

# **Отчет по лабораторной работе №2**

-

Овениязов Артур

# 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>8</b>
<b>5</b>	<b>Выводы</b>	<b>26</b>
	<b>Список литературы</b>	<b>27</b>

## Список иллюстраций

4.1	Создание учетной записи . . . . .	8
4.2	Вход в систему . . . . .	9
4.3	Результат pwd . . . . .	10
4.4	Результат whoami . . . . .	10
4.5	Результат id и groups . . . . .	11
4.6	Результат /etc/passwd   grep guest . . . . .	11
4.7	Результат ls -l и lsattr /home/ . . . . .	12
4.8	Результат mkdir dir1, ls -l и lsattr . . . . .	12
4.9	Результат chmod 000 dir1 и ls -l . . . . .	12
4.10	Результат echo "test" > /home/guest/dir1/file1 . . . . .	13

## Список таблиц

4.1	Установленные права и разрешённые действия . . . . .	13
4.2	Минимально необходимые права для выполнения операций . . .	24

# 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

Лабораторная работа подразумевает практическое исследование дискреционных разграничений в современных системах с открытым кодом на базе ОС Linux

## 3 Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов. Один из подходов к разграничению доступа — так называемый дискреционный (от англ, discretion — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют. Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. [1]

## 4 Выполнение лабораторной работы

Создал учетную запись guest и задал ей пароль

```
[root@aoveniyazov aoveniyazov]# useradd guest
[root@aoveniyazov aoveniyazov]# guest
bash: guest: команда не найдена...
[root@aoveniyazov aoveniyazov]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Рис. 4.1: Создание учетной записи

Выполнил вход в систему от имени пользователя guest



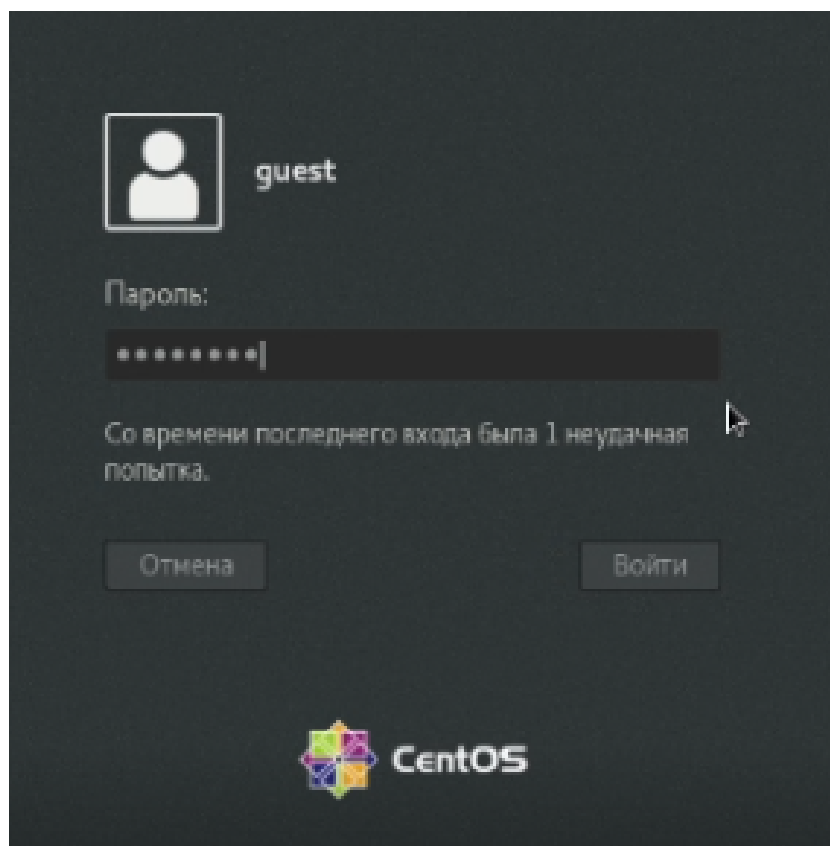


Рис. 4.2: Вход в систему

Определил директорию где я нахожусь командой `pwd`. Нахожусь в домашней директории

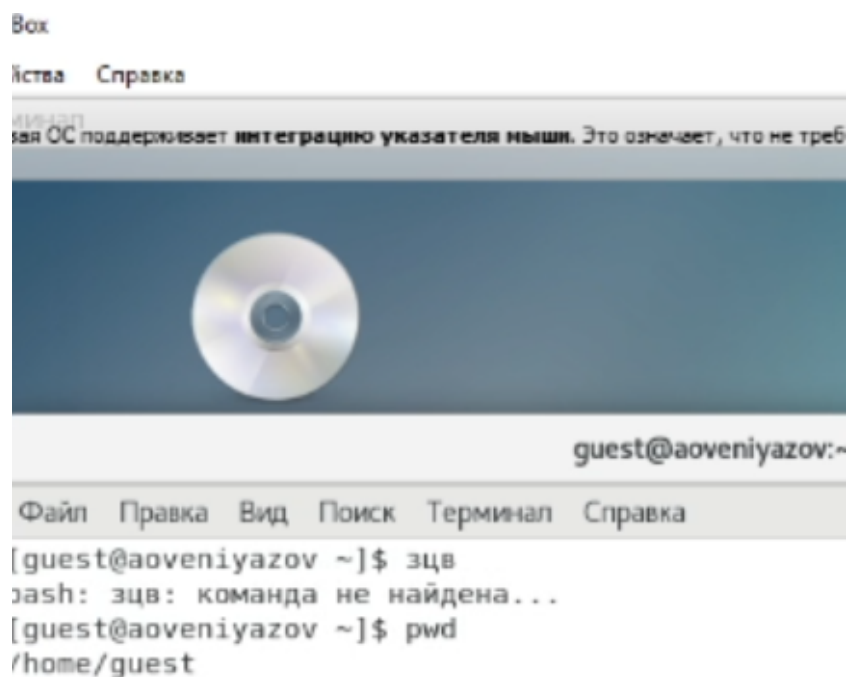


Рис. 4.3: Результат pwd

Уточнил имя текущего пользователя командой whoami.

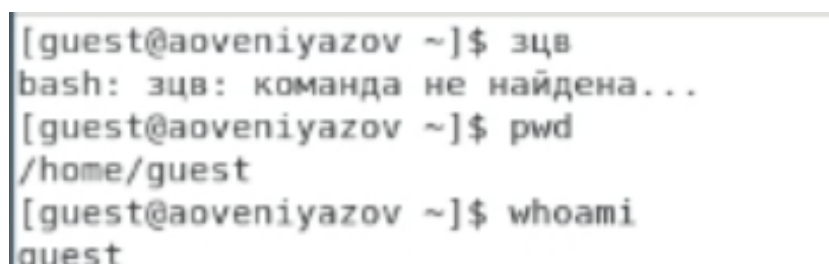
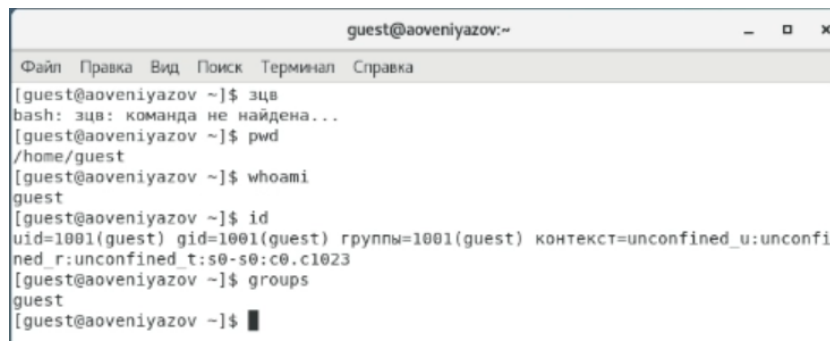


Рис. 4.4: Результат whoami

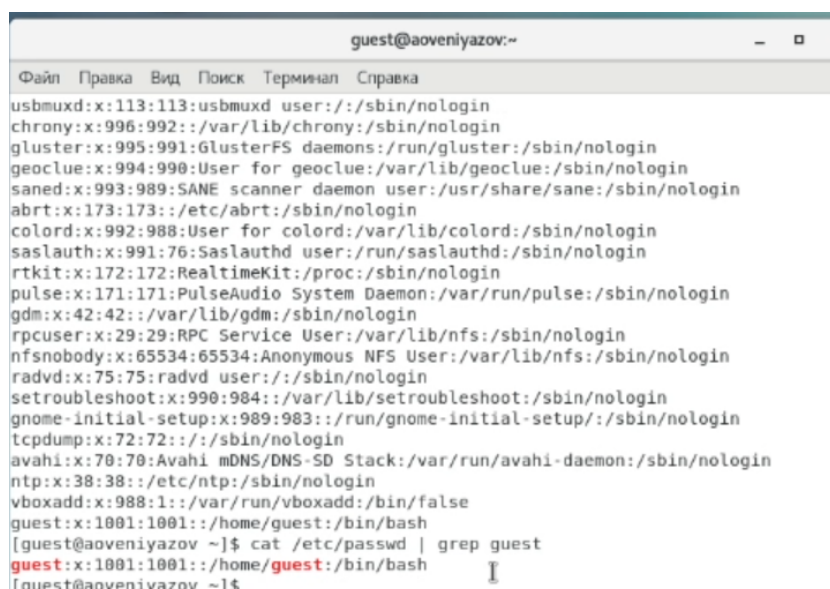
Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой id и groups. Выведенные значения uid, gid и др. запомнил и сравнил вывод команд. Выводы одинаковы, оба говорят о группе guest.



```
guest@aoveniyazov:~  
[guest@aoveniyazov ~]$ зца  
bash: зца: команда не найдена...  
[guest@aoveniyazov ~]$ pwd  
/home/guest  
[guest@aoveniyazov ~]$ whoami  
guest  
[guest@aoveniyazov ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@aoveniyazov ~]$ groups  
guest  
[guest@aoveniyazov ~]$
```

Рис. 4.5: Результат id и groups

Просмотрел файл /etc/passwd командой cat /etc/passwd. Нашел в нём свою учётную запись, определил uid пользователя. Определил gid пользователя. Сравнил найденные значения с полученными в предыдущих пунктах. Отфильтровал результат с помощью grep.



```
guest@aoveniyazov:~  
usbmuxd:x:113:113:usbmuxd user:/usr/sbin/nologin  
chrony:x:996:992:/var/lib/chrony:/usr/sbin/nologin  
gluster:x:995:991:GlusterFS daemons:/run/gluster:/usr/sbin/nologin  
geoclue:x:994:990:User for geoclue:/var/lib/geoclue:/usr/sbin/nologin  
sane:x:993:989:SANE scanner daemon user:/usr/share/sane:/usr/sbin/nologin  
abrt:x:173:173:/etc/abrt:/usr/sbin/nologin  
colord:x:992:988:User for colord:/var/lib/colord:/usr/sbin/nologin  
saslauthd:x:991:76:Saslauthd user:/run/saslauthd:/usr/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/usr/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/usr/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/usr/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/usr/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/usr/sbin/nologin  
radvd:x:75:75:radvd user:/usr/sbin/nologin  
setroubleshoot:x:990:984:/var/lib/setroubleshoot:/usr/sbin/nologin  
gnome-initial-setup:x:989:983:/run/gnome-initial-setup:/usr/sbin/nologin  
tcpdump:x:72:72:/usr/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/usr/sbin/nologin  
ntp:x:38:38:/etc/ntp:/usr/sbin/nologin  
vboxadd:x:988:1:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@aoveniyazov ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@aoveniyazov ~]$
```

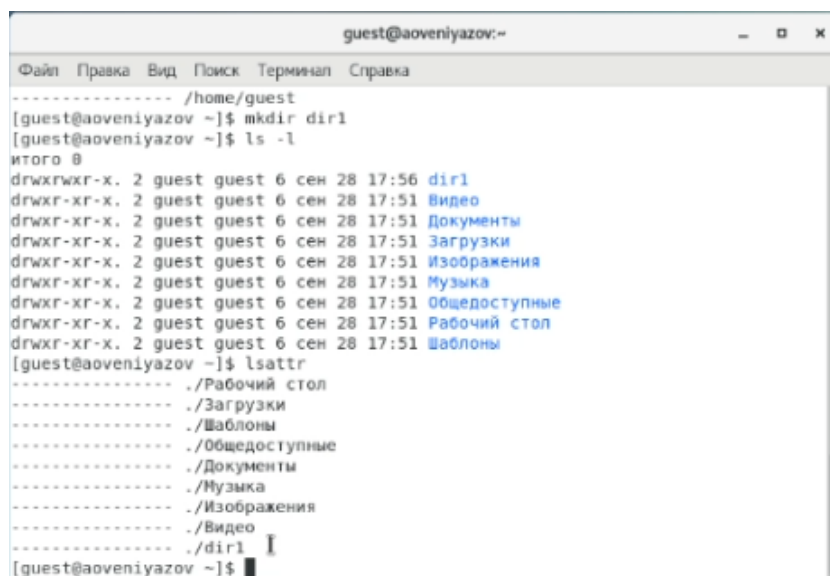
Рис. 4.6: Результат /etc/passwd | grep guest

Определил существующие в системе директории командой ls -l /home/ и проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home/. Посмотрел директорию, но lsattr отказал в доступе.

```
[guest@aoveniyazov ~]$ ls -l /home/
итого 8
drwx-----. 17 aoveniyazov aoveniyazov 4096 сен 28 13:55 aoveniyazov
drwx-----. 15 guest      guest      4096 сен 28 17:51 guest
[guest@aoveniyazov ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/aoveniyazov
----- /home/guest
```

Рис. 4.7: Результат ls -l и lsattr /home/

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.



```
guest@aoveniyazov:~
Файл Правка Вид Поиск Терминал Справка
----- /home/guest
[guest@aoveniyazov ~]$ mkdir dir1
[guest@aoveniyazov ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 28 17:56 dir1
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Видео
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Документы
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Изображения
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Музыка
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Шаблоны
[guest@aoveniyazov ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@aoveniyazov ~]$
```

Рис. 4.8: Результат mkdir dir1, ls -l и lsattr

Снял с директории dir1 все атрибуты командой chmod 000 dir1 и проверил её правильность выполнения командой ls -l

```
[guest@aoveniyazov ~]$ chmod 000 dir1
[guest@aoveniyazov ~]$ ls -l
итого 0
d-----. 2 guest guest 6 сен 28 17:56 dir1
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Видео
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Документы
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Изображения
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Музыка
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 28 17:51 Шаблоны
```

Рис. 4.9: Результат chmod 000 dir1 и ls -l

Попытался создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1. Попытка неудачна.

```
[guest@aoveniyazov ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@aoveniyazov ~]$
```

Рис. 4.10: Результат echo “test” > /home/guest/dir1/file1

Заполнил таблицу «Установленные права и разрешённые действия» (см. табл. 1.1) и на основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнил табл. 1.2.

Таблица 4.1: Установленные права и разрешённые действия

Права		Смена							
кто	Права	Создание	Удаление	Запись	Чтение	рек-	Просмотр	Переименование	Смена
рии	фай-	фай-	фай-	в	фай-	то-	файлов	фай-	бутов
	ла	ла	ла	файл	ла	рии	в дирек-	ла	файла
							тории		
d---	---	-	-	-	-	-	-	-	-
(000)	(000)								
d-	---	-	-	-	-	+	-	-	+
x---	---								
(100)	(000)								
d-	---	-	-	-	-	-	-	-	-
w---	---								
(200)	(000)								

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-- wx- (300)	-- (000)	+	+	-	-	+	-	+	+
dr-- -- (400)	-- (000)	-	-	-	-	-	+	-	-
dr- x-- (500)	-- (000)	-	-	-	-	+	+	-	+
drw-- -- (600)	-- (000)	-	-	-	-	-	+	-	-
drwx- -- (700)	-- (000)	+	+	-	-	+	+	+	+
d-- -- (000)	-x-- (100)	-	-	-	-	-	-	-	-

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- 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)	-	-	-	-	-	+	-	-

Права				Смена					
ди- ре- кто рии	Права фай- ла	Создан фай- ла	Удален фай- ла	Запис в файл	Итени фай- ла	рек- то- рии	Просмотр файлов в дирек- тории	Переимено- вание фай- ла	Смена бутов файла
drwx-	-x-	+	+	-	-	+	+	+	+
-	--								
(700)	(100)								
d--	-w-	-	-	-	-	-	-	-	-
-	--								
(000)	(200)								
d-	-w-	-	-	+	-	+	-	-	+
x--	--								
(100)	(200)								
d-	-w-	-	-	-	-	-	-	-	-
w--	--								
(200)	(200)								
d--	-w-	+	+	+	-	+	-	+	+
wx-	--								
(030)	(200)								
d-	-w-	-	-	-	-	-	+	-	-
r--	--								
(040)	(200)								



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)	-w- -- (200)	-	-	+	-	+	+	-	+
d- rw- (060)	-w- -- (200)	-	-	-	-	-	+	-	-
d- rwx- (070)	-w- -- (200)	+	+	+	-	+	+	+	+
d-- - (000)	- wx- -- (300)	-	-	-	-	-	-	-	-
d- x-- (100)	- wx- -- (300)	-	-	+	-	+	-	-	+

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-- (200)	- wx-- (300)	-	-	-	-	-	-	-	-
d-- wx- (300)	- wx-- (300)	+	+	+	-	+	-	+	+
dr- -- (400)	- wx-- (300)	-	-	-	-	-	+	-	-
dr- x-- (500)	- wx-- (300)	-	-	+	-	+	+	-	+
drw- -- (600)	- wx-- (300)	-	-	-	-	-	+	-	-

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
drwx— — (700)	— wx— — (300)	+	+	+	-	+	+	+	+
d— — (000)	r— — (400)	-	-	-	-	-	-	-	-
d- x— (100)	r— — (400)	-	-	-	+	+	-	-	+
d- w— (200)	r— — (400)	-	-	-	-	-	-	-	-
d— wx- (300)	r— — (400)	+	+	-	+	+	-	+	+

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
dr-- (400)	r---	-	-	-	-	-	+	-	-
dr- x-- (500)	r---	-	-	-	+	+	+	-	+
drw- (600)	r---	-	-	-	-	-	+	-	-
drwx- (700)	r---	+	+	-	+	+	+	+	+
d--- (000)	r-x-	-	-	-	-	-	-	-	-
d- x-- (100)	r-x-	-	-	-	+	+	-	-	+

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- 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)	+	+	-	+	+	+	+	+

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— — (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)	-	-	+	+	+	+	-	+

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
drw— — (600)	rw— — (600)	-	-	-	-	-	+	-	-
drwx— — (700)	rw— — (600)	+	+	+	+	+	+	+	+
d— — (000)	rw— — (700)	-	-	-	-	-	-	-	-
d— x— (100)	rw— — (700)	-	-	+	+	+	-	-	+
d- w— (200)	rw— — (700)	-	-	-	-	-	-	-	-
d— wx- (300)	rw— — (700)	+	+	+	+	+	-	+	+

Права				Смена					
ди-	Права	Создание	Удаление	Запись	Чтение	Рекон-	Просмотр	Смена	
кто	фай-	фай-	фай-	в	фай-	то-	файлов	Переимено-	вание
рии	ла	ла	ла	файл	ла	рии	в дирек-	фай-	бутов
	ла	ла	ла	файл	ла	рии	тории	ла	файла
dr-	rw-	-	-	-	-	-	+	-	-
--	--								
(400)	(700)								
dr-	rw-	-	-	+	+	+	+	-	+
x--	--								
(500)	(700)								
drw-	rw-	-	-	-	-	-	+	-	-
--	--								
(600)	(700)								
drwx-	rw-	+	+	+	+	+	+	+	+
-	--								
(700)	(700)								

Таблица 4.2: Минимально необходимые права для выполнения 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)



Операция	Минимальные права на директорию	Минимальные права на файл
Переименование файла	d-wx— (300)	— — — — (000)
Создание поддиректории	d-wx— (300)	— — — — (000)
Удаление поддиректории	d-wx— (300)	— — — — (000)

## 5 Выводы

Сегодня я приобрел 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. Дискреционное разграничение доступа Linux [Электронный ресурс]. Сайт, 2021. URL: <http://debianinstall.ru/diskretnoe-razgranichenie-dostupa-linux/>.