

# Дискреционное разграничение прав в Linux. Основные атрибуты

---

Авырал Донгак<sup>1</sup>

1 марта, 2024, Москва, Россия

<sup>1</sup>Российский 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

```
[adongak@adongak ~]$ su
Пароль:
[root@adongak adongak]# useradd guest
Создание почтового ящика: Файл существует
[root@adongak adongak]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@adongak adongak]# su guest
[guest@adongak adongak]$
[guest@adongak adongak]$ pwd
/home/adongak
[guest@adongak adongak]$ cd
[guest@adongak ~]$ pwd
/home/guest
[guest@adongak ~]$ whoami
guest
[guest@adongak ~]$ id
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfined_r:guest_t:s0
[guest@adongak ~]$ groups
guest
[guest@adongak ~]$ █
```

**Figure 1:** Информация о пользователе guest

# Файл с данными о пользователях

```
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:/nonexistent:/sbin/nologin
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexistent:/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/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:981:980::/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
adongak:x:1000:1000:/home/adongak:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash
[guest@adongak ~]$
```

Figure 2: Содержимое файла /etc/passwd

# Доступ к домашним директориям

```
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
adongak:x:1000:1000::/home/adongak:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@adongak ~]$
[guest@adongak ~]$
[guest@adongak ~]$ ls -l /home
итого 4
drwx-----. 14 adongak adongak 4096 map 1 16:06 adongak
drwx-----. 3 guest guest 78 map 1 16:14 guest
[guest@adongak ~]$
```

Figure 3: Расширенные атрибуты

# Атрибуты директории

```
[guest@adongak ~]$  
[guest@adongak ~]$ cd  
[guest@adongak ~]$ mkdir dir1  
[guest@adongak ~]$ ls -l  
итого 0  
drwxr-xr-x. 2 guest guest 6 map 1 16:18 dir1  
[guest@adongak ~]$ chmod 000 dir1  
[guest@adongak ~]$ ls -l  
итого 0  
d-----, 2 guest guest 6 map 1 16:18 dir1  
[guest@adongak ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@adongak ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@adongak ~]$
```

**Figure 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)

**Figure 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.