

Лабораторная работа № 3

Дискреционное разграничение прав в Linux.
Два пользователя

Миленин Иван Витальевич

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

Задание

Провести эксперимент по выявлению минимально необходимых прав для совершения различных действий для групп пользователей.

Теоретическое описание

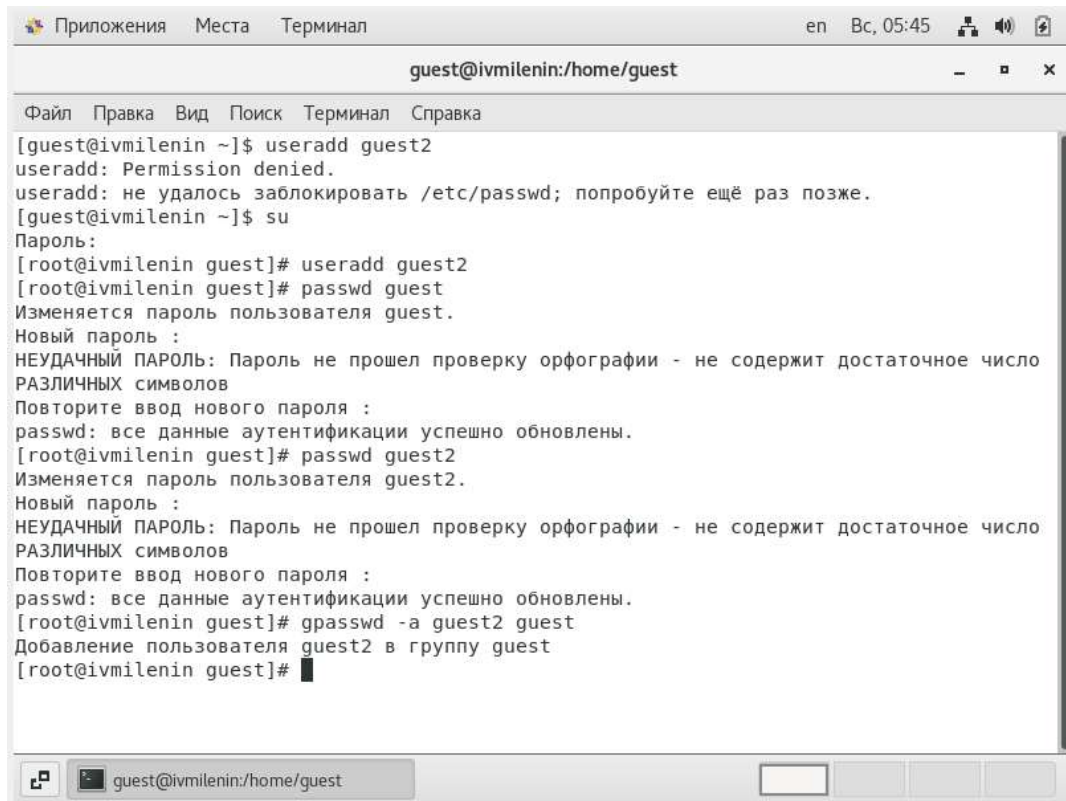
В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

Изначально каждый файл имел три параметра доступа [1]:

- Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;

Ход работы

1. Создаем в ОС двух новых пользователей guest и guest2. Так как первый у нас уже был, нам нужен всего один. Задаем ему пароль и добавляем его в группу guest (иллюстр. [-@fig:001]). Командой pwd проверяем местонахождение консоли. Видим, что guest находится в своей домашней директории, о чем свидетельствует значок тильда в приглашении командной строки (иллюстр. [-@fig:002]). Guest2 же находится в той же папке, однако для него она не домашняя, что показывает нам имя пользователя-владельца папки в приглашении командной строки (иллюстр. [-@fig:003]).

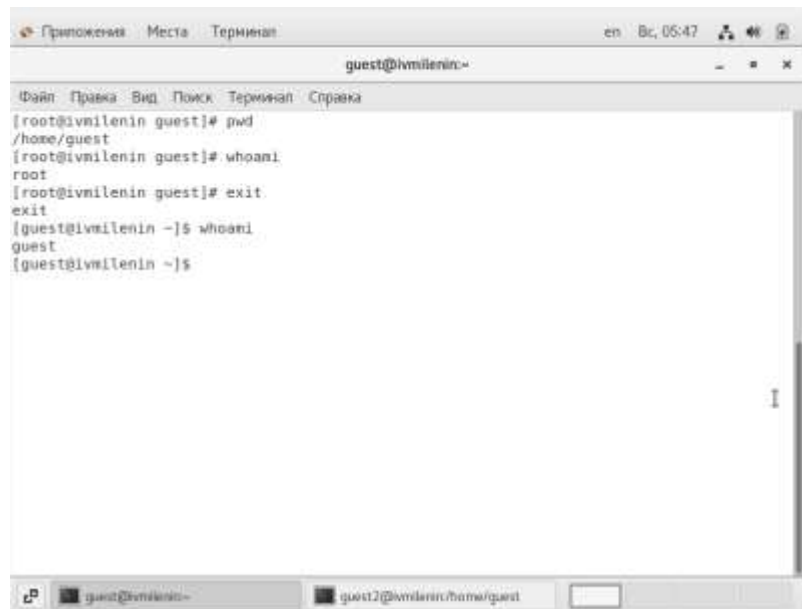


```
guest@ivmilenin:/home/guest

Файл  Правка  Вид  Поиск  Терминал  Справка

[guest@ivmilenin ~]$ useradd guest2
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[guest@ivmilenin ~]$ su
Пароль:
[root@ivmilenin guest]# useradd guest2
[root@ivmilenin guest]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - не содержит достаточное число
РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@ivmilenin guest]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - не содержит достаточное число
РАЗЛИЧНЫХ символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@ivmilenin guest]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@ivmilenin guest]#
```

Добавление нового пользователя



The screenshot shows a terminal window titled "guest@ivmlenin:~". The window has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The status bar at the top right shows "en", "Вт, 05:47", and system icons. The terminal content shows the following sequence of commands and outputs:

```
guest@ivmlenin:~  
[root@ivmlenin guest]# pwd  
/home/guest  
[root@ivmlenin guest]# whoami  
root  
[root@ivmlenin guest]# exit  
exit  
[guest@ivmlenin ~]$ whoami  
guest  
[guest@ivmlenin ~]$
```

The terminal window has a scrollbar on the right side. At the bottom, there are two tabs: "guest@ivmlenin:~" and "guest2@ivmlenin:/home/guest".

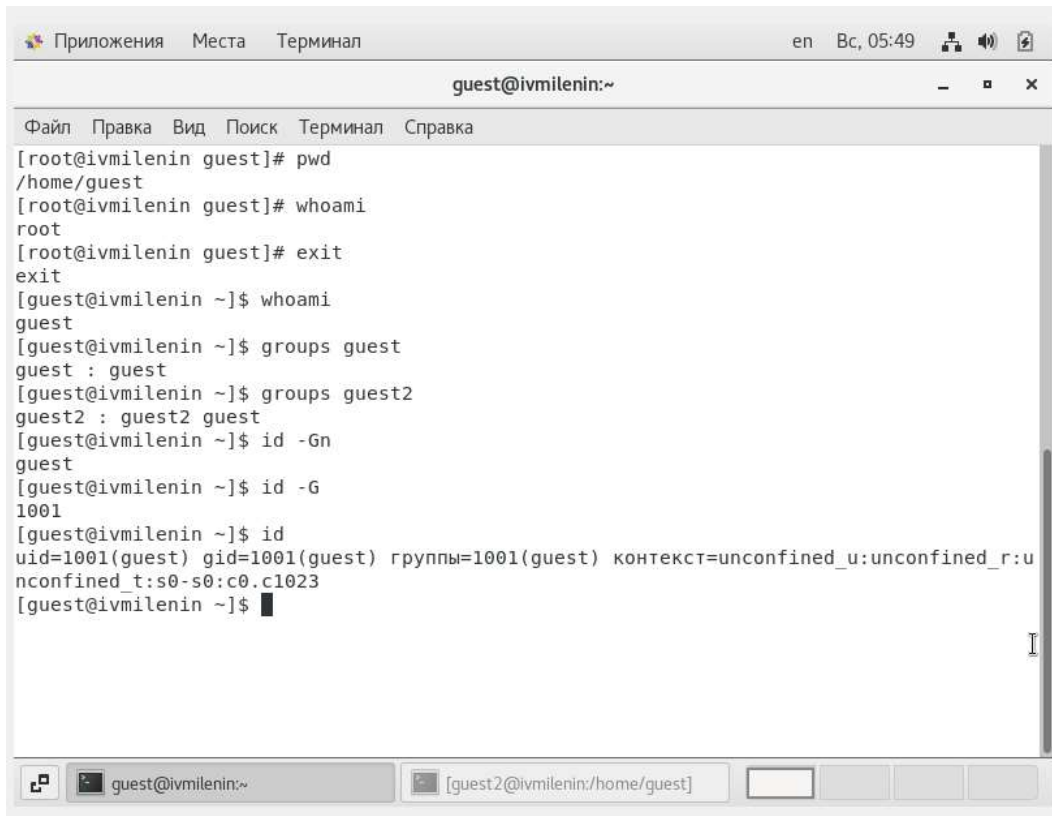
pwd для guest



```
guest2@ivmilenin:/home/guest
Файл Правка Вид Поиск Терминал Справка
[guest@ivmilenin ~]$ su guest2
Пароль:
[guest2@ivmilenin guest]$ pwd
/home/guest
[guest2@ivmilenin guest]$ whoami
guest2
[guest2@ivmilenin guest]$
```

pwd для guest2

2. Проверяем командами `id`, `id -G`, `id -Gn` и `groups` к каким группам принадлежат пользователи. Видим, что `guest` входит только в группу `guest`, а `guest2` входит и в группу `guest`, и в группу `guest2` (иллюстр. [-@fig:004], [-@fig:005]).



```
Приложения  Места  Терминал  en  Вс, 05:49  [иконки]
guest@ivmilenin:~

Файл  Правка  Вид  Поиск  Терминал  Справка
[root@ivmilenin guest]# pwd
/home/guest
[root@ivmilenin guest]# whoami
root
[root@ivmilenin guest]# exit
exit
[guest@ivmilenin ~]$ whoami
guest
[guest@ivmilenin ~]$ groups guest
guest : guest
[guest@ivmilenin ~]$ groups guest2
guest2 : guest2 guest
[guest@ivmilenin ~]$ id -Gn
guest
[guest@ivmilenin ~]$ id -G
1001
[guest@ivmilenin ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0.c1023
[guest@ivmilenin ~]$
```

Группы для guest

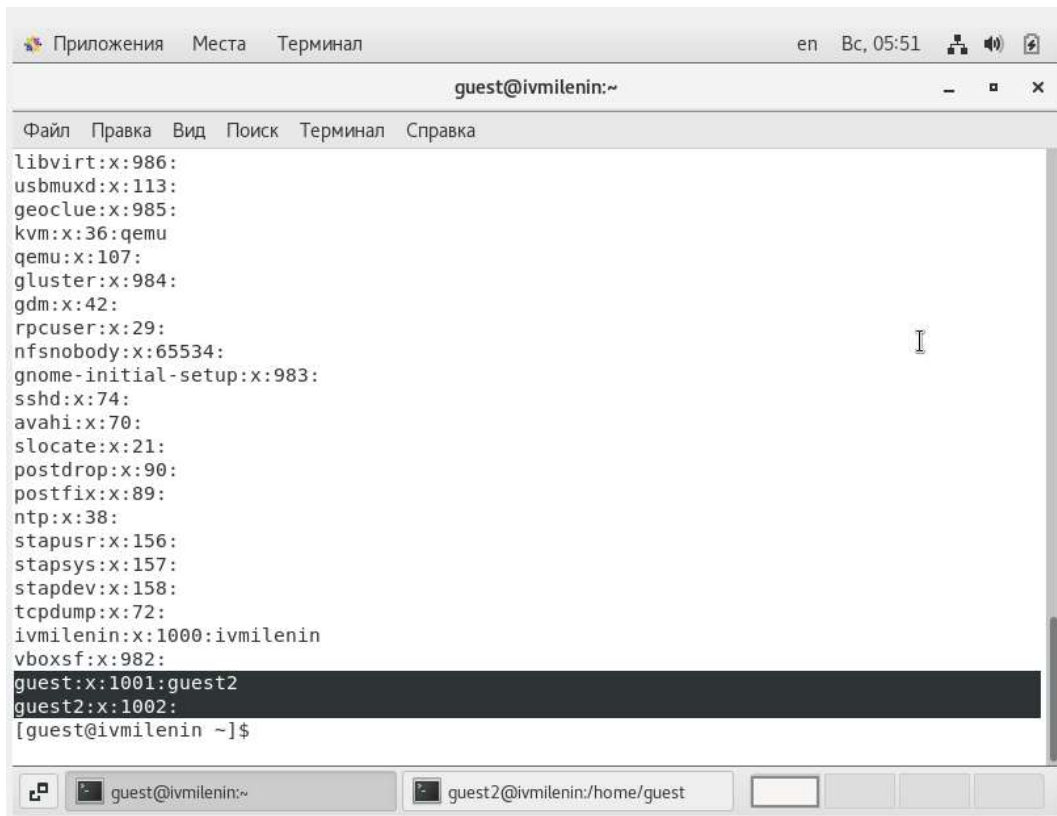
The screenshot shows a terminal window titled "guest2@ivmlenin:/home/guest". The user is logged in as "guest2" and is in the directory "/home/guest". The terminal shows the following commands and output:

```
[guest@ivmlenin ~]$ su guest2
Пароль:
[guest2@ivmlenin guest]$ pwd
/home/guest
[guest2@ivmlenin guest]$ whoami
guest2
[guest2@ivmlenin guest]$ groups guest
guest : guest
[guest2@ivmlenin guest]$ groups guest2
guest2 : guest2 guest
[guest2@ivmlenin guest]$ id -Gn
guest2 guest
[guest2@ivmlenin guest]$ id -G
1002 1001
[guest2@ivmlenin guest]$ id
uid=1002(guest2) gid=1002(guest2) rpynm=1002(guest2),1001(guest) контекст=unconfined_u
:unconfined :unconfined t:s0:s0:c8:c1023
[guest2@ivmlenin guest]$
```

The terminal window has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The status bar at the bottom shows the current directory and the user's name.

Группы для guest2

3. Информация в файле `/etc/groups` так же соответствует полученным прежде данным, а именно `guest` в группе `guest`, а `guest2` в группах `guest` и `guest2` (иллюстр. [-@fig:006]). Регистрируем пользователя `guest2` в группе `guest` (иллюстр. [-@fig:007]).



```
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
kvm:x:36:qemu
qemu:x:107:
gluster:x:984:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
avahi:x:70:
slocate:x:21:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
stapusr:x:156:
stapusr:x:157:
stapdev:x:158:
tcpdump:x:72:
ivmilenin:x:1000:ivmilenin
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
[guest@ivmilenin ~]$
```

`/etc/groups`

```
[guest2@ivmilenin guest]$ newgrp guest  
[guest2@ivmilenin guest]$
```

Регистрация guest2

4. Изменяем права директории `/home/guest`, разрешив все действия для пользователей группы (иллюстр. [-@fig:008]). Снимаем все права с `dir1` (иллюстр. [-@fig:009]).

```
avahi:x:70:
slocate:x:21:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
tcpdump:x:72:
ivmilenin:x:1000:ivmilenin
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
[guest@ivmilenin ~]$ clear

[guest@ivmilenin ~]$ chmod g+rw /home/guest
```

Разрешение на домашнюю папку guest

```

[guest@ivmilenin ~]$ chmod 000 dir1
[guest@ivmilenin ~]$ ls -l
итого 0
d----- . 2 guest guest 19 фев 13 03:41 dir1
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Видео
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Документы
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Загрузки
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Изображения
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Музыка
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Общедоступные
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Рабочий стол
drwxr-xr-x. 2 guest guest 6 фев 13 02:41 Шаблоны
[guest@ivmilenin ~]$ cd home/
bash: cd: home/: Нет такого файла или каталога
[guest@ivmilenin ~]$ cd
[guest@ivmilenin ~]$ cd
[guest@ivmilenin ~]$ ls
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка      Рабочий стол
[guest@ivmilenin ~]$

```

I

Нулевые права на dir1

5. Следующим шагом проведем эксперимент по выявлению минимально необходимых прав для действий над файловой структурой. Для этого используем нашу папку dir1, файлы внутри неё и функционал прав доступа ОС Linux. Для каждой комбинации атрибутов доступа (r, w, x) на папку и на файл попробуем осуществить ряд действий и таким образом выявим минимально необходимые права для каждого действия. Атрибуты используем только для группы, поэтому комбинаций будет $2^3 \cdot 2^3 = 2^6 = 64$. В каждой строчке будет по 8 действий. Проверять осуществимость функции будем следующими командами:

touch для создания файла в директории;

rm для удаления файла в директории;

echo для записи в файл;

cat для чтения из файла;

mv для переименования файла;

chattr для изменения атрибутов файла;

cd для смены директории;

ls для просмотра файлов в директории;

```
[guest@ivmilenin dirl]$ chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
[guest@ivmilenin dirl]$ lsattr /home/guest/dirl/file1
----- /home/guest/dirl/file1
[guest@ivmilenin dirl]$ chmod 000 file1
[guest@ivmilenin dirl]$ mv file1 file2
[guest@ivmilenin dirl]$ mv file2 file1
[guest@ivmilenin dirl]$ cat file1
```

Пример ввода команд для проверки прав

Табличка (иллюстр. [-@fig:0011]).

[illegible]

таблица

Таблица прав из данной работы и аналогичная таблица из предыдущей весьма похожи и имеют четкие аналогии. Тем не менее, различия также присутствуют.

На основе данных полученной выше таблицы построим вторую таблицу, иллюстрирующую минимально необходимые права для совершения определенных операций.

Операция	Мин. права на директорию	Мин. права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	-
Удаление поддиректории	030	-

Выводы

В ходе работы мы успешно провели эксперимент по выявлению минимально необходимых прав для действий над файловой структурой и получили ряд практических навыков работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Права доступа к файлам в linux. // Losst. 2020. URL: <https://losst.ru/prava-dostupa-k-fajlam-v-linux> (дата обращения 11.10.2021).
2. Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask). // habr.com. 2019. URL: <https://habr.com/ru/post/469667/> (дата обращения 11.10.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-