

Ощепков Дмитрий Владимирович НКАбд-02-22

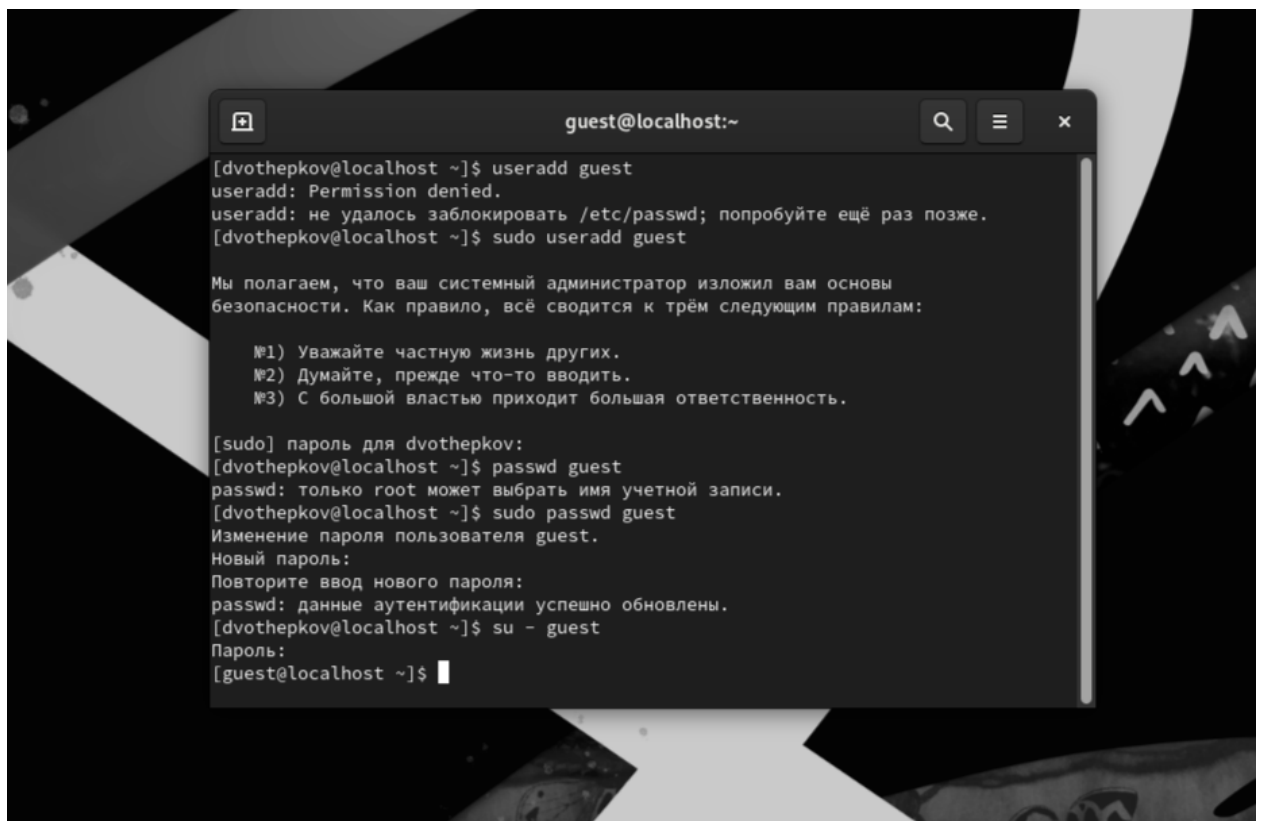
Дисциплина: Основы информационной безопасности

Лабораторная работа №2

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.

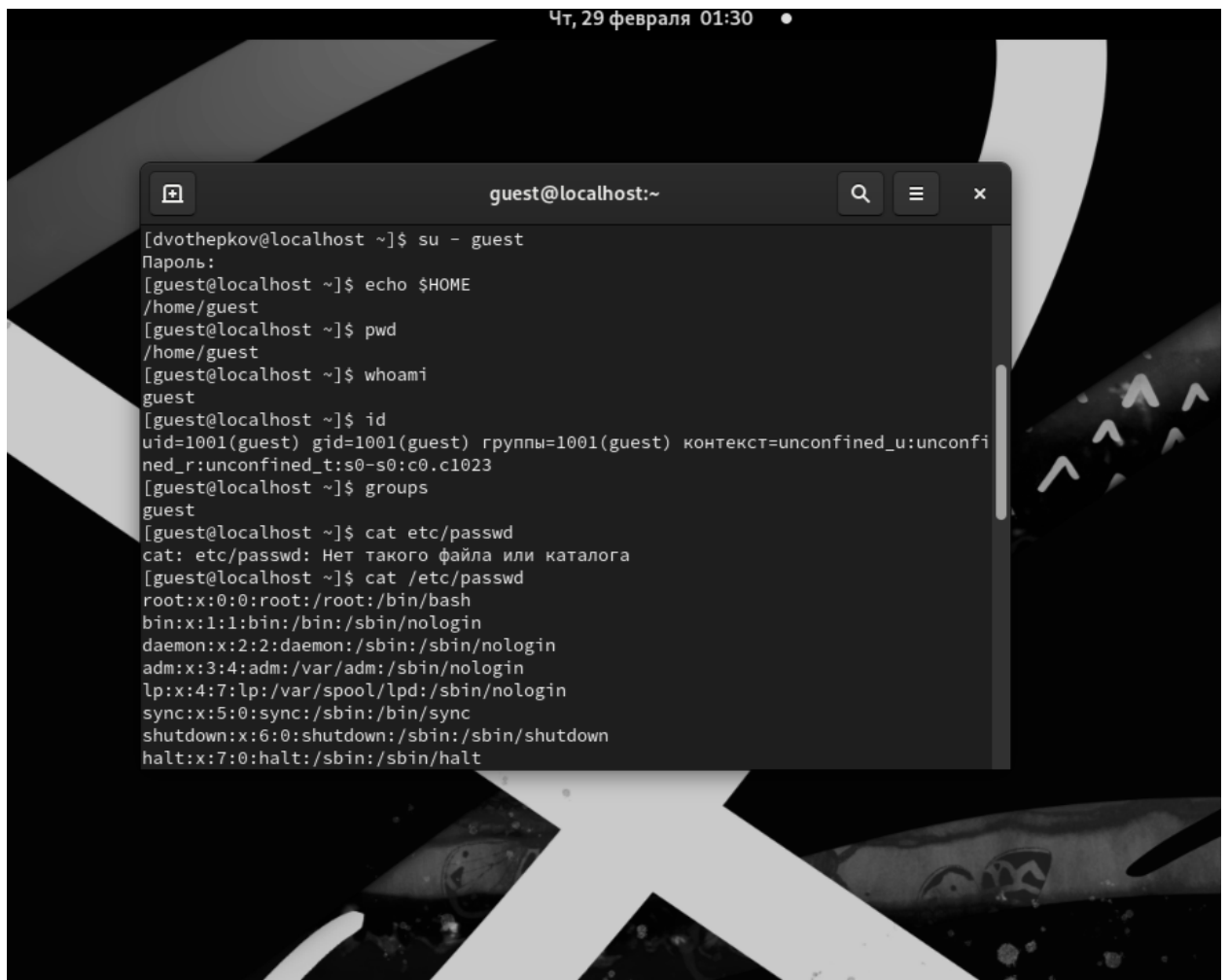
Выполнение работы:

Создал учетную запись гостю. Придумал ему пароль и зашел в его аккаунт.



```
guest@localhost:~  
[dvothepkov@localhost ~]$ useradd guest  
useradd: Permission denied.  
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.  
[dvothepkov@localhost ~]$ sudo useradd guest  
  
Мы полагаем, что ваш системный администратор изложил вам основы  
безопасности. Как правило, всё сводится к трём следующим правилам:  
  
№1) Уважайте частную жизнь других.  
№2) Думайте, прежде что-то вводить.  
№3) С большой властью приходит большая ответственность.  
  
[sudo] пароль для dvothepkov:  
[dvothepkov@localhost ~]$ passwd guest  
passwd: только root может выбрать имя учетной записи.  
[dvothepkov@localhost ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[dvothepkov@localhost ~]$ su - guest  
Пароль:  
[guest@localhost ~]$
```

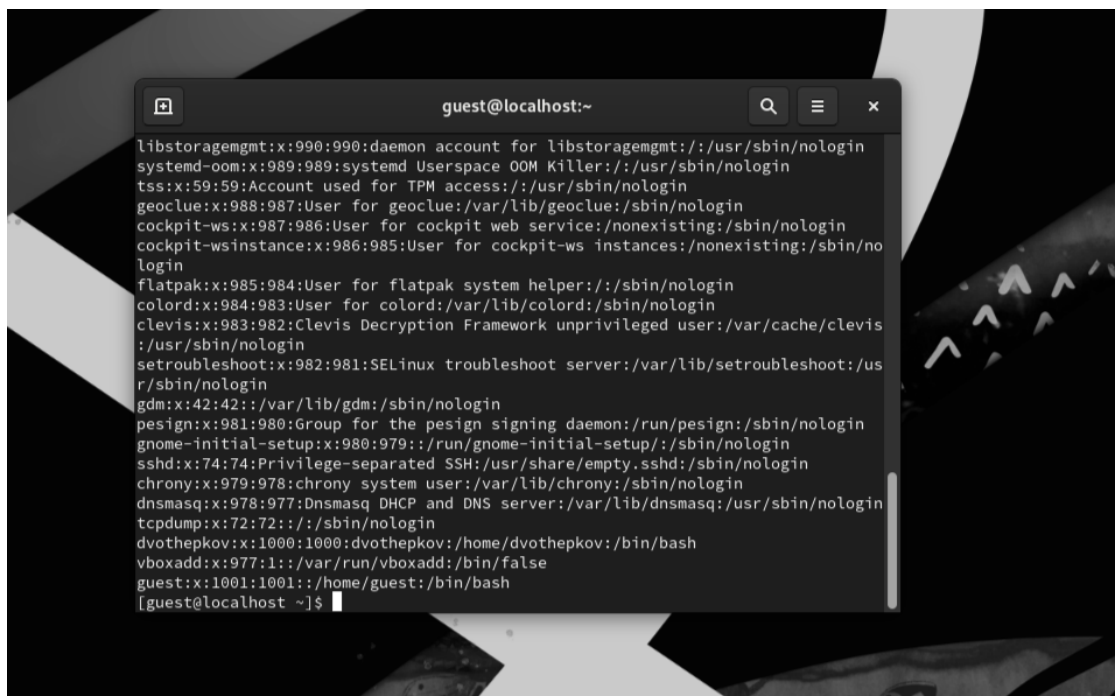
Проверил домашнюю папку гостя. Ввел команды `id` и `groups`. Посмотрел содержимое файла `passwd`



A terminal window titled 'guest@localhost:~' with a search icon, menu icon, and close button. The terminal shows the following commands and output:

```
[dvothepkov@localhost ~]$ su - guest
Пароль:
[guest@localhost ~]$ echo $HOME
/home/guest
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ whoami
guest
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ groups
guest
[guest@localhost ~]$ cat etc/passwd
cat: etc/passwd: Нет такого файла или каталога
[guest@localhost ~]$ 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
```

Содержимое файла для сверки данных



A terminal window titled 'guest@localhost:~' with a search icon, menu icon, and close button. The terminal shows the output of the `cat /etc/passwd` command:

```
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:/usr/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/no
login
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:/us
r/sbin/nologin
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
pesign:x:981:980:Group for the pesign signing daemon:/run/psign:/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:/usr/sbin/nologin
tcpdump:x:72:72:./sbin/nologin
dvothepkov:x:1000:1000:dvothepkov:/home/dvothepkov:/bin/bash
vboxadd:x:977:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@localhost ~]$
```

Посмотрел содержимое домашней директории

```
[guest@localhost ~]$ ls -l /home/  
итого 4  
drwx-----. 15 dvothepkov dvothepkov 4096 фев 29 01:06 dvothepkov  
drwx-----.  4 guest      guest      112 фев 29 01:22 guest  
[guest@localhost ~]$
```

Не смог посмотреть внешние атрибуты домашней директории

```
[guest@localhost ~]$ lsattr /home  
lsattr: Отказано в доступе While reading flags on /home/dvothepkov  
----- /home/guest  
[guest@localhost ~]$
```

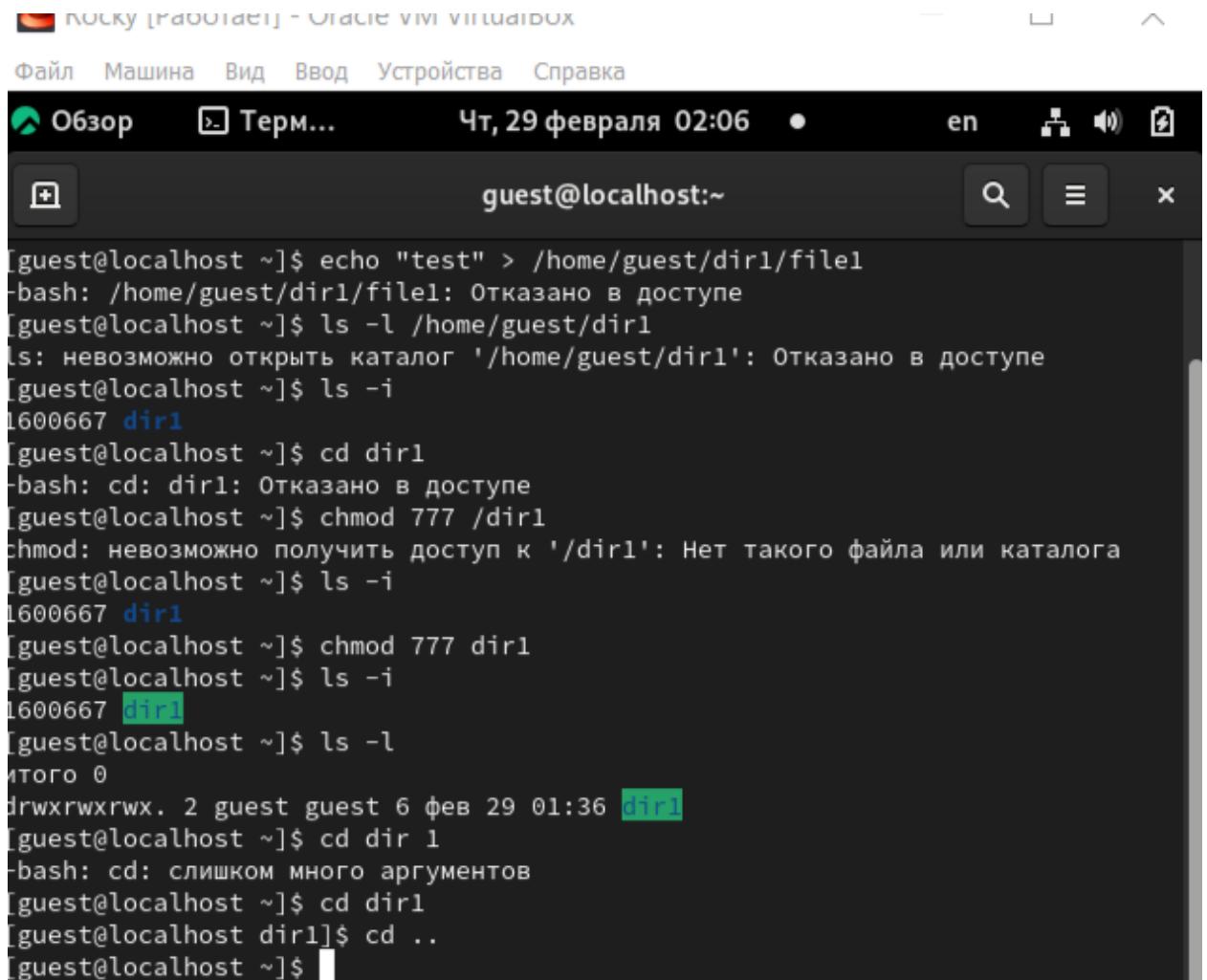
Проверил права папки dir1

```
[guest@localhost ~]$ cd dir1  
[guest@localhost dir1]$ cd ..  
[guest@localhost ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 фев 29 01:36 dir1  
[guest@localhost ~]$ ls -l lsattr
```

Отобрали все права у директории

```
guest@localhost:~  
[guest@localhost ~]$ chmod 000 dir1  
[guest@localhost ~]$ ls -l  
итого 0  
d------. 2 guest guest 6 фев 29 01:36 dir1  
[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1  
-bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@localhost ~]$ ls -l /home/guest/dir1  
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе  
[guest@localhost ~]$ ls -li  
1600667 dir1  
[guest@localhost ~]$ cd dir1  
-bash: cd: dir1: Отказано в доступе  
[guest@localhost ~]$
```

Вернули все права директории



```

[guest@localhost ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Отказано в доступе
[guest@localhost ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@localhost ~]$ ls -i
1600667 dir1
[guest@localhost ~]$ cd dir1
-bash: cd: dir1: Отказано в доступе
[guest@localhost ~]$ chmod 777 /dir1
chmod: невозможно получить доступ к '/dir1': Нет такого файла или каталога
[guest@localhost ~]$ ls -i
1600667 dir1
[guest@localhost ~]$ chmod 777 dir1
[guest@localhost ~]$ ls -i
1600667 dir1
[guest@localhost ~]$ ls -l
итого 0
drwxrwxrwx. 2 guest guest 6 фев 29 01:36 dir1
[guest@localhost ~]$ cd dir 1
-bash: cd: слишком много аргументов
[guest@localhost ~]$ cd dir1
[guest@localhost dir1]$ cd ..
[guest@localhost ~]$
```

Вывод: получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.