

# **Лабораторная работа № 2**

**Дискреционное разграничение прав в Linux. Основные атрибуты**

Усов Александр Александрович НБибд-02-18

# Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	22
	Список литературы	23

## Список иллюстраций

4.1	создал учётную запись пользователя guest . . . . .	9
4.2	Задал пароль для пользователя guest . . . . .	10
4.3	Вошел в систему . . . . .	10
4.4	Определил директорию . . . . .	11
4.5	Уточнил имя пользователя . . . . .	11
4.6	Уточнил имя пользователя, его группу, а также группы, куда входит пользователь . . . . .	12
4.7	Сравнение . . . . .	12
4.8	Просмотрел файл . . . . .	12
4.9	Просмотрел файл . . . . .	13
4.10	cat /etc/passwd   grep guest . . . . .	13
4.11	Определил существующие в системе директории . . . . .	14
4.12	Проверил, какие расширенные атрибуты установлены на поддиректориях . . . . .	14
4.13	создайте в домашней директории поддиректорию . . . . .	14
4.14	Определите командами ls -l и lsattr, какие права доступа . . . . .	15
4.15	Снял с директории dir1 все атрибуты . . . . .	15
4.16	Попытался создать в директории dir1 файл file1 . . . . .	15

## Список таблиц

4.1	Установленные права и разрешённые действия 1/4 . . . . .	17
4.2	Установленные права и разрешённые действия 2/4 . . . . .	18
4.3	Установленные права и разрешённые действия 3/4 . . . . .	19
4.4	Установленные права и разрешённые действия 4/4 . . . . .	20
4.5	Минимальные права для совершения операций . . . . .	21

# 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 Задание

1. Добавить пользователя guest
2. Создать пароль для пользователя guest
3. Опытным путём заполнить таблицу “Установленные права и разрешённые действия”
4. 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.

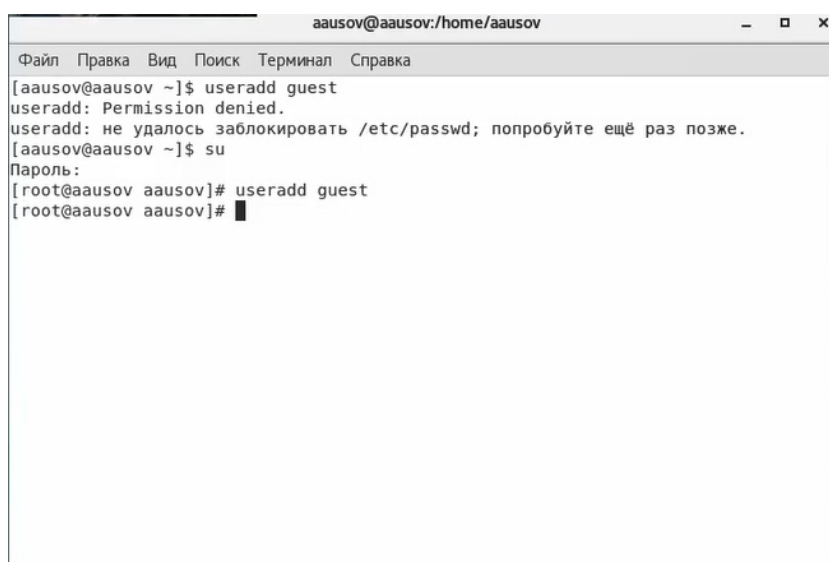
Но со временем такой системы стало не хватать и было добавлено еще несколько флагов, которые позволяют делать файлы не изменяемыми или же выполнять от имени суперпользователя

Более подробно о правах см. в [1].



## 4 Выполнение лабораторной работы

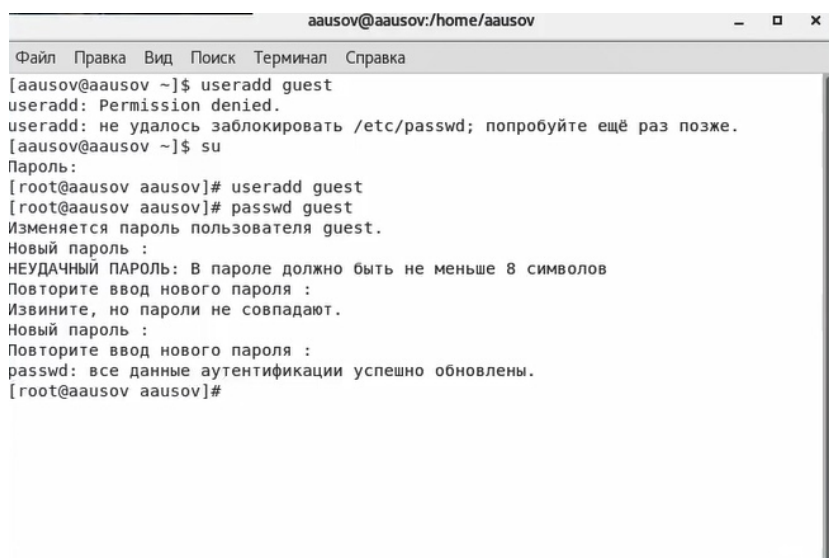
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (используя учётную запись администратора)(рис. 4.1): `useradd guest`



```
aausov@aausov: /home/aausov
Файл Правка Вид Поиск Терминал Справка
[aausov@aausov ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[aausov@aausov ~]$ su
Пароль:
[root@aausov aausov]# useradd guest
[root@aausov aausov]#
```

Рис. 4.1: создал учётную запись пользователя guest

2. Задал пароль для пользователя guest (используя учётную запись администратора) (рис. 4.2): `passwd guest`



```
aausov@aausov:/home/aausov
Файл Правка Вид Поиск Терминал Справка
[aausov@aausov ~]$ useradd guest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[aausov@aausov ~]$ su
Пароль:
[root@aausov aausov]# useradd guest
[root@aausov aausov]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@aausov aausov]#
```

Рис. 4.2: Задал пароль для пользователя guest

3. Вошел в систему от имени пользователя guest (рис. 4.3).

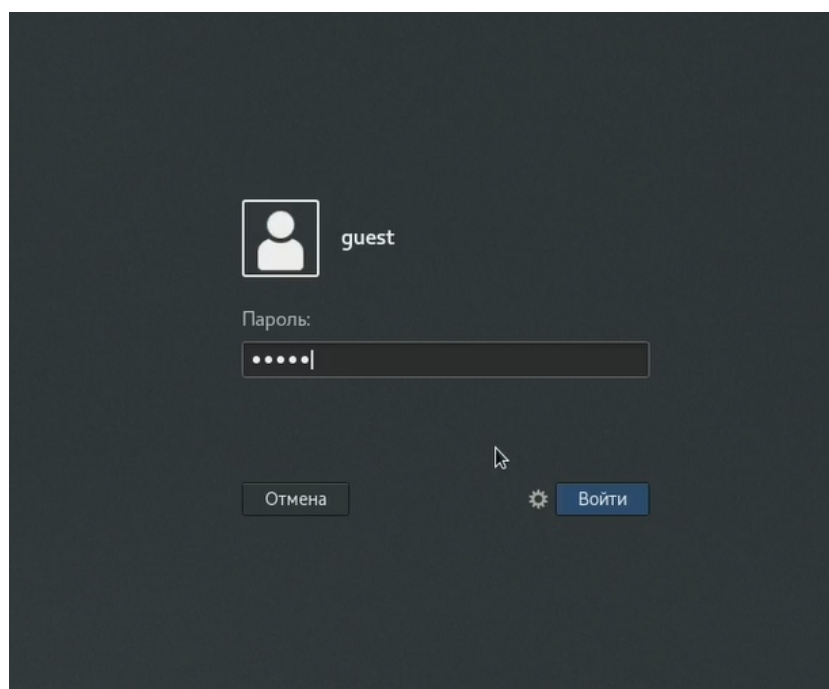
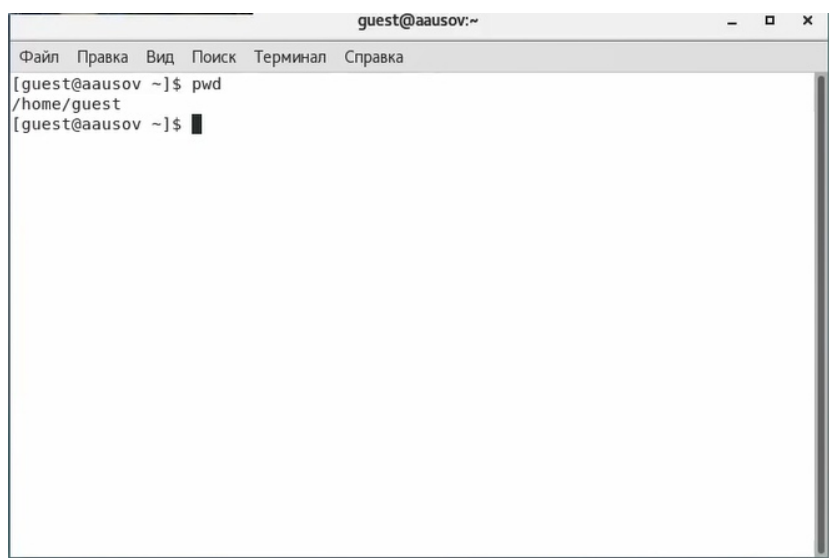


Рис. 4.3: Вошел в систему

4. Определил директорию, в которой находился, командой pwd (рис. 4.4).

Данная строка является домашней директорией для данного пользователя.



```
guest@aausov:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@aausov ~]$ pwd  
/home/guest  
[guest@aausov ~]$
```

Рис. 4.4: Определил директорию

5. Уточнил имя пользователя командой whoami (рис. 4.5).



```
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@aausov ~]$ pwd  
/home/guest  
[guest@aausov ~]$ cd /home/guest  
[guest@aausov ~]$ whoami  
guest
```

Рис. 4.5: Уточнил имя пользователя

6. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой id. Сравните вывод id с выводом команды groups (рис. 4.6) и (рис. 4.7).

```

guest
[guest@aausov ~]$ id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest)
[guest@aausov ~]$ groups guest
guest : guest
[guest@aausov ~]$ █

```

Рис. 4.6: Уточнил имя пользователя, его группу, а также группы, куда входит пользователь

7. Сравнил полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.

```

[guest@aausov ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@aausov ~]$ groups
guest
-

```

Рис. 4.7: Сравнение

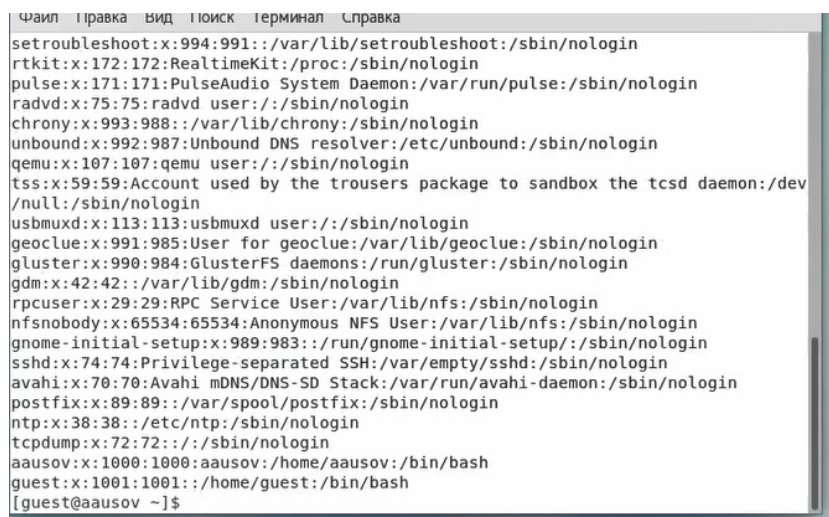
8. Просмотрел файл /etc/passwd командой cat /etc/passwd (рис. 4.8) и (рис. 4.9)

```

cat: /etc/passwd: Нет такого файла или каталога
[guest@aausov ~]$ cat /etc/passwd

```

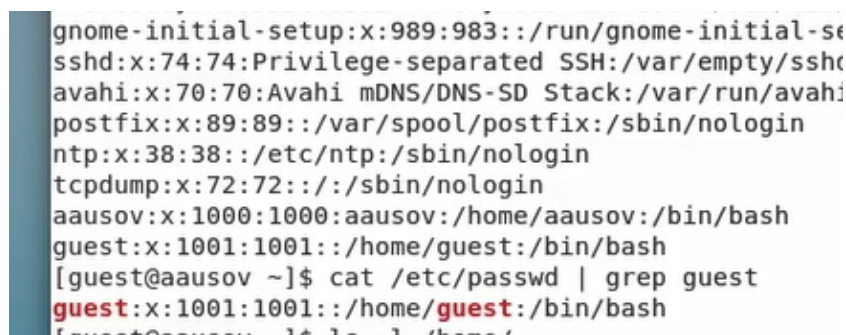
Рис. 4.8: Просмотрел файл



```
Файл  Правка  Вид  Поиск  Терминал  Справка
setroubleshoot:x:994:991::/var/lib/setroubleshoot:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
chrony:x:993:988::/var/lib/chrony:/sbin/nologin
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev
/null:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gnome-initial-setup:x:989:983::/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
aausov:x:1000:1000:aausov:/home/aausov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@aausov ~]$
```

Рис. 4.9: Просмотрел файл

Замечание: в случае, когда вывод команды не уместается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу shift, нажимайте page up и page down) либо программу грер в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания (рис. 4.10): `cat /etc/passwd | grep guest`



```
gnome-initial-setup:x:989:983::/run/gnome-initial-se
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
aausov:x:1000:1000:aausov:/home/aausov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@aausov ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@aausov ~]$
```

Рис. 4.10: `cat /etc/passwd | grep guest`

Сравнил данные, полученные в пункте 6 и в пункте 8.

При сравнении мы видим, что данные равны

9. Определил существующие в системе директории командой `ls -l /home/` (рис. 4.11)

```
guest@aausov: /home/guest$ ls -l /home/
итого 8
drwx-----, 15 aausov aausov 4096 сен 27 12:44 aausov
drwx-----, 15 guest guest 4096 сен 27 12:58 guest
[guest@aausov ~]$
```

Рис. 4.11: Определил существующие в системе директории

Список получен. Для каждого объекта файловой системы в модели полномочий Linux есть три типа полномочий: полномочия чтения (r от read), записи (w от write) и выполнения (x от execution). В полномочия записи входят также возможности удаления и изменения объекта.

На тех директориях, что находятся в home для владельцев предоставлен полный доступ.

10. Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home (рис. 4.12)

```
drwx-----, 15 guest guest 4096 сен 27 12:58 guest
[guest@aausov ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/aausov
----- /home/guest
[guest@aausov ~]$
```

Рис. 4.12: Проверил, какие расширенные атрибуты установлены на поддиректориях

11. Создал в домашней директории поддиректорию dir1 командой mkdir dir1  
Определил командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1. (рис. 4.13) и (рис. 4.14)

```
----- /home/guest
[guest@aausov ~]$ mkdir dir1
[guest@aausov ~]$ ls -l
ls: невозможно получить доступ к -: Нет такого файла или каталога
ls: невозможно получить доступ к l: Нет такого файла или каталога
[guest@aausov ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 27 13:06 dir1
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@aausov ~]$
```

Рис. 4.13: оздайте в домашней директории поддиректорию

```
[guest@aausov ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Рис. 4.14: Определите командами `ls -l` и `lsattr`, какие права доступа

12. Снял с директории `dir1` все атрибуты командой `chmod 000 dir1` (рис. 4.15) и проверил с её помощью правильность выполнения команды `ls -l` (рис. 4.15)

```
[guest@aausov ~]$ chmod 000 dir1
[guest@aausov ~]$ ls -l
итого 0
d----- 2 guest guest 6 сен 27 13:06 dir1
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@aausov ~]$
```

Рис. 4.15: Снял с директории `dir1` все атрибуты

13. Попытался создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` (рис. 4.16)

```
[guest@aausov ~]$ chmod 000 dir1
[guest@aausov ~]$ ls -l
итого 0
d----- 2 guest guest 6 сен 27 13:06 dir1
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@aausov ~]$
```

Рис. 4.16: Попытался создать в директории `dir1` файл `file1`

Недостаточно прав для создания файла в этой директории, поэтому выходит ошибка. Ещё нельзя проверить что внутри, т.к. у текущего пользователя на это тоже нет прав.

14. Заполнил таблицу «Установленные права и разрешённые действия»

15. На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1



Таблица 4.1: Установленные права и разрешённые действия 1/4

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переим. файла	Смена атрибутов файл
d---(000)	---(000)	-	-	-	-	-	-	-	-
d-x--(100)	---(000)	-	-	-	-	+	-	-	+
d-w--(200)	---(000)	-	-	-	-	-	-	-	-
d-wx--(300)	---(000)	+	+	-	-	+	-	+	+
dr---(400)	---(000)	-	-	-	-	-	+	-	-
dr-x--(500)	---(000)	-	-	-	-	+	+	-	+
drw--(600)	---(000)	-	-	-	-	-	+	-	-
drwx--(700)	---(000)	+	+	-	-	+	+	+	+
d---(000)	-x---(100)	-	-	-	-	-	-	-	-
d-x--(100)	-x---(100)	-	-	-	-	+	-	-	+
d-w--(200)	-x---(100)	-	-	-	-	-	-	-	-
d-wx--(300)	-x---(100)	+	+	-	-	+	-	+	+
dr---(400)	-x---(100)	-	-	-	-	-	+	-	-
dr-x--(500)	-x---(100)	-	-	-	-	+	+	-	+
drw--(600)	-x---(100)	-	-	-	-	-	+	-	-
drwx--(700)	-x---(100)	+	+	-	-	+	+	+	+

Таблица 4.2: Установленные права и разрешённые действия 2/4

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переим. файла	Смена атрибутов файл
d---(000)	-W---(200)	-	-	-	-	-	-	-	-
d-x--(100)	-W---(200)	-	-	+	-	+	-	-	+
d-w---(200)	-W---(200)	-	-	-	-	-	-	-	-
d-wx--(300)	-W---(200)	+	+	+	-	+	-	+	+
dr---(400)	-W---(200)	-	-	-	-	-	+	-	-
dr-x--(500)	-W---(200)	-	-	+	-	+	+	-	+
drw---(600)	-W---(200)	-	-	-	-	-	+	-	-
drwx--(700)	-W---(200)	+	+	+	-	+	+	+	+
d---(000)	-wx---(300)	-	-	-	-	-	-	-	-
d-x--(100)	-wx---(300)	-	-	+	-	+	-	-	+
d-w---(200)	-wx---(300)	-	-	-	-	-	-	-	-
d-wx--(300)	-wx---(300)	+	+	+	-	+	-	+	+
dr---(400)	-wx---(300)	-	-	-	-	-	+	-	-
dr-x--(500)	-wx---(300)	-	-	+	-	+	+	-	+
drw---(600)	-wx---(300)	-	-	-	-	-	+	-	-
drwx--(700)	-wx---(300)	+	+	+	-	+	+	+	+

Таблица 4.3: Установленные права и разрешённые действия 3/4

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переим. файла	Смена атрибутов файл
d---(000)	r---(400)	-	-	-	-	-	-	-	-
d-x--(100)	r---(400)	-	-	-	+	+	-	-	+
d-w--(200)	r---(400)	-	-	-	-	-	-	-	-
d-wx--(300)	r---(400)	+	+	-	+	+	-	+	+
dr---(400)	r---(400)	-	-	-	-	-	+	-	-
dr-x--(500)	r---(400)	-	-	-	+	+	+	-	+
drw--(600)	r---(400)	-	-	-	-	-	+	-	-
drwx--(700)	r---(400)	+	+	-	+	+	+	+	+
d---(000)	r-x---(500)	-	-	-	-	-	-	-	-
d-x--(100)	r-x---(500)	-	-	-	+	+	-	-	+
d-w--(200)	r-x---(500)	-	-	-	-	-	-	-	-
d-wx--(300)	r-x---(500)	+	+	-	+	+	-	+	+
dr---(400)	r-x---(500)	-	-	-	-	-	+	-	-
dr-x--(500)	r-x---(500)	-	-	-	+	+	+	-	+
drw--(600)	r-x---(500)	-	-	-	-	-	+	-	-
drwx--(700)	r-x---(500)	+	+	-	+	+	+	+	+

Таблица 4.4: Установленные права и разрешённые действия 4/4

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переим. файла	Смена атрибутов файл
d---(000)	rw---(600)	-	-	-	-	-	-	-	-
d-x--(100)	rw---(600)	-	-	+	+	+	-	-	+
d-w--(200)	rw---(600)	-	-	-	-	-	-	-	-
d-wx--(300)	rw---(600)	+	+	+	+	+	-	+	+
dr---(400)	rw---(600)	-	-	-	-	-	+	-	-
dr-x--(500)	rw---(600)	-	-	+	+	+	+	-	+
drw--(600)	rw---(600)	-	-	-	-	-	+	-	-
drwx--(700)	rw---(600)	+	+	+	+	+	+	+	+
d---(000)	rwx---(700)	-	-	-	-	-	-	-	-
d-x--(100)	rwx---(700)	-	-	+	+	+	-	-	+
d-w--(200)	rwx---(700)	-	-	-	-	-	-	-	-
d-wx--(300)	rwx---(700)	+	+	+	+	+	-	+	+
dr---(400)	rwx---(700)	-	-	-	-	-	+	-	-
dr-x--(500)	rwx---(700)	-	-	+	+	+	+	-	+
drw--(600)	rwx---(700)	-	-	-	-	-	+	-	-
drwx--(700)	rwx---(700)	+	+	+	+	+	+	+	+

Таблица 4.5: Минимальные права для совершения операций

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

## 5 Выводы

Выполняя данную лабораторную работу, я получил практические навыки работы в консоли с атрибутами файлов, закрепил 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]. Сайт, 2021.  
URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux>.