

# **Лабораторная работа №2**

**Информационная безопасность**

Леонтьева Ксения Андреевна | НПМбд-01-19

# Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Выводы	20
	Список литературы	21

## Список иллюстраций

3.1	Создание пользователя . . . . .	7
3.2	Вход в систему . . . . .	8
3.3	Вход в систему . . . . .	8
3.4	Команды pwd, whoami, id, groups, cat . . . . .	9
3.5	Содержание файла /etc/passwd . . . . .	10
3.6	Права доступа и расширенные атрибуты . . . . .	11
3.7	Попытка создать файл в директории . . . . .	12

# 1 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.

## 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)

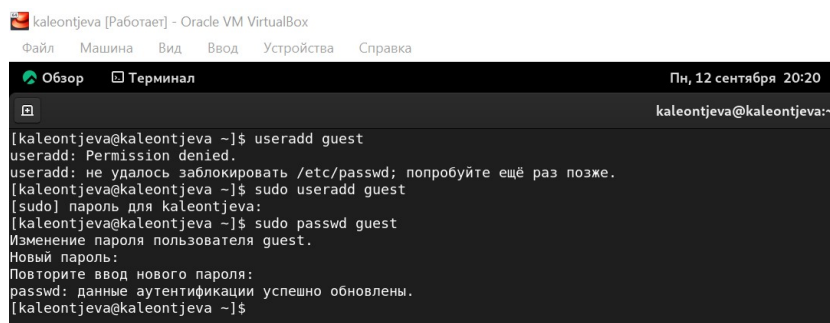
Значения флагов прав:

- — - 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 созда-  
ла учётную запись пользователя guest с помощью команды “sudo useradd guest”  
и задала пароль для этого пользователя командой “sudo passwd guest” (рис. 3.1).



```
kaleontjeva [Работае] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Пн, 12 сентября 20:20
kaleontjeva@kaleontjeva:~

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

Рис. 3.1: Создание пользователя

Вошла в систему от имени пользователя guest (рис. 3.2, 3.3).

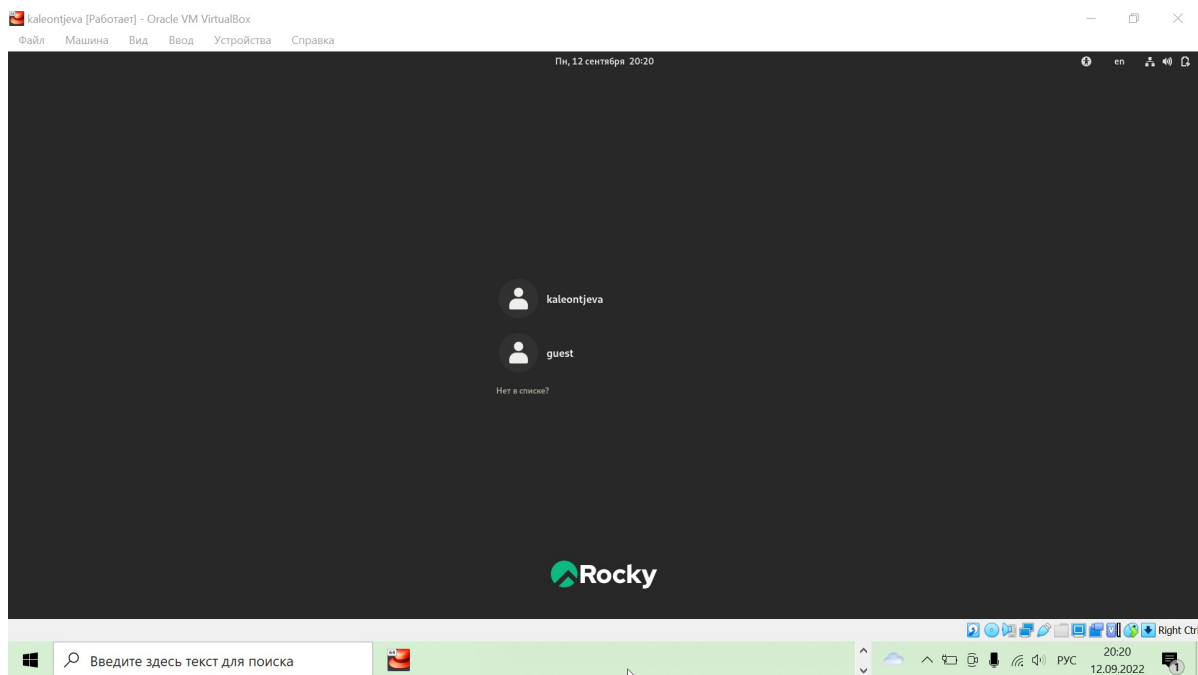


Рис. 3.2: Вход в систему

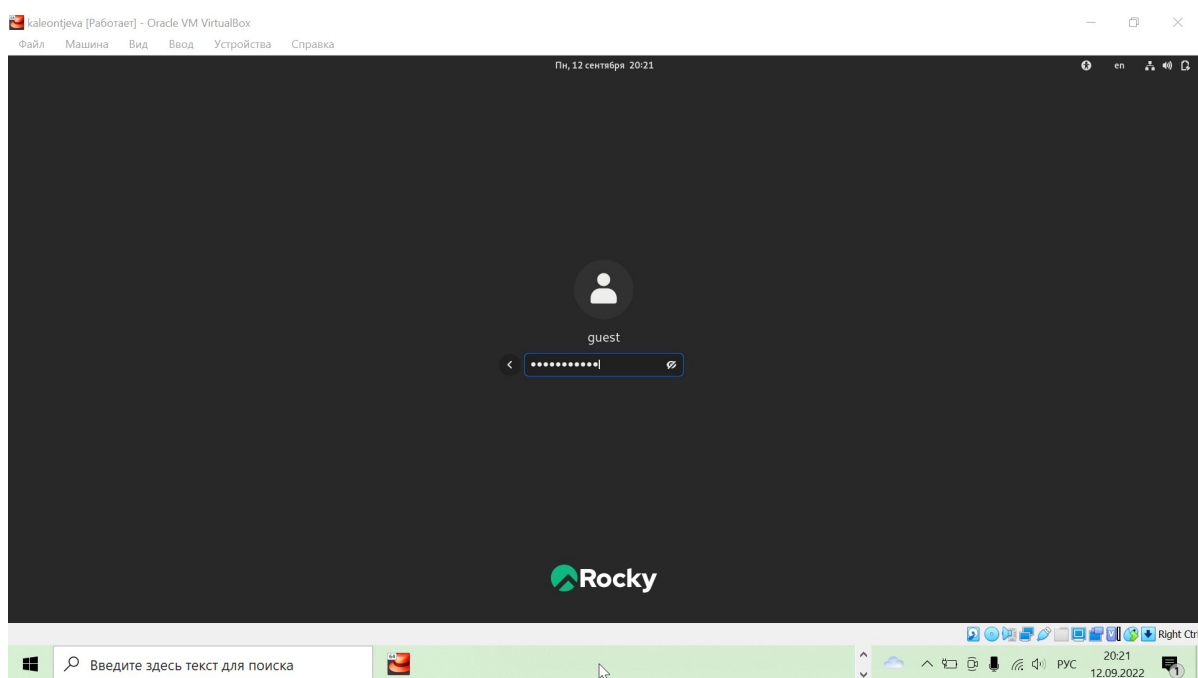


Рис. 3.3: Вход в систему

Командой “pwd” определила, что нахожусь в директории /home/guest, которая и является моей домашней директорией (рис. 3.4). С приглашением командной

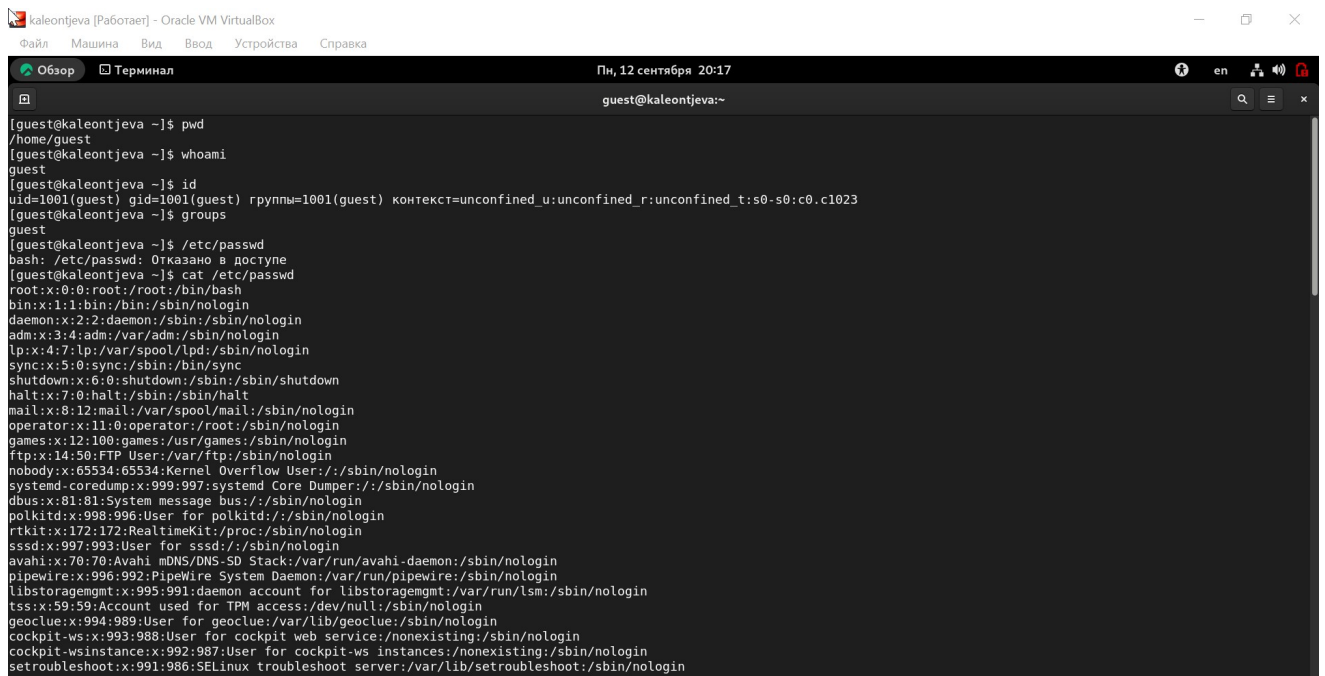


строки совпадает.

Уточнила имя моего пользователя командой “whoami” и получила вывод: guest (рис. 3.4).

С помощью команды “id” определила имя своего пользователя - всё так же guest, uid = 1001 (guest), gid = 1001 (guest). Затем сравнила полученную информацию с выводом команды “groups”, которая вывела “guest”. Мой пользователь входит только в одну группу, состоящую из него самого, поэтому вывод обеих команд “id” и “groups” совпадает (рис. 3.4). Данные, выводимые в приглашении командной строки, совпадают с полученной информацией.

Затем просмотрела файл /etc/passwd командой “cat /etc/passwd” (рис. 3.4).



```
guest@kaleontjeva ~]$ pwd
/home/guest
guest@kaleontjeva ~]$ whoami
guest
guest@kaleontjeva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
guest@kaleontjeva ~]$ groups
guest
guest@kaleontjeva ~]$ /etc/passwd
bash: /etc/passwd: Отказано в доступе
guest@kaleontjeva ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
firestorm:x:990:985:User for firestorm system:/sbin/nologin
```

Рис. 3.4: Команды pwd, whoami, id, groups, cat

Нашла в нём свою учётную запись в самом конце (рис. 3.5). Uid = 1001, gid = 1001, то есть они совпадают с тем, что мы получили ранее.

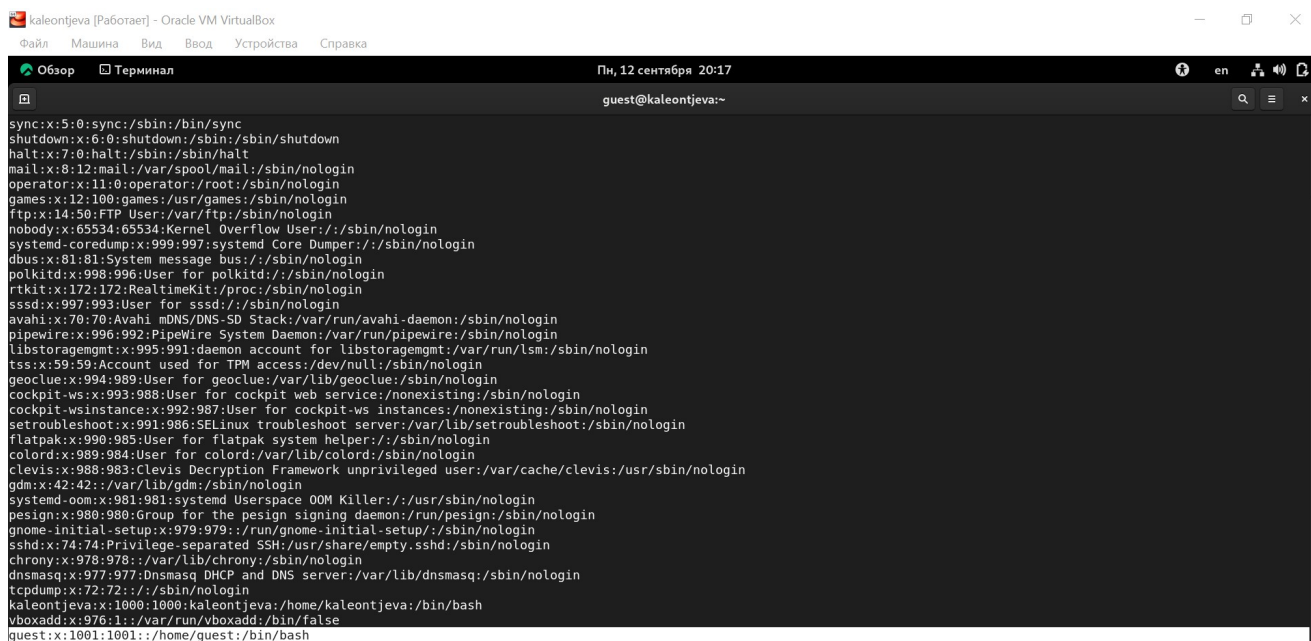


Рис. 3.5: Содержание файла /etc/passwd

Посмотрела, какие директории существуют в системе командой “ls -l /home/” (рис. 3.6). Список поддиректорий директории /home получить удалось. На директориях установлены права чтения, записи и выполнения для самого пользователя (для группы и остальных пользователей никаких прав доступа не установлено).

Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой “lsattr /home” (рис. 3.6). Удалось увидеть расширенные атрибуты только директории того пользователя, от имени которого я нахожусь в системе.

Создала в домашней директории поддиректорию dir1 командой “mkdir dir1” и определила, какие права доступа и расширенные атрибуты были на неё выставлены: чтение, запись и выполнение доступны для самого пользователя и для группы, для остальных - только чтение и выполнение, расширенных атрибутов не установлено (рис. 3.6).

```
kaleontjeva [Работаю] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Пн, 12 сентября 20:18
guest@kaleontjeva:~
[guest@kaleontjeva ~]$ ls -l /home/
итого 8
drwx----- 14 guest      guest      4096 сен 12 20:02 guest
drwx----- 27 kaleontjeva kaleontjeva 4096 сен 12 19:59 kaleontjeva
[guest@kaleontjeva ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/kaleontjeva
----- /home/guest
[guest@kaleontjeva ~]$ mkdir dir1
[guest@kaleontjeva ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 12 20:11 dir1
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Видео
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Документы
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Изображения
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Музыка
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 12 20:01 Шаблоны
[guest@kaleontjeva ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Рис. 3.6: Права доступа и расширенные атрибуты

Сняла с директории `dir1` все атрибуты командой `“chmod 000 dir1”` и проверила с её помощью правильность выполнения команды `“ls -l”`. Действительно, все атрибуты были сняты (рис. 3.7).

Попыталась создать в директории `dir1` файл `file1` командой `echo “test” > /home/guest/dir1/file1` (рис. 3.7). Этого сделать не получилось, т.к. предыдущим действием мы убрали право доступа на запись в директории. В итоге файл не был создан (открыть директорию с помощью команды `“ls -l /home/guest/dir1”` изначально тоже не удалось по той же причине, поэтому я поменяла права доступа и снова воспользовалась этой командой, и тогда смогла просмотреть содержимое директории, убедившись, что файл не был создан).

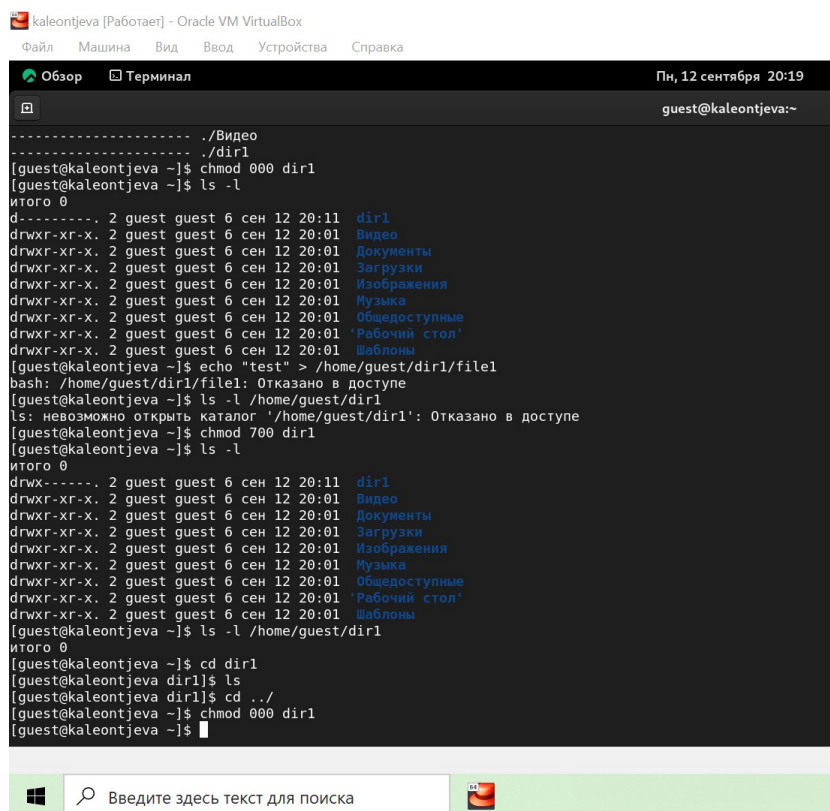


Рис. 3.7: Попытка создать файл в директории

Заполним таблицу «Установленные права и разрешённые действия» 3.1.

Таблица 3.1: Установленные права и разрешённые действия

		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	(000)	-	-	-	-	-	-	-	-
(000)									
d -x	(000)	-	-	-	-	+	-	-	-
(100)									

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- (200)	(000)	-	-	-	-	-	-	-	-
d -wx (300)	(000)	+	+	-	-	+	-	+	-
d r- (400)	(000)	-	-	-	-	-	+	-	-
d r-x (500)	(000)	-	-	-	-	+	+	-	-
d rw- (600)	(000)	-	-	-	-	-	+	-	-
d rwx (700)	(000)	+	+	-	-	+	+	+	-
<hr/>									
d (000)	(100)	-	-	-	-	-	-	-	-
d -x (100)	(100)	-	-	-	-	+	-	-	-
d -w- (200)	(100)	-	-	-	-	-	-	-	-
d -wx (300)	(100)	+	+	-	-	+	-	+	-
d r- (400)	(100)	-	-	-	-	-	+	-	-

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 (500)	(100)	-	-	-	-	+	+	-	-
d rw- (600)	(100)	-	-	-	-	-	+	-	-
d rwx (700)	(100)	+	+	-	-	+	+	+	-
-----									
d (000)	(200)	-	-	-	-	-	-	-	-
d -x (100)	(200)	-	-	+	-	+	-	-	-
d -w- (200)	(200)	-	-	-	-	-	-	-	-
d -wx (300)	(200)	+	+	+	-	+	-	+	-
d r- (400)	(200)	-	-	-	-	-	+	-	-
d r-x (500)	(200)	-	-	+	-	+	+	-	-
d rw- (600)	(200)	-	-	-	-	-	+	-	-
d rwx (700)	(200)	+	+	+	-	+	+	+	-

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)	(300)	-	-	-	-	-	-	-	-
d -x (100)	(300)	-	-	+	-	+	-	-	-
d -w- (200)	(300)	-	-	-	-	-	-	-	-
d -wx (300)	(300)	+	+	-	+	+	-	+	-
d r- (400)	(300)	-	-	-	-	-	+	-	-
d r-x (500)	(300)	-	-	+	-	+	+	-	-
d rw- (600)	(300)	-	-	-	-	-	+	-	-
d rwx (700)	(300)	+	+	+	-	+	+	+	-
d (000)	(400)	-	-	-	-	-	-	-	-
d -x (100)	(400)	-	-	-	+	+	-	-	+

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- (200)	(400)	-	-	-	-	-	-	-	-
d -wx (300)	(400)	+	+	-	+	+	-	+	+
d r- (400)	(400)	-	-	-	-	-	+	-	-
d r-x (500)	(400)	-	-	-	+	+	+	-	+
d rw- (600)	(400)	-	-	-	-	-	+	-	-
d rwx (700)	(400)	+	+	-	+	+	+	+	+
<hr/>									
d (000)	(500)	-	-	-	-	-	-	-	-
d -x (100)	(500)	-	-	-	+	+	-	-	+
d -w- (200)	(500)	-	-	-	-	-	-	-	-
d -wx (300)	(500)	+	+	-	+	+	-	+	+
d r- (400)	(500)	-	-	-	-	-	+	-	-



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 (500)	(500)	-	-	-	+	+	+	-	+
d rw- (600)	(500)	-	-	-	-	-	+	-	-
d rwx (700)	(500)	+	+	-	+	+	+	+	+
-----									
d (000)	(600)	-	-	-	-	-	-	-	-
d -x (100)	(600)	-	-	+	+	+	-	-	+
d -w- (200)	(600)	-	-	-	-	-	-	-	-
d -wx (300)	(600)	+	+	+	+	+	-	+	+
d r- (400)	(600)	-	-	-	-	-	+	-	-
d r-x (500)	(600)	-	-	+	+	+	+	-	+
d rw- (600)	(600)	-	-	-	-	-	+	-	-
d rwx (700)	(600)	+	+	+	+	+	+	+	+

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)	(700)	-	-	-	-	-	-	-	-
d -x (100)	(700)	-	-	+	+	+	-	-	+
d -w- (200)	(700)	-	-	-	-	-	-	-	-
d -wx (300)	(700)	+	+	+	+	+	-	+	+
d r- (400)	(700)	-	-	-	-	-	+	-	-
d r-x (500)	(700)	-	-	+	+	+	+	-	+
d rw- (600)	(700)	-	-	-	-	-	+	-	-
d rwx (700)	(700)	+	+	+	+	+	+	+	+

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 (300)	(000)
Удаление файла	d -wx (300)	(000)
Чтение файла	d -x (100)	(400)
Запись в файл	d -x (100)	(200)
Переименование файла	d -wx (300)	(000)
Создание поддиректории	d -wx (300)	(000)
Удаление поддиректории	d -wx (300)	(000)

## 4 Выводы

В ходе выполнения данной лабораторной работы я приобрела практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

## Список литературы

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