	-	-	-	-	-	-	-	-
d -x (010)	(040)	-	-	-	+	+	-	-	-
d -w- (020)	(040)	-	-	-	-	-	-	-	-
d -wx (030)	(040)	+	+	-	+	+	-	+	-
d r- (040)	(040)	-	-	-	-	-	+	-	-
d r-x (050)	(040)	-	-	-	+	+	+	-	-
d rw- (060)	(040)	-	-	-	-	-	+	-	-
d rwx (070)	(040)	+	+	-	+	+	+	+	-

d (000)	(050)	-	-	-	-	-	-	-	-
d -x (010)	(050)	-	-	-	+	+	-	-	-

Сме-									
Права	Соз-	Уда-	на						
ди- рек- то- рии	Пра- ва фай- ла	да- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d -w- (020)	(050)	-	-	-	-	-	-	-	-
d -wx (030)	(050)	+	+	-	+	+	-	+	-
d r- (040)	(050)	-	-	-	-	-	+	-	-
d r-x (050)	(050)	-	-	-	+	+	+	-	-
d rw- (060)	(050)	-	-	-	-	-	+	-	-
d rwx (070)	(050)	+	+	-	+	+	+	+	-

d (000)	(060)	-	-	-	-	-	-	-	-
d -x (010)	(060)	-	-	+	+	+	-	-	-
d -w- (020)	(060)	-	-	-	-	-	-	-	-
d -wx (030)	(060)	+	+	+	+	+	-	+	-
d r- (040)	(060)	-	-	-	-	-	+	-	-

Сме-									
Права	Соз-	Уда-	на						
ди- рек- то- рии	Пра- ва фай- ла	да- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d r-x (050)	(060)	-	-	+	+	+	+	-	-
d rw- (060)	(060)	-	-	-	-	-	+	-	-
d rwx (070)	(060)	+	+	+	+	+	+	+	-
d (000)	(070)	-	-	-	-	-	-	-	-
d -x (010)	(070)	-	-	+	+	+	-	-	-
d -w- (020)	(070)	-	-	-	-	-	-	-	-
d -wx (030)	(070)	+	+	+	+	+	-	+	-
d r- (040)	(070)	-	-	-	-	-	+	-	-
d r-x (050)	(070)	-	-	+	+	+	+	-	-
d rw- (060)	(070)	-	-	-	-	-	+	-	-

Сме-									
Права	Соз-	Уда-	на						
ди-	Пра-	да-	ле-	За-	Чте-	ди-	Просмотр	Пере-	Смена
рек-	ва	ние	ние	пись	ние	рек-	файлов в	имено-	атрибу-
то-	фай-	фай-	фай-	в	фай-	то-	директо-	вание	тов
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
d rwx	(070)	+	+	+	+	+	+	+	-
(070)									

Сравнивая полученную таблицу с таблицей из прошлой лабораторной работы, приходим к выводу, что изменился только последний столбец, позволяющий изменять атрибуты у файла: теперь это сделать невозможно, т.к. у владельца файла и директории нет на это прав (во всех случаях в первой позиции стоят 0). При определенном наборе прав остальные действия выполняются или не выполняются аналогично предыдущей таблице, но теперь как для владельца, так и для группы.

Заполним таблицу «Минимально необходимые права для выполнения операций внутри директории» 3.2.

Таблица 3.2: Минимально необходимые права для выполнения операций внутри директории

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)	(040)
Запись в файл	d -x (010)	(020)
Переименование файла	d -wx (030)	(000)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание поддиректории	d -wx (030)	(000)
Удаление поддиректории	d -wx (030)	(000)

4 Выводы

В ходе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Права доступа к файлам в Linux [Электронный ресурс]. 2019. URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux>.