

Дискреционное разграничение прав в Linux. Основные атрибуты

Алексей Горбачев¹

8 марта, 2025, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Процесс выполнения лабораторной работы

Определяем UID и группу

```
aagorbachev@aagorbachev:~$ su
Пароль:
root@aagorbachev:/home/aagorbachev# useradd guest
useradd: пользователь «guest» уже существует
root@aagorbachev:/home/aagorbachev# passwd guest
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
root@aagorbachev:/home/aagorbachev# su guest
guest@aagorbachev:/home/aagorbachev$ pwd
/home/aagorbachev
guest@aagorbachev:/home/aagorbachev$ cd
guest@aagorbachev:~$ pwd
/home/guest
guest@aagorbachev:~$ whoami
guest
guest@aagorbachev:~$ id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest)
guest@aagorbachev:~$ groups guest
guest : guest
guest@aagorbachev:~$
```

Рис. 1: Информация о пользователе guest

Файл с данными о пользователях

A terminal window titled 'guest@aagorbachev:~' with the current directory set to '/home/guest'. The window displays the output of a command that lists the contents of the /etc/passwd file. Each line represents a system or user account, showing the username, UID, GID, and the full path to the user's home directory and the shell they use. The accounts listed include various system daemons and regular users like 'guest' and 'aagorbachev'.

```
rtkit:x:172:172:RealtimeKit:/:sbin/nologin
geoclue:x:997:996:User for geoclue:/var/lib/geoclue:/sbin/nologin
sssd:x:996:995:User for sssd:/run/sss:/sbin/nologin
libstoragemgmt:x:994:994:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-coredump:x:993:993:systemd Core Dumper:/:usr/sbin/nologin
wsdd:x:992:992:Web Services Dynamic Discovery host daemon:/:sbin/nologin
clevis:x:991:991:Clevis Decryption Framework unprivileged user:/var/cache/clevis
:/:usr/sbin/nologin
setroubleshoot:x:990:990:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr
/sbin/nologin
pipewire:x:989:989:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
flatpak:x:988:988:Flatpak system helper:/:usr/sbin/nologin
gdm:x:42:42:GNOME Display Manager:/var/lib/gdm:/usr/sbin/nologin
gnome-initial-setup:x:987:986:/:run/gnome-initial-setup:/sbin/nologin
dnsmasq:x:986:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
pesign:x:985:984:Group for the design signing daemon:/run/psign:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:984:983:chrony system user:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:tcpdump:/:usr/sbin/nologin
gnome-remote-desktop:x:981:981:GNOME Remote Desktop:/var/lib/gnome-remote-deskto
p:/usr/sbin/nologin
guest:x:1001:1001:/:home/guest:/bin/bash
aagorbachev:x:1002:1002:/:home/aagorbachev:/bin/bash
guest@aagorbachev:~$
```

Рис. 2: Содержимое файла /etc/passwd

Доступ к домашним директориям

```
guest@aagorbachev:~$  
guest@aagorbachev:~$ ls -l /home  
итого 8  
drwx-----, 14 aagorbachev aagorbachev 4096 мар  8 21:01 aagorbachev  
drwx-----,  3 guest      guest      78 фев  5 19:27 guest  
drwx-----, 14          1000          1000 4096 фев  5 17:57 user  
guest@aagorbachev:~$ lsattr /home/  
lsattr: Отказано в доступе While reading flags on /home/user  
----- /home/guest  
lsattr: Отказано в доступе While reading flags on /home/aagorbachev  
guest@aagorbachev:~$
```

Рис. 3: Расширенные атрибуты

Атрибуты директории

```
guest@aagorbachev:~$  
guest@aagorbachev:~$ cd  
guest@aagorbachev:~$ mkdir dir1  
guest@aagorbachev:~$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 map 8 21:08 dir1  
guest@aagorbachev:~$ chmod 000 dir1  
guest@aagorbachev:~$ ls -l | grep dir1  
d----- . 2 guest guest 6 map 8 21:08 dir1  
guest@aagorbachev:~$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
guest@aagorbachev:~$ cd dir1  
bash: cd: dir1: Отказано в доступе  
guest@aagorbachev:~$ █
```

Рис. 4: Снятие атрибутов с директории

Права и разрешённые действия

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. 5: Минимальные права для совершения операций

Выводы по проделанной работе

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.