

Информационная безопасность

Л.2. Дискреционное разграничение прав в Linux. Основные атрибуты

Греков Максим Сергеевич

2021

Содержание

1	Цель работы	4
2	Ход работы	5
2.1	Новый пользователь и вход	5
2.2	Информация о новом пользователе	7
2.3	Существующие директории и их атрибуты	8
2.4	Изменение атрибутов и проверка	10
2.5	Таблица «Установленные права и разрешённые действия»	11
2.6	Таблица «Минимальные права для совершения операций»	19
3	Вывод	21

List of Figures

2.1	Пункты лабораторной 1-2	6
2.2	Пункт лабораторной 3	6
2.3	Пункт лабораторной 4-7	7
2.4	Пункт лабораторной 8	8
2.5	Пункты лабораторной 9-10	9
2.6	Пункт лабораторной 11	9
2.7	Пункт лабораторной 12	10
2.8	Пункт лабораторной 13	11
2.9	Установленные права и разрешённые действия	12
2.10	Установленные права и разрешённые действия	20

1 Цель работы

Целью данной лабораторной работы является 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 Ход работы

2.1 Новый пользователь и вход

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создали учётную запись пользователя guest.
2. Задали пароль для пользователя guest
3. Вошли в систему от имени пользователя guest.
4. Определили директорию, в которой находились, командой pwd. Она совпала с приглашением командной строки. Определили домашнюю директорию и перешли в нее.

```
grekovms@grekovms:/home/grekovms
Файл Правка Вид Поиск Терминал Справка
Пароль:
[root@grekovms grekovms]# useradd guest
The memcache was not invalidated by NSS responder.
[root@grekovms grekovms]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
passwd: Ошибка при операциях с маркером проверки подлинности
[root@grekovms grekovms]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
passwd: Ошибка при операциях с маркером проверки подлинности
[root@grekovms grekovms]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@grekovms grekovms]#
```

Figure 2.1: Пункты лабораторной 1-2

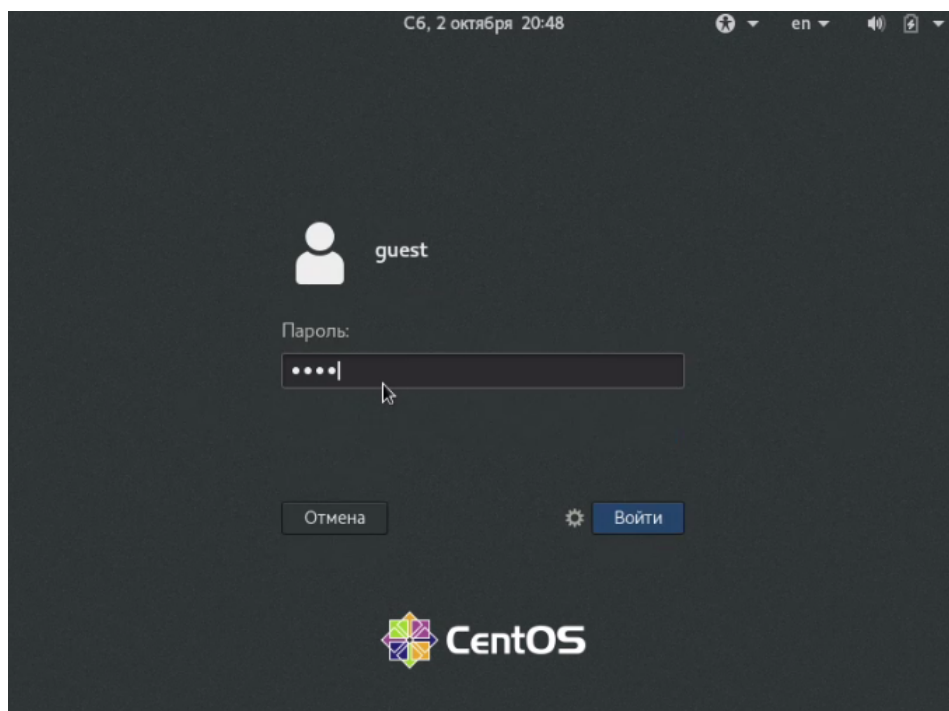
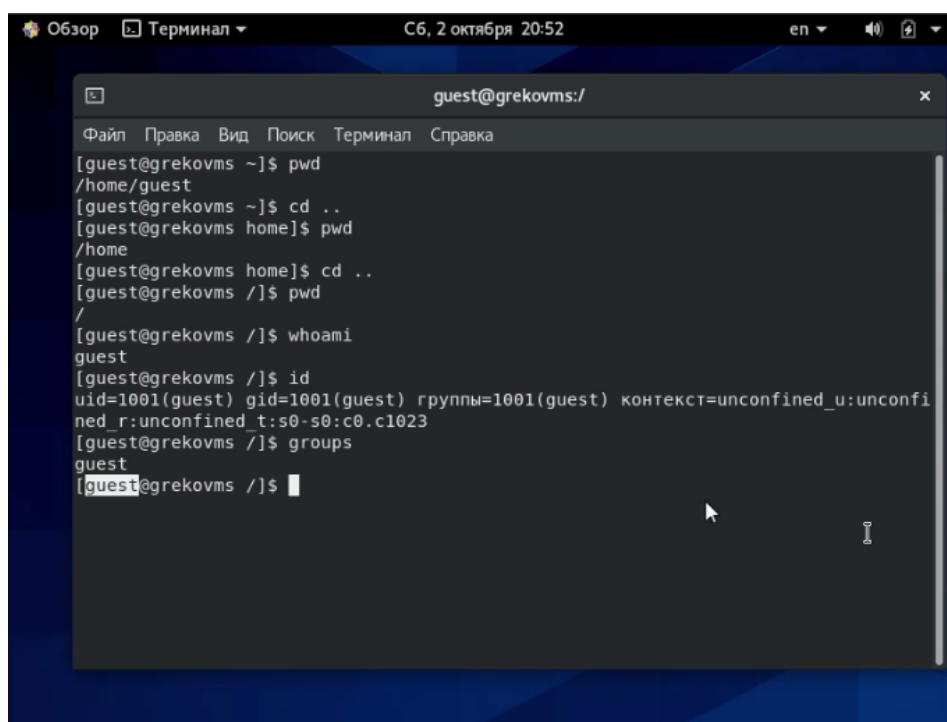


Figure 2.2: Пункт лабораторной 3

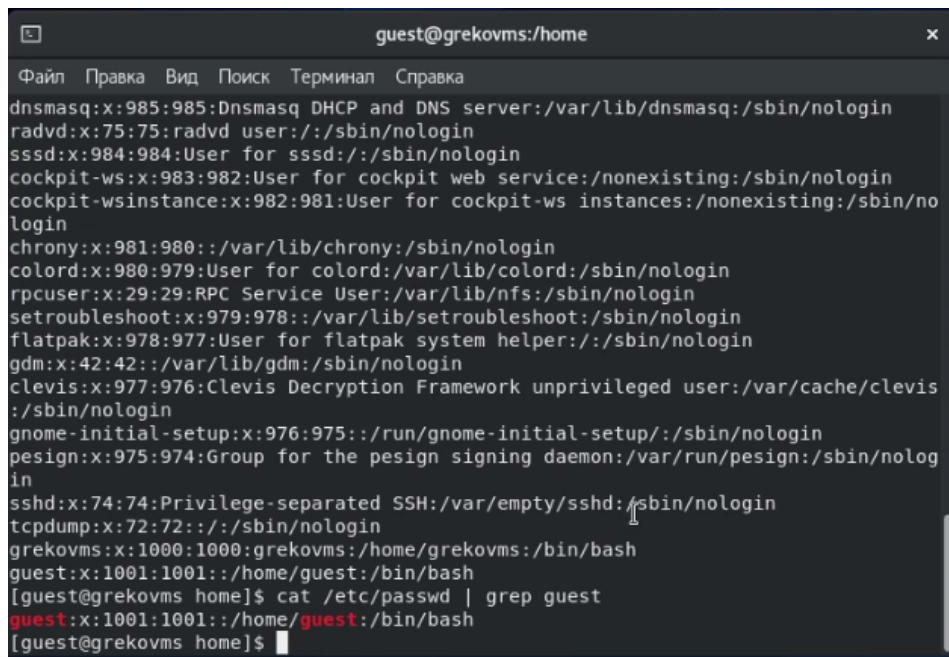
2.2 Информация о новом пользователе

5. Уточнили имя пользователя командой `whoami`.
6. Уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Вывод `id` совпал с выводом команды `groups`.
7. Сравнили полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки, они идентичны.
8. Просмотрели файл `/etc/passwd` командой `cat /etc/passwd` и командой `cat /etc/passwd | grep guest`.



```
Обзор Терминал C6, 2 октября 20:52 en
guest@grekovms:/
Файл Правка Вид Поиск Терминал Справка
[guest@grekovms ~]$ pwd
/home/guest
[guest@grekovms ~]$ cd ..
[guest@grekovms home]$ pwd
/home
[guest@grekovms home]$ cd ..
[guest@grekovms /]$ pwd
/
[guest@grekovms /]$ whoami
guest
[guest@grekovms /]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@grekovms /]$ groups
guest
[guest@grekovms /]$
```

Figure 2.3: Пункт лабораторной 4-7



```
guest@grekovms:/home
Файл  Правка  Вид  Поиск  Терминал  Справка
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/sbin/nologin
sssd:x:984:984:User for sssd:/sbin/nologin
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
chrony:x:981:980::/var/lib/chrony:/sbin/nologin
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot:x:979:978::/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
gnome-initial-setup:x:976:975:/run/gnome-initial-setup:/sbin/nologin
pesign:x:975:974:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
grekovms:x:1000:1000:grekovms:/home/grekovms:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@grekovms home]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@grekovms home]$
```

Figure 2.4: Пункт лабораторной 8

2.3 Существующие директории и их атрибуты

9. Определили существующие в системе директории командой `ls -l /home/`. Увидели, какие права доступа установлены на директориях.

10. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`

Удалось увидеть расширенные атрибуты директории нашего пользователя, но не других пользователей.

11. Создали в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определили командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.


```

guest@grekovms:~
Файл Правка Вид Поиск Терминал Справка
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
grekovms:x:1000:1000:grekovms:/home/grekovms:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@grekovms home]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@grekovms home]$ ls -l /home/
итого 8
drwx-----. 15 grekovms grekovms 4096 окт  2 20:44 grekovms
drwx-----. 15 guest      guest    4096 окт  2 20:48 guest
[guest@grekovms home]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/grekovms
----- /home/guest
[guest@grekovms home]$ cd duest
bash: cd: duest: Нет такого файла или каталога
[guest@grekovms home]$ cd guest
[guest@grekovms ~]$ ls
Видео      Загрузки      Музыка      'Рабочий стол'
Документы  Изображения  Общедоступные  Шаблоны
[guest@grekovms ~]$ mkdir dir1
[guest@grekovms ~]$ ls
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка      'Рабочий стол'
[guest@grekovms ~]$

```

Figure 2.5: Пункты лабораторной 9-10

```

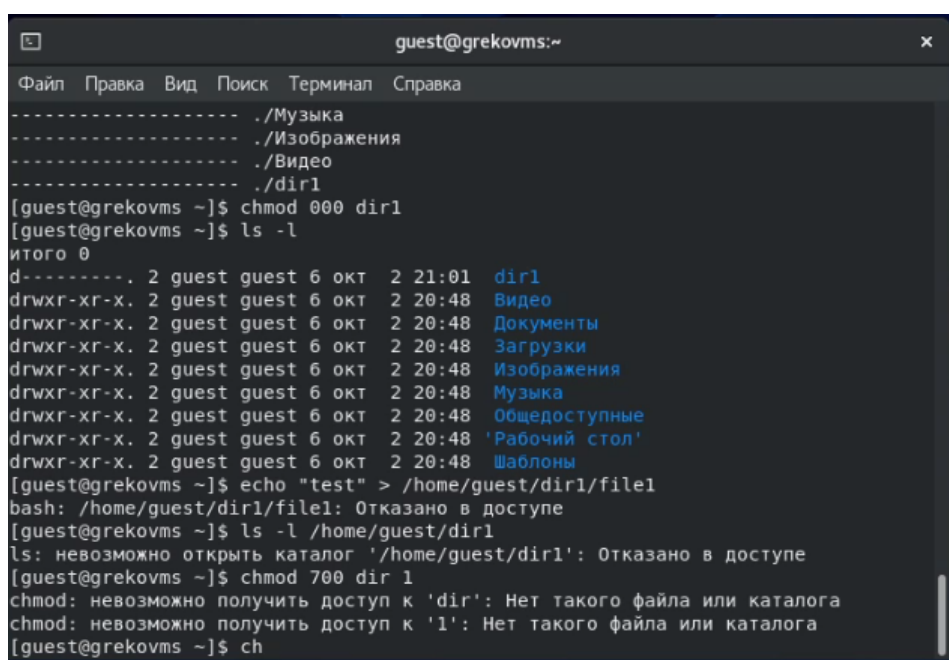
guest@grekovms:~
Файл Правка Вид Поиск Терминал Справка
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки      Музыка      'Рабочий стол'
[guest@grekovms ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 окт  2 21:01 dir1
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 Видео
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 Документы
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 Загрузки
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 Изображения
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 Музыка
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт  2 20:48 Шаблоны
[guest@grekovms ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@grekovms ~]$

```

Figure 2.6: Пункт лабораторной 11

2.4 Изменение атрибутов и проверка

12. Сняли с директории dir1 все атрибуты командой `chmod 000 dir1` и проверили с её помощью правильность выполнения команды `ls -l`
13. Попытались создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` и получили отказ, так как не имеем на это действие прав доступа. Сообщение об ошибке дало подтверждение того, что файл не был создан, проверили это командой `ls -l /home/guest/dir1`



```
guest@grekovms:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
-----  
./Музыка  
./Изображения  
./Видео  
./dir1  
[guest@grekovms ~]$ chmod 000 dir1  
[guest@grekovms ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 окт  2 21:01  dir1  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  Видео  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  Документы  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  Загрузки  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  Изображения  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  Музыка  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  Общедоступные  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  'Рабочий стол'  
drwxr-xr-x. 2 guest guest 6 окт  2 20:48  Шаблоны  
[guest@grekovms ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@grekovms ~]$ ls -l /home/guest/dir1  
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе  
[guest@grekovms ~]$ chmod 700 dir 1  
chmod: невозможно получить доступ к 'dir': Нет такого файла или каталога  
chmod: невозможно получить доступ к '1': Нет такого файла или каталога  
[guest@grekovms ~]$ ch
```

Figure 2.7: Пункт лабораторной 12

```

guest@grekovms:~/dir1
Файл Правка Вид Поиск Терминал Справка
итого 0
d----- . 2 guest guest 6 окт 2 21:01 dir1
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 Видео
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 Документы
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 Загрузки
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 Изображения
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 Музыка
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 окт 2 20:48 Шаблоны
[guest@grekovms ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@grekovms ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@grekovms ~]$ chmod 700 dir 1
chmod: невозможно получить доступ к 'dir': Нет такого файла или каталога
chmod: невозможно получить доступ к '1': Нет такого файла или каталога
[guest@grekovms ~]$ chmod 700 dir1
[guest@grekovms ~]$ ls
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка  'Рабочий стол'
[guest@grekovms ~]$ cd dir1
[guest@grekovms dir1]$ ls
[guest@grekovms dir1]$

```

Figure 2.8: Пункт лабораторной 13

2.5 Таблица «Установленные права и разрешённые действия»

- Заполнили таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определяя опытным путём, какие операции разрешены, а какие нет.
- Если операция разрешена, занесли в таблицу знак «+», если не разрешена, знак «-».

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Установленные права и разрешённые действия													
	Права директо- рии	Права фай- ла	Создани- е файла	Удалени- е файла	Запись в файл	Чтение файла	Смена директо- рии	Просмот- р файлов в директо- рии	Переиме- нование ов файла	Смена атрибу- тов файла				
3	---	(000)	---	(000)	-	-	-	-	-	-				
4	--x	(100)	---	(000)	-	-	-	+	-	-				
5	-w-	(200)	---	(000)	-	-	-	-	-	-				
6	-wx	(300)	---	(000)	+	-	-	+	-	+				
7	r--	(400)	---	(000)	-	-	-	+	-	-				
8	r-x	(500)	---	(000)	-	-	-	+	+	-				
9	rwx	(600)	---	(000)	-	-	-	+	-	-				
10	rwx	(700)	---	(000)	+	-	-	+	+	+				
11	---	(000)	--x	(100)	-	-	-	-	-	-				
12	--x	(100)	--x	(100)	-	-	-	+	-	+				
13	-w-	(200)	--x	(100)	-	-	-	-	-	-				
14	-wx	(300)	--x	(100)	+	-	-	+	-	+				
15	r--	(400)	--x	(100)	-	-	-	+	-	-				
16	r-x	(500)	--x	(100)	-	-	-	+	+	-				
17	rwx	(600)	--x	(100)	-	-	-	+	-	-				
18	rwx	(700)	--x	(100)	+	-	-	+	+	+				
19	---	(000)	-w-	(200)	-	-	-	-	-	-				
20	--x	(100)	-w-	(200)	-	+	-	+	-	+				
21	-w-	(200)	-w-	(200)	-	-	-	-	-	-				
22	-wx	(300)	-w-	(200)	+	-	-	+	-	+				
23	r--	(400)	-w-	(200)	-	-	-	+	-	-				
24	r-x	(500)	-w-	(200)	-	+	-	+	-	+				
25	rwx	(600)	-w-	(200)	-	-	-	+	-	-				
26	rwx	(700)	-w-	(200)	+	+	-	+	+	+				
27	---	(000)	-wx	(300)	-	-	-	-	-	-				

Figure 2.9: Установленные права и разрешённые действия

Права директо- рии	Права фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на директо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание Файла	Смена атрибу- тов файла
---	---	-	-	-	-	-	-	-	-
(000)	(000)								
--x	---	-	-	-	-	+	-	-	+
(100)	(000)								
-w-	---	-	-	-	-	-	-	-	-
(200)	(000)								
-wx	---	+	+	-	-	+	-	+	+
(300)	(000)								
r--	---	-	-	-	-	-	+	-	-
(400)	(000)								

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
r - x (500)	- - - (000)	-	-	-	-	+	+	-	+
r w - (600)	- - - (000)	-	-	-	-	-	+	-	-
r w x (700)	- - - (000)	+	+	-	-	+	+	+	+
- - - (000)	- - x (100)	-	-	-	-	-	-	-	-
- - x (100)	- - x (100)	-	-	-	-	+	-	-	+
- w - (200)	- - x (100)	-	-	-	-	-	-	-	-
- w x (300)	- - x (100)	+	+	-	-	+	-	+	+
r - - (400)	- - x (100)	-	-	-	-	-	+	-	-
r - x (500)	- - x (100)	-	-	-	-	+	+	-	+
r w - (600)	- - x (100)	-	-	-	-	-	+	-	-
r w x (700)	- - x (100)	+	+	-	-	+	+	+	+

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

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
- w - (200)	- w x (300)	-	-	-	-	-	-	-	-
- w x (300)	- w x (300)	+	+	+	-	+	-	+	+
r - - (400)	- w x (300)	-	-	-	-	-	+	-	-
r - x (500)	- w x (300)	-	-	+	-	+	+	-	+
r w - (600)	- w x (300)	-	-	-	-	-	+	-	-
r w x (700)	- w x (300)	+	+	+	-	+	+	+	+
- - - (000)	r - - (400)	-	-	-	-	-	-	-	-
- - x (100)	r - - (400)	-	-	-	+	+	-	-	+

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
- w - (200)	r - - (400)	-	-	-	-	-	-	-	-
- w x (300)	r - - (400)	+	+	-	+	+	-	+	+
r - - (400)	r - - (400)	-	-	-	-	-	+	-	-
r - x (500)	r - - (400)	-	-	-	+	+	+	-	+
r w - (600)	r - - (400)	-	-	-	-	-	+	-	-
r w x (700)	r - - (400)	+	+	-	+	+	+	+	+
- - - (000)	r - x (500)	-	-	-	-	-	-	-	-
- - x (100)	r - x (500)	-	-	-	+	+	-	-	+
- w - (200)	r - x (500)	-	-	-	-	-	-	-	-
- w x (300)	r - x (500)	+	+	-	+	+	-	+	+
r - - (400)	r - x (500)	-	-	-	-	-	+	-	-

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
r - x (500)	r - x (500)	-	-	-	+	+	+	-	+
r w - (600)	r - x (500)	-	-	-	-	-	+	-	-
r w x (700)	r - x (500)	+	+	-	+	+	+	+	+
- - - (000)	r w x (600)	-	-	-	-	-	-	-	-
- - x (100)	r w x (600)	-	-	+	+	+	-	-	+
- w - (200)	r w x (600)	-	-	-	-	-	-	-	-
- w x (300)	r w x (600)	+	+	+	+	+	-	+	+
r - - (400)	r w x (600)	-	-	-	-	-	+	-	-

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
r - x (500)	r w x (600)	-	-	+	+	+	+	-	+
r w - (600)	r w x (600)	-	-	-	-	-	+	-	-
r w x (700)	r w x (600)	+	+	+	+	+	+	+	+
- - - (000)	r w x (700)	-	-	-	-	-	-	-	-
- - x (100)	r w x (700)	-	-	+	+	+	-	-	+
- w - (200)	r w x (700)	-	-	-	-	-	-	-	-
- w x (300)	r w x (700)	+	+	+	+	+	-	+	+

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
r - - (400)	r w x (700)	-	-	-	-	-	+	-	-
r - x (500)	r w x (700)	-	-	+	+	+	+	-	+
r w - (600)	r w x (700)	-	-	-	-	-	+	-	-
r w x (700)	r w x (700)	+	+	+	+	+	+	+	+

2.6 Таблица «Минимальные права для совершения операций»

На основании заполненной таблицы определили те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнили вторую таблицу “Минимальные права для совершения операций”.

	A	B	C
1	<u>Минимальные права для совершения операций</u>		
2	Операция	Минимальные права на директорию	Минимальные права на файл
3	Создание файла	- w x (300)	- - - (000)
4	Удаление файла	- w x (300)	- - - (000)
5	Чтение файла	- - x (100)	r - - (400)
6	Запись в файл	- - x (100)	- w - (200)
7	Переименование файла	- w x (300)	- - - (000)
8	Создание поддиректории	- w x (300)	- - - (000)
9	Удаление поддиректории	- w x (300)	- - - (000)
10			

Figure 2.10: Установленные права и разрешённые действия

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	- w x (300)	- - - (000)
Удаление файла	- w x (300)	- - - (000)
Чтение файла	- - x (100)	r - - (400)
Запись в файл	- - x (100)	- w - (200)
Переименование файла	- w x (300)	- - - (000)
Создание поддиректории	- w x (300)	- - - (000)
Удаление поддиректории	- w x (300)	- - - (000)

3 Вывод

В ходе лабораторной работы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.