

Отчет по лабораторной работе №2

Дискреционное разграничение прав Linux

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	15
	Список литературы	16

Список иллюстраций

3.1	Командная строка. Работа с пользователем	7
3.2	Командная строка. Сравнение id и groups	8
3.3	Командная строка. Просмотр файла /etc/passwd	9
3.4	Командная строка. Команды lsattr и ls -l	10
3.5	Командная строка. Снятие дистрибутов для dirl	10
3.6	Права на директорию и файл	14

Список таблиц

3.1	Установленные права и разрешенные действия	11
3.2	Минимальные права для совершения операций	13

1 Цель работы

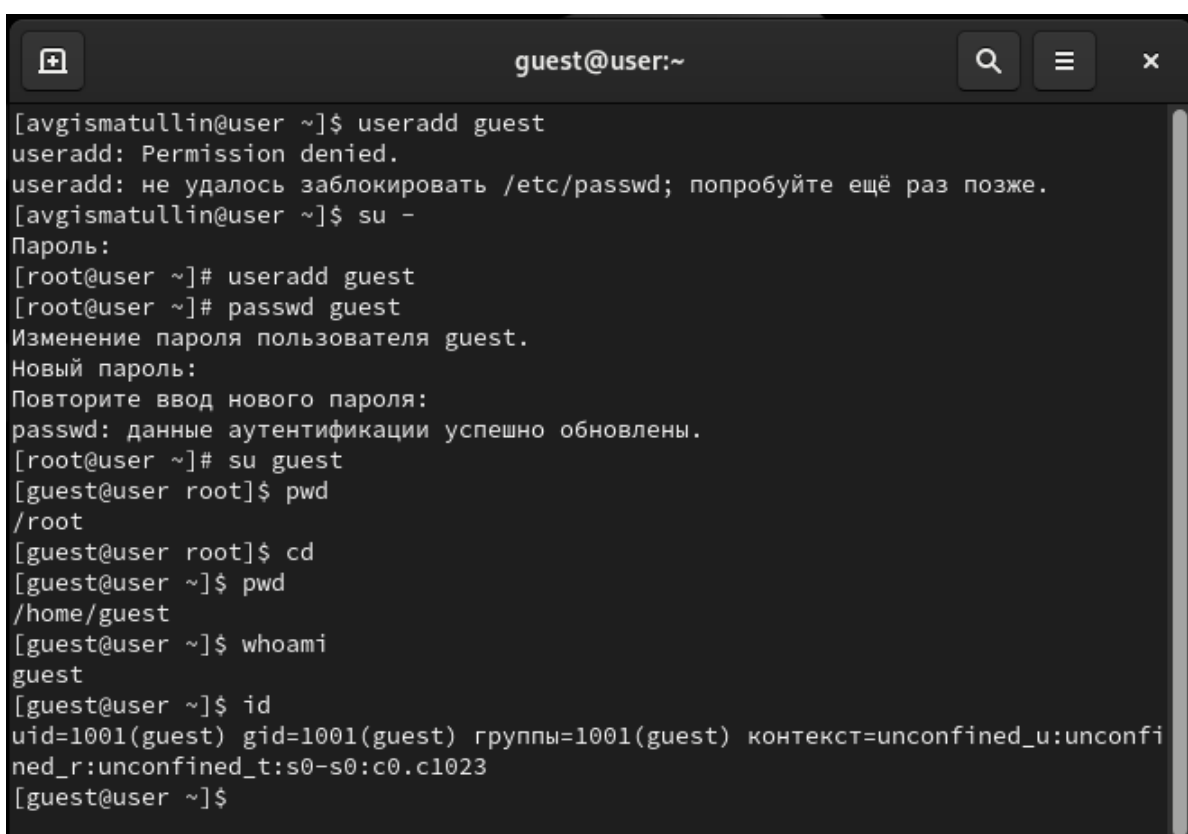
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Задание

Последовательно выполнять все пункты, занося ответы и замечания в отчет.

3 Выполнение лабораторной работы

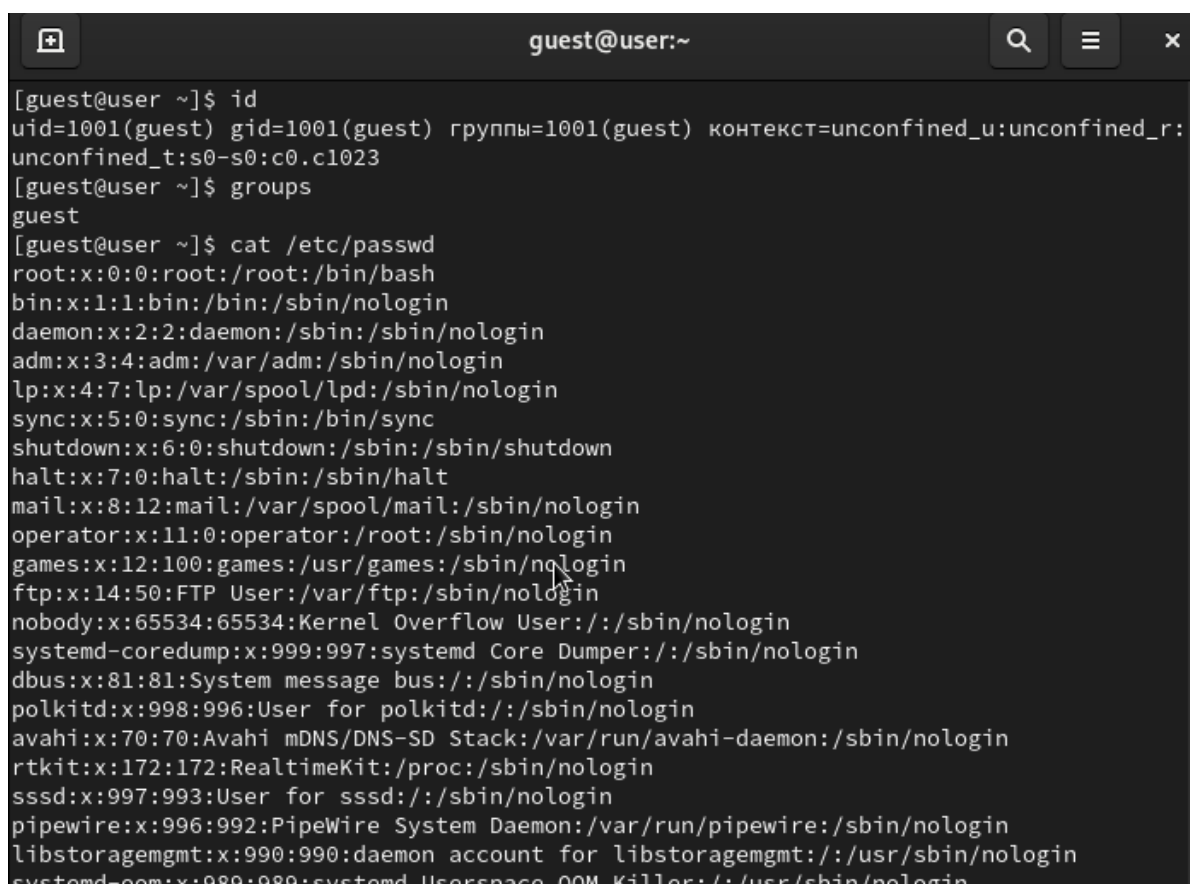
1. Создадим пользователя `guest`, зададим ему пароль и войдем под этим именем в систему через команду `su guest`. Далее перейдем в корневую директорию и узнаем через команду `id - uid` и `gid` пользователя `guest` (рис. 3.1)



```
guest@user:~  
[avgismatullin@user ~]$ useradd guest  
useradd: Permission denied.  
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.  
[avgismatullin@user ~]$ su -  
Пароль:  
[root@user ~]# useradd guest  
[root@user ~]# passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[root@user ~]# su guest  
[guest@user root]$ pwd  
/root  
[guest@user root]$ cd  
[guest@user ~]$ pwd  
/home/guest  
[guest@user ~]$ whoami  
guest  
[guest@user ~]$ id  
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@user ~]$
```

Рис. 3.1: Командная строка. Работа с пользователем

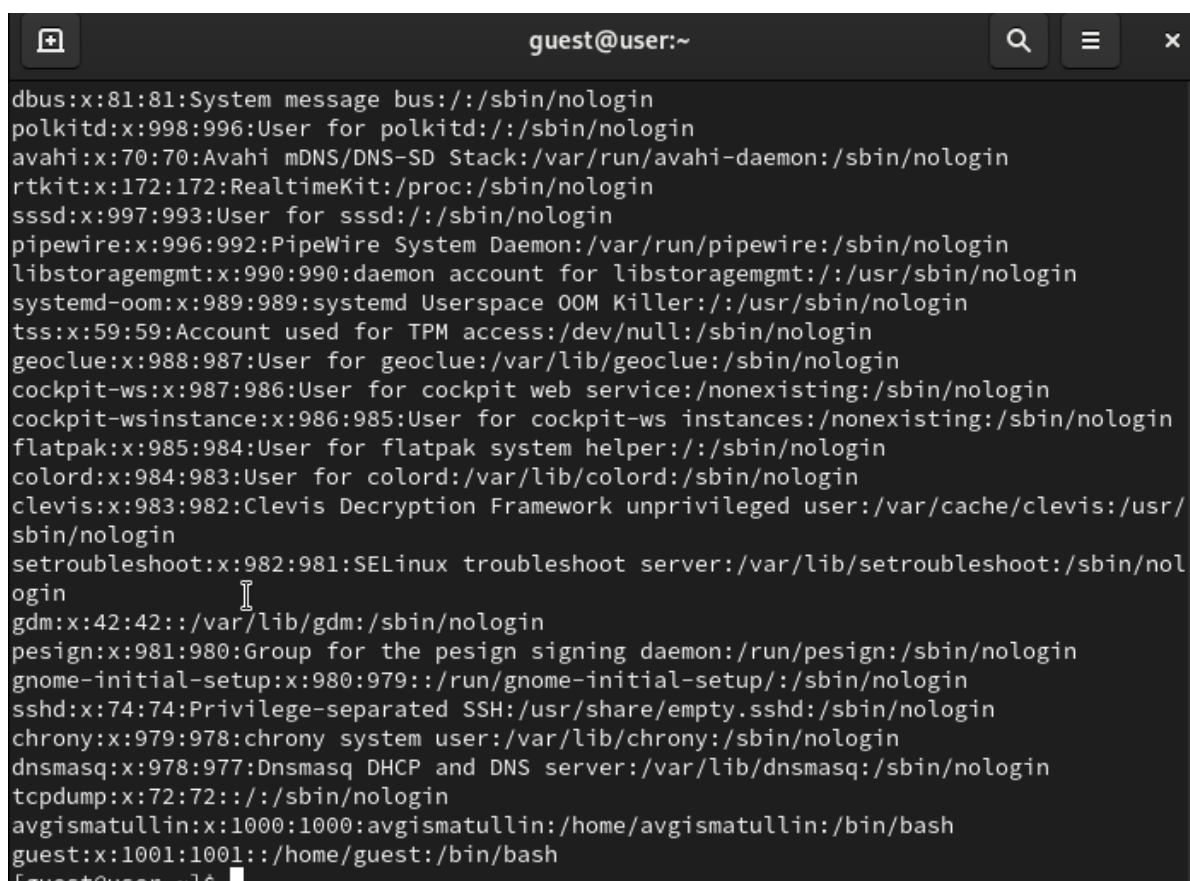
2. После этого сравним команду `id` с выводом `groups`. Убедимся, что данные совпадают (рис. 3.2)

A terminal window titled 'guest@user:~' with search, menu, and close icons in the title bar. The terminal shows the output of the 'id' and 'groups' commands, followed by the contents of the '/etc/passwd' file.

```
[guest@user ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@user ~]$ groups
guest
[guest@user ~]$ 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
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:usr/sbin/nologin
```

Рис. 3.2: Командная строка. Сравнение id и groups

Здесь же посмотрим файл `/etc/passwd` командой `cat` и найдем данные о пользователе `avgismatullin` и `guest`. Разница лишь в порядке `id`, ведь отсчет начинается с 1000, поэтому у `guest` показатели `uid` и `gid` 1001 (рис. 3.3)

A terminal window titled 'guest@user:~' with search, menu, and close buttons in the title bar. The terminal displays the output of the 'cat /etc/passwd' command, listing system and regular users. The output is as follows:

```
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-oom:x:989:989:systemd Userspace OOM Killer:/:usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:985:984:User for flatpak system helper:/:/sbin/nologin
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/
sbin/nologin
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nol
ogin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:980:979:/:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:978:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
avgismatullin:x:1000:1000:avgismatullin:/home/avgismatullin:/bin/bash
guest:x:1001:1001:/:/home/guest:/bin/bash
```

Рис. 3.3: Командная строка. Просмотр файла /etc/passwd

3. Через пользователя guest выведем данные командой `ls -l /home/`, чтобы посмотреть права доступа. Мы видим, что для владельца файла доступно редактирование, удаление и чтение файлов. Командой `lsattr /home` можем посмотреть только содержимое файлов пользователя guest. Для avgismatullin доступ отказан (рис. 3.4)

```
guest@user:~  
[guest@user ~]$ ls -l /home/  
итого 4  
drwx-----. 14 avgismatullin avgismatullin 4096 map  2 17:51 avgismatullin  
drwx-----.  4 guest          guest          92 map  2 18:02 guest  
[guest@user ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/avgismatullin  
----- /home/guest  
[guest@user ~]$ mkdir dirl  
[guest@user ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 map  2 18:02 dirl  
[guest@user ~]$ lsattr dirl
```

Рис. 3.4: Командная строка. Команды lsattr и ls -l

Здесь же создадим директорию dirl и проверим права доступа.

4. При помощи команды `chmod 000 dirl` снимем все атрибуты и попробуем создать в этой директории файл, записав что-то в него. Ни это, ни даже посетить данную директорию не удастся (рис. 3.5)

```
guest@user:~/dirl  
[guest@user ~]$ chmod 000 dirl  
[guest@user ~]$ ls -l  
итого 0  
d------. 2 guest guest 6 map  2 18:02 dirl  
[guest@user ~]$ echo "test" > /home/guest/dirl/file1  
bash: /home/guest/dirl/file1: Отказано в доступе  
[guest@user ~]$ ls -l/home/guest/dirl  
ls: неверный ключ - «/»  
По команде «ls --help» можно получить дополнительную информацию.  
[guest@user ~]$ ls -l /home/guest/dirl  
ls: невозможно открыть каталог '/home/guest/dirl': Отказано в доступе  
[guest@user ~]$ cd dirl/  
bash: cd: dirl/: Отказано в доступе
```

Рис. 3.5: Командная строка. Снятие дистрибутов для dirl

5. Далее заполним таблицу “Установленные права и разрешенные действия” 3.1, где “+” и “-” - знак того, разрешена или нет операция.

Здесь каждый параметр обозначает следующее:

- 1 - Создание файла

- 2 - Удаление файла
- 3 - Запись в файл
- 4 - Чтение в файл
- 5 - Смена директории
- 6 - Просмотр файлов в директории
- 7 - Переименовывание файла
- 8 - Смена атрибутов файла

Таблица 3.1: Установленные права и разрешенные действия

Права директории	Права файла	1	2	3	4	5	6	7	8
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)	+	+	-	-	+	+	+	+
d------(000)	--w------(200)	-	-	-	-	-	-	-	-
d--x------(100)	--w------(200)	-	-	+	-	+	-	-	+
d-w------(200)	--w------(200)	-	-	-	-	-	-	-	-

Права директории	Права файла	1	2	3	4	5	6	7	8
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)	+	+	+	-	+	+	+	+
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)	-	-	-	+	+	+	-	+

Права директории	Права файла	1	2	3	4	5	6	7	8
drw----- (600)	-r-x----- (500)	-	-	-	-	-	-	-	-
drwx----- (700)	-r-x----- (500)	+	+	-	+	+	+	+	+
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)	+	+	+	+	+	+	+	+

На основании таблицы выше определили минимально необходимые права для выполнения операций внутри директории dir1 и заполнили таблицу 3.2. Для заполнения последних двух строк опытным путем проверили минимальные права.

Таблица 3.2: Минимальные права для совершения операций

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)

Операция	Права на директорию	Права на файл
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)

Эти данные мы вносим в соответствие с показателями (рис. 3.6)

Операция	Права на директорию	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)

Рис. 3.6: Права на директорию и файл

4 Выводы

В ходе выполнения данной лабораторной работы были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux1.

Список литературы

1. Теория разграничения прав пользователей
2. Разрешения доступа к файлам