

Отчет к лабораторной работе №2

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

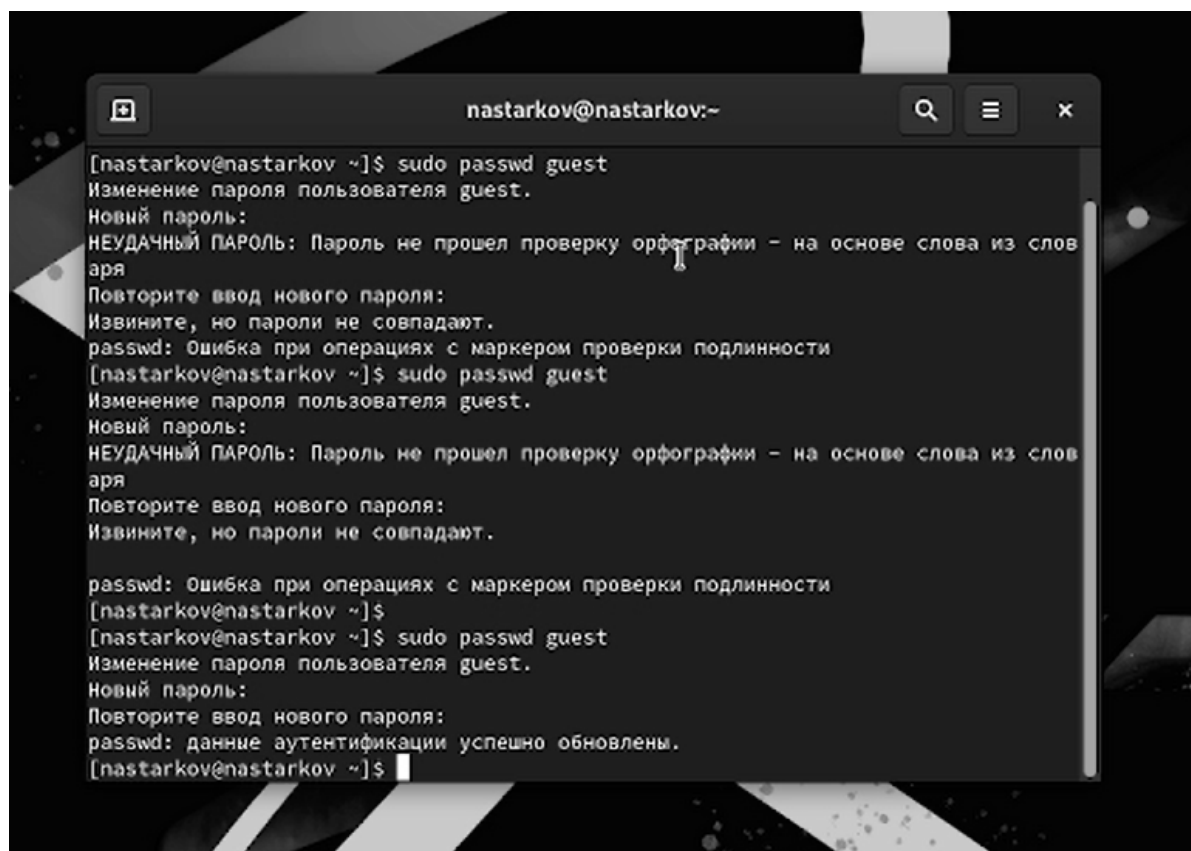
author: Старков Н.А.

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.

Выполнение работы

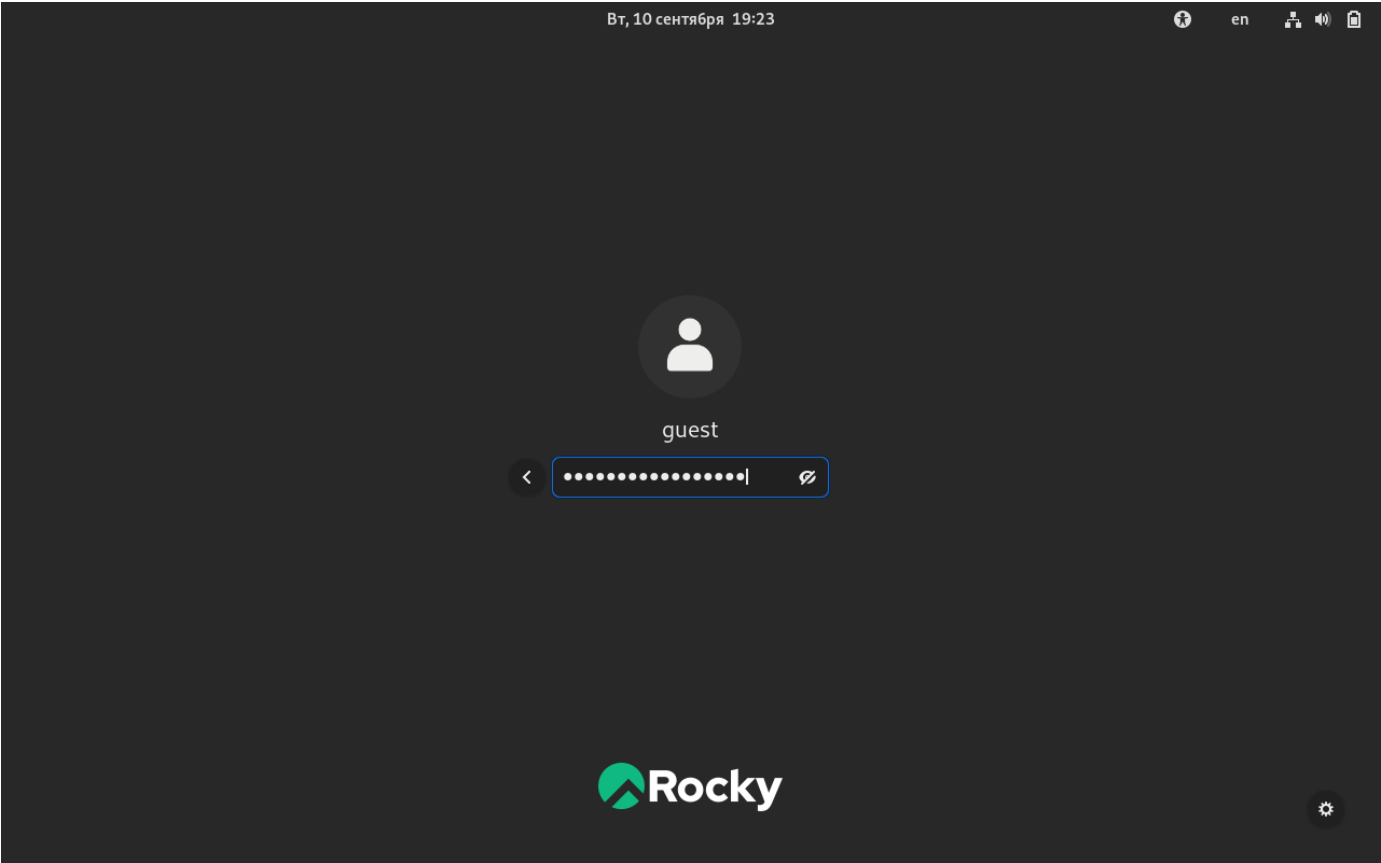
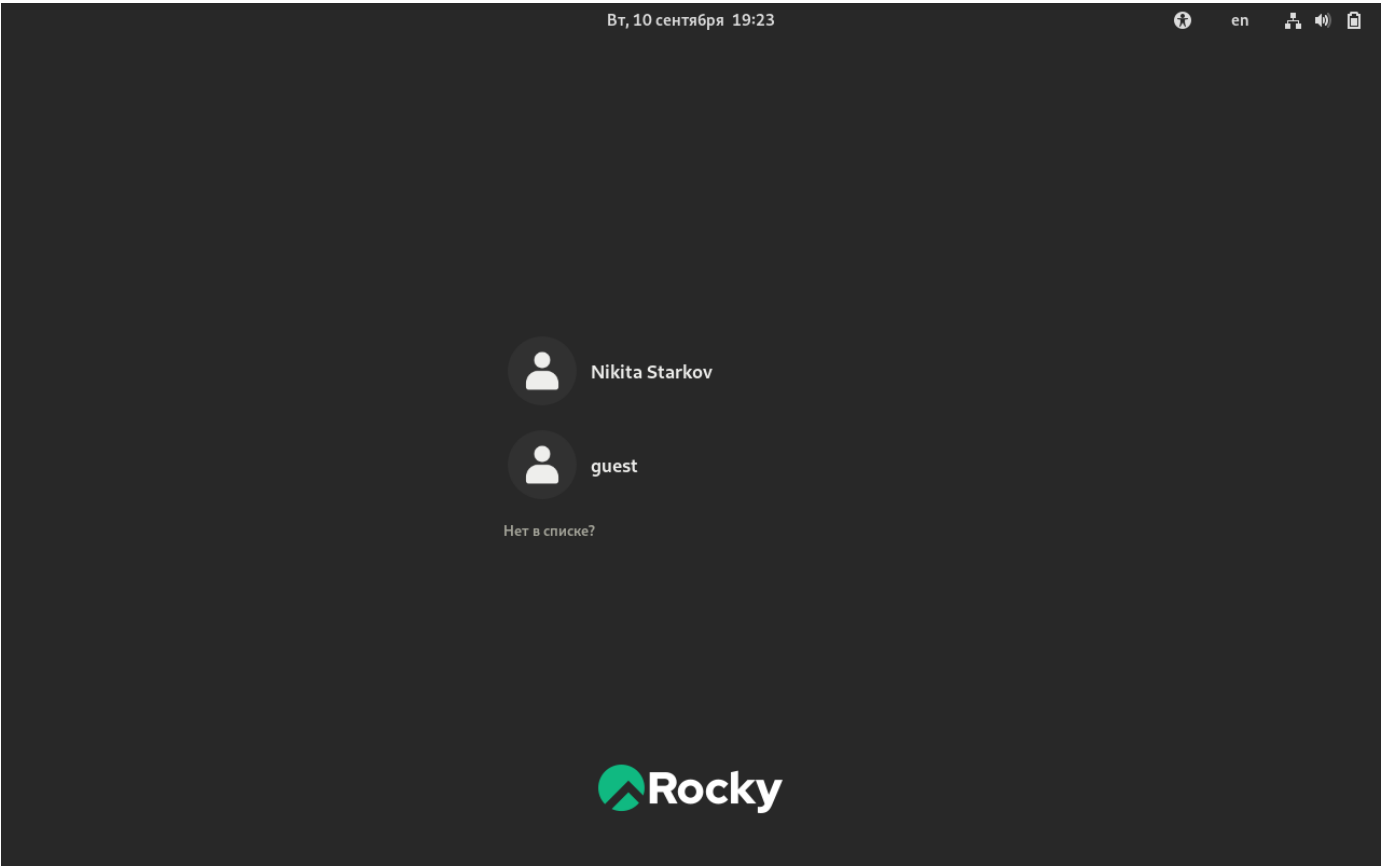
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создали учётную запись пользователя guest (используя учётную запись администратора):
 - с помощью команды `sudo useradd guest` инициировали добавление нового пользователя в систему;
 - с помощью команды `passwd guest` задали пароль.



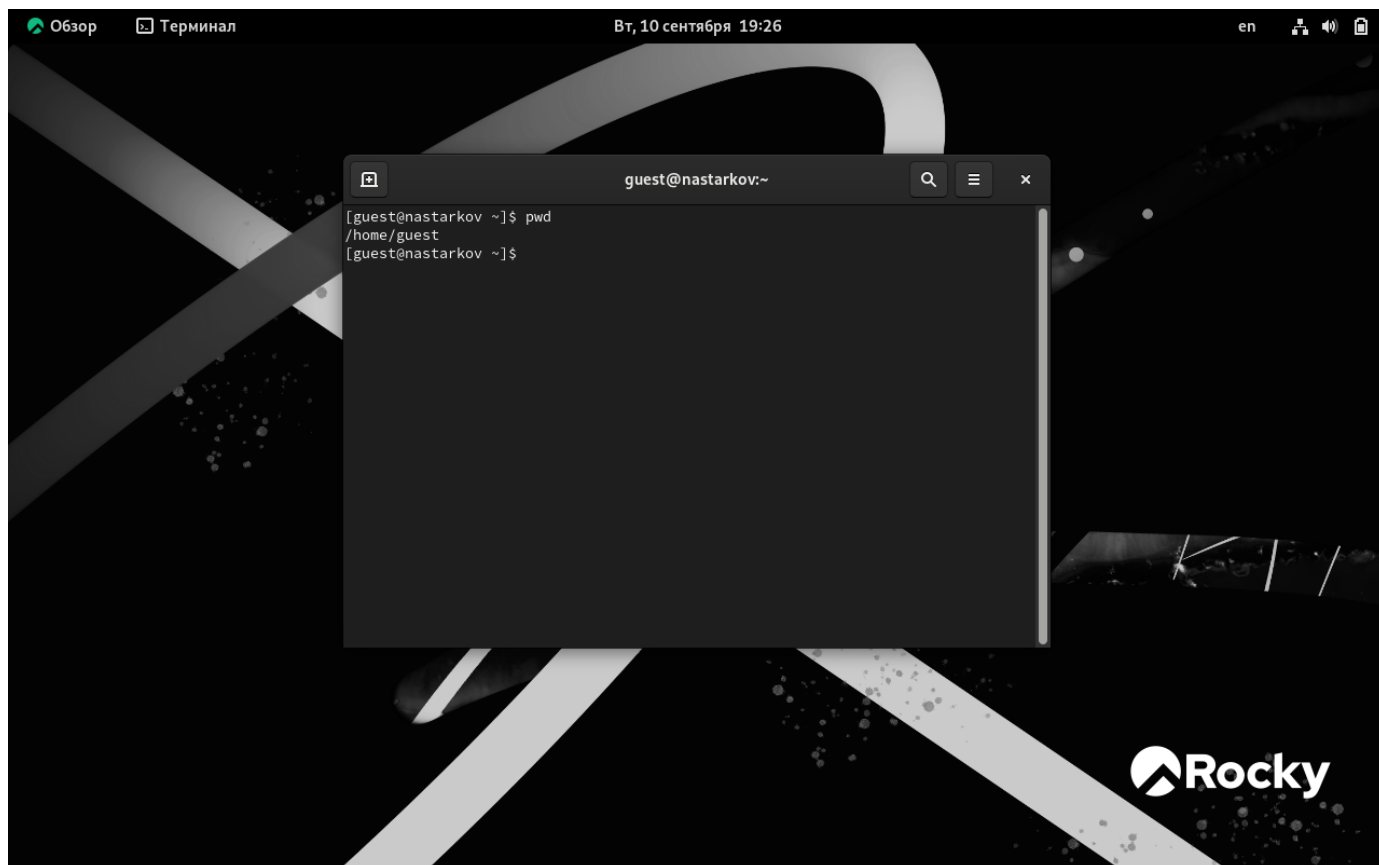
```
nastarkov@nastarkov:~$ sudo useradd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - на основе слова из словаря
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
passwd: Ошибка при операциях с маркером проверки подлинности
[nastarkov@nastarkov ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - на основе слова из словаря
Повторите ввод нового пароля:
Извините, но пароли не совпадают.

passwd: Ошибка при операциях с маркером проверки подлинности
[nastarkov@nastarkov ~]$
[nastarkov@nastarkov ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[nastarkov@nastarkov ~]$
```

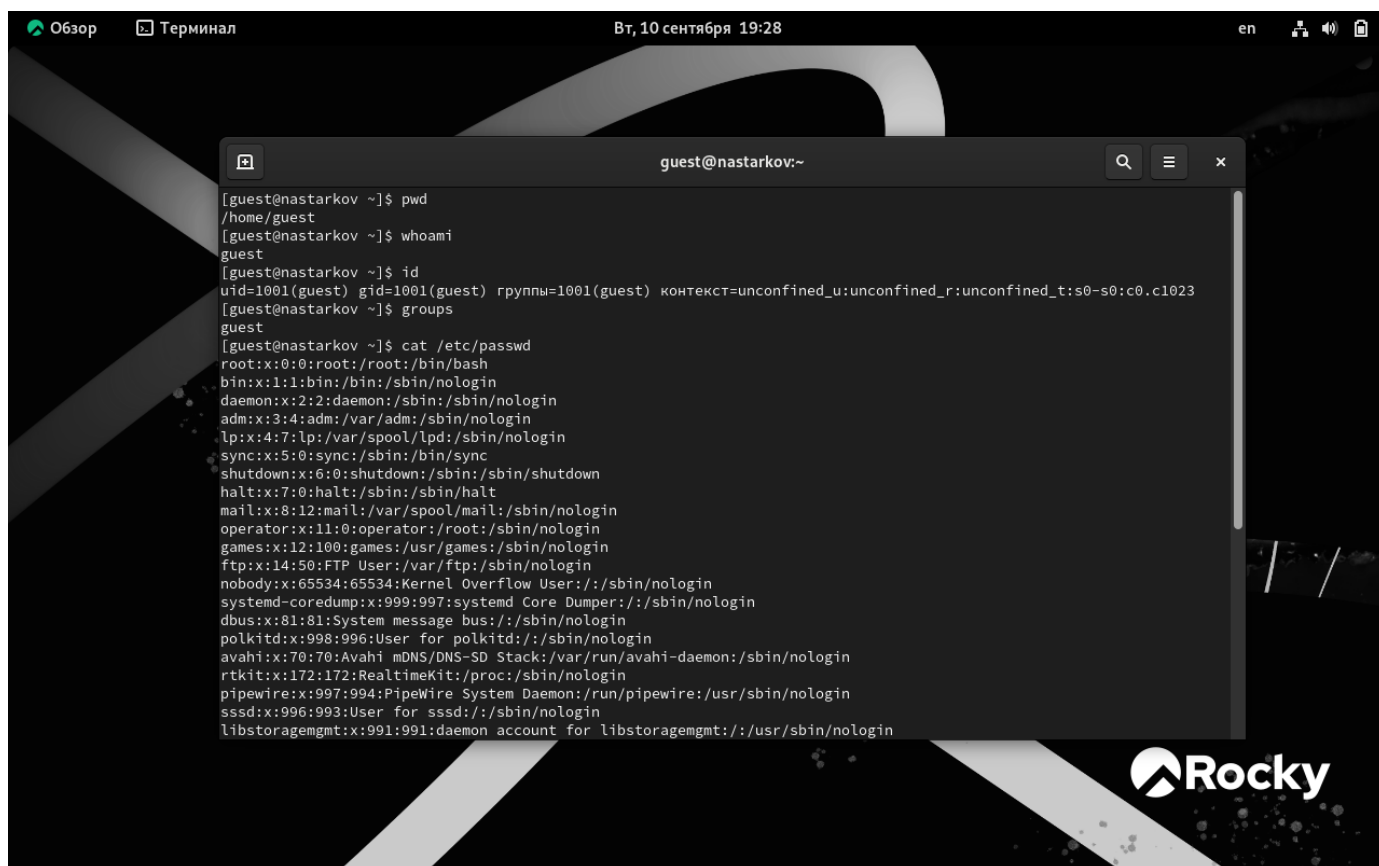
2. Вошли в систему от имени guest.



3. Определили директорию, в которой находимся, командой pwd



4. Уточнили имя пользователя командой `whoami`



5. Просмотрели файл командой `cat /etc/passwd`. Определили `uid` и `gid` пользователя (они равны 1001). Найденные значения совпадают с тем, что было в предыдущих пунктах.

```
[guest@nastarkov ~]$ whoami
guest
[guest@nastarkov ~]$ id
uid=1001(guest) gid=1001(guest) ргруппы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@nastarkov ~]$ groups
guest
[guest@nastarkov ~]$ 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
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
nastarkov:x:1000:1000:Nikita Starkov:/home/nastarkov:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@nastarkov ~]$
```

6. Определили существующие в системе директории командой `ls -l /home/`. Командой `lsattr /home` проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`. Получили отказано в доступе.

Командой `mkdir` создали директорию `dir1`. Сняли с директории `dir1` все значения командой `chmod 000 dir1`. Проверили правильность выполнения команды `ls -l`

```
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
nastarkov:x:1000:1000:Nikita Starkov:/home/nastarkov:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@nastarkov ~]$ ls -l /home/
итого 8
drwx-----. 14 guest guest 4096 сен 10 19:24 guest
drwx-----. 14 nastarkov nastarkov 4096 сен 9 23:32 nastarkov
[guest@nastarkov ~]$ lsattr /home
lsattr: Отказано в достуtne While reading flags on /home/nastarkov
----- /home/guest
[guest@nastarkov ~]$ mkdir dir1
[guest@nastarkov ~]$ chmod 000 dir1
[guest@nastarkov ~]$ ls -l
итого 0
d-----.. 2 guest guest 6 сен 10 19:33 dir1
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 Видео
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 Документы
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 Изображения
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 Музыка
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 10 19:23 Шаблоны
[guest@nastarkov ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Нет такого файла или каталога
[guest@nastarkov ~]$ echo "test" > /home/guest/dir1
bash: /home/guest/dir1: Нет такого файла или каталога
[guest@nastarkov ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@nastarkov ~]$
```

7. Попытались создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Этого сделать не удалось. Командой `ls -l /home/guest/dir1` оценили, как сообщение об ошибке отразилось на создании файла

```
[guest@nastarkov ~]$ echo "test" > /home/guest/dir1
bash: /home/guest/dir1: Нет такого файла или каталога
[guest@nastarkov ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@nastarkov ~]$
```

8. Заполним таблицу "Установленные права и разрешённые действия". Нужно заполнить 64 ячейки.

Создание файла: echo"test" > /home/guest/dir1/file2. Удаление файла: rm -r /home/guest/dir1/file1. Запись в файл: echo"textnew" > /home/guest/dir1/file1. Чтение файла: cat /home/guest/dir1/file1. Смена директории: cd dir1. Просмотр файлов в директории: ls dir1. Переименование файла: mv /home/guest/dir1/file1 filenew. Смена атрибутов файла: chattr -a /home/guest/dir1/file1.

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d (000)	(000)	-	-	-	-	-	-	-	-
d -x (100)	(000)	-	-	-	-	+	-	-	-
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)	+	+	-	-	+	+	+	-
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
----	-----	-----	-----	-----	-----	----	--	-	-----
d (000)	(100)	-	-	-	-	-	-	-	-
d -x (100)	(100)	-	-	-	-	+	-	-	-
d -w- (200)	(100)	-	-	-	-	-	-	-	-
d -wx (300)	(100)	+	+	-	-	+	-	+	-
d r- (400)	(100)	-	-	-	-	-	+	-	-
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)	+	+	+	-	+	+	+	-
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
----	-----	-----	-----	-----	-----	----	--	-	-----

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов 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)	-	-	-	+	+	-	-	+
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)	+	+	-	+	+	+	+	+
----- ----	----- -----	----- -----	----- -----	----- -----	----- -----	----- ----	----- ----- --	----- -	----- -----
d (000)	(500)	-	-	-	-	-	-	-	-
d -x (100)	(500)	-	-	-	+	+	-	-	+
d -w- (200)	(500)	-	-	-	-	-	-	-	-
d -wx (300)	(500)	+	+	-	+	+	-	+	+
d r- (400)	(500)	-	-	-	-	-	+	-	-
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)	-	-	-	-	-	+	-	-

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d rwx (700)	(600)	+	+	+	+	+	+	+	+
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
----	-----	-----	-----	-----	-----	----	--	-	-----
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)	+	+	+	+	+	+	+	+

9. Заполним таблицу "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)	(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)

Вывод

В ходе выполнения лабораторной работы №2 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.