

# Лабораторная работа №2

## Дискреционное разграничение прав Linux

---

Гисматуллин А.В.

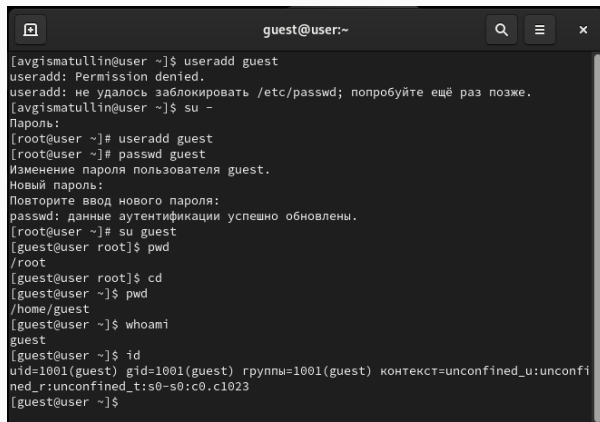
Российский университет дружбы народов, Москва, Россия

- 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

# **Процесс выполнения лабораторной работы**

---

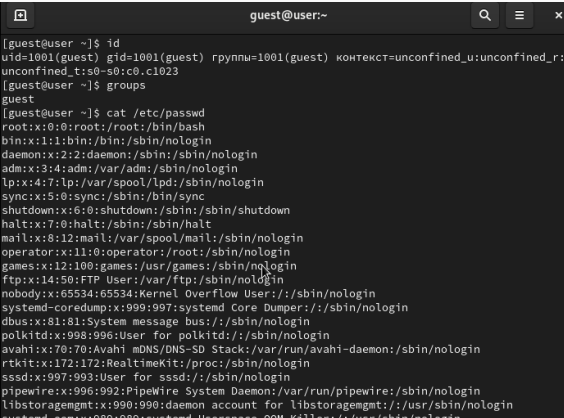
# Создание пользователя и определение его uid и группы



```
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) rpyнны=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@user ~]$
```

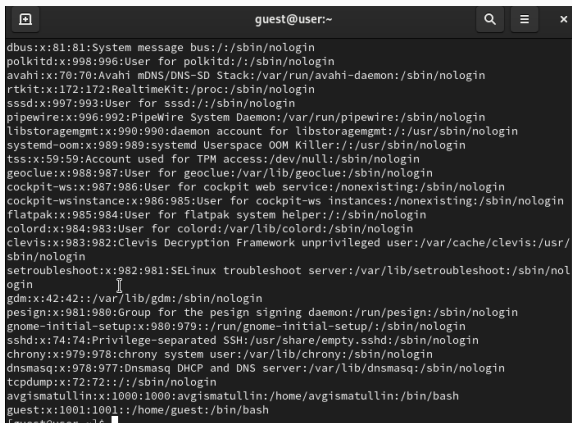
**Рис. 1:** Командная строка. Работа с пользователем

# Сравнение id и groups



```
guest@user:~  
[guest@user ~]$ id  
uid=1001(guest) gid=1001(guest) rpyнны=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-pqm:x:989:989:systemd Userspace PQM Killer:/:usr/sbin/nologin
```

Рис. 2: Командная строка. Сравнение id и groups

A terminal window titled 'guest@user:~' with search, menu, and close icons in the title bar. The terminal displays the output of the 'cat /etc/passwd' command, showing a list of system and user accounts in the format 'username:x:UID:GID:full\_name:home\_directory:shell'. The accounts listed include dbus, polkitd, avahi, rtkit, sssd, pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, cockpit-wsinstance, flatpak, colord, clevis, setroubleshoot, gdm, pesign, gnome-initial-setup, sshd, chrony, dnsmasq, tcpdump, avgismatullin, and guest. The 'guest' user is the last entry, with a home directory of /home/guest and shell /bin/bash.

```
guest@user:~  
cat /etc/passwd  
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  
[guest@user ~]$
```

Рис. 3: Командная строка. Просмотр файла /etc/passwd

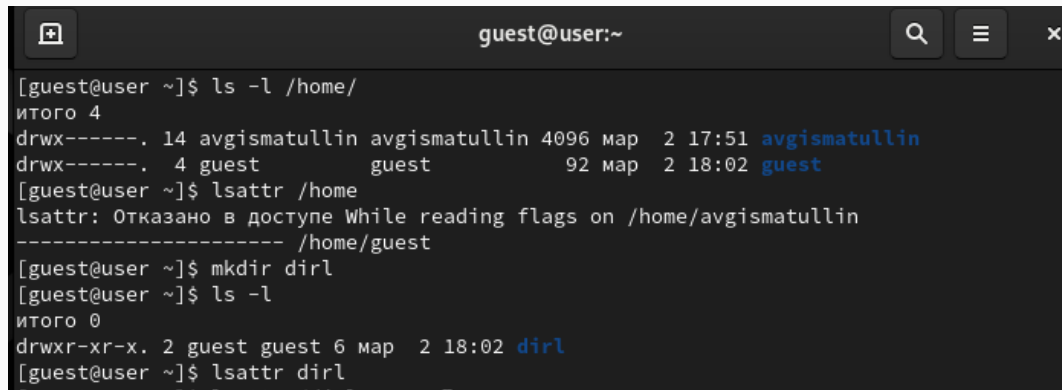
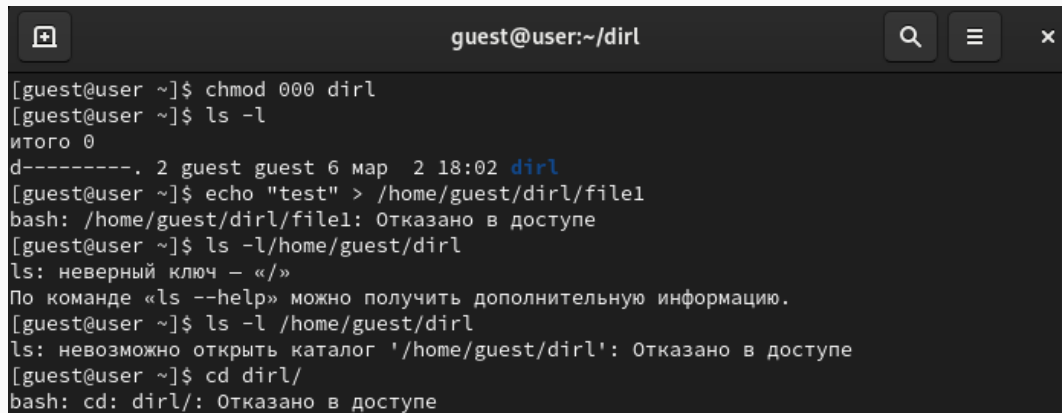
A terminal window with a dark background and light text. The title bar shows 'guest@user:~' and standard window controls. The terminal shows the execution of 'ls -l /home/' and 'lsattr /home' commands. The output of 'lsattr' shows an error for '/home/avgismatullin' and success for '/home/guest'. Finally, 'mkdir dirl' is executed, followed by 'ls -l' which shows the new directory 'dirl' with permissions 'drwxr-xr-x'.

Рис. 4: Командная строка. Команды lsattr и ls -l

## Снятие дистрибутов



```
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. 5:** Командная строка. Снятие дистрибутов для dirl



## Права на директорию и файл

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. 6: Права на директорию и файл

## **Выводы по проделанной работе**

---

## Выводы по проделанной работе

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.