

Операционные системы и виртуализация (Linux) (семинары)

Права доступа и безопасность

- [Операционные системы и виртуализация \(Linux\) \(семинары\)](#)
- [Права доступа и безопасность](#)
 - [Задание](#)
 - [Назначение доступов к файлам](#)
 - [Управление пользователями](#)

Задание

Создать два произвольных файла. Первому присвоить права на чтение и запись для владельца и группы, только на чтение — для всех. Второму присвоить права на чтение и запись только для владельца. Сделать это в численном и символьном виде. Назначить нового владельца и группу для директории целиком.

Управление пользователями:

- создать пользователя, используя утилиту `useradd` и `adduser`;
- удалить пользователя, используя утилиту `userdel`. Управление группами:
- создать группу с использованием утилит `groupadd` и `addgroup`;
- попрактиковаться в смене групп у пользователей;
- добавить пользователя в группу, не меняя основной; Создать пользователя с правами суперпользователя. Сделать так, чтобы `sudo` не требовал пароль для выполнения команд.

Дополнительные (необязательные) задания:

- Используя дополнительные материалы, выдать одному из созданных пользователей право на выполнение ряда команд, требующих прав суперпользователя (команды выбираем на своё усмотрение).
- Создать группу `developer` и нескольких пользователей, входящих в неё. Создать директорию для совместной работы. Сделать так, чтобы созданные одними пользователями файлы могли изменять другие пользователи этой группы.
- Создать в директории для совместной работы поддиректорию для обмена файлами, но чтобы удалять файлы могли только их создатели.
- Создать директорию, в которой есть несколько файлов. Сделать так, чтобы открыть файлы можно было, только зная имя файла, а через `ls` список файлов посмотреть было нельзя.

Результат: Текст команд, которые применялись при выполнении задания. Присылаем в формате текстового документа: задание и команды для решения (без вывода). Формат - PDF (один файл на все задания).

Назначение доступов к файлам

```
joker@joker-vbox: ~/hw_03
joker@joker-vbox:~/hw_03$ touch file1 file2
joker@joker-vbox:~/hw_03$ ll
итого 8
drwxrwxr-x  2 joker joker 4096 янв 23 15:51 ./
drwxr-x--- 19 joker joker 4096 янв 23 15:50 ../
-rw-rw-r--  1 joker joker   0 янв 23 15:51 file1
-rw-rw-r--  1 joker joker   0 янв 23 15:51 file2
joker@joker-vbox:~/hw_03$
```

Присвоим права доступа на file1 - чтение и запись для владельца и группы, только чтение — для остальных

```
joker@joker-vbox: ~/hw_03
joker@joker-vbox:~/hw_03$ touch file1 file2
joker@joker-vbox:~/hw_03$ ll
итого 8
drwxrwxr-x  2 joker joker 4096 янв 23 15:51 ./
drwxr-x--- 19 joker joker 4096 янв 23 15:50 ../
-rw-rw-r--  1 joker joker   0 янв 23 15:51 file1
-rw-rw-r--  1 joker joker   0 янв 23 15:51 file2
joker@joker-vbox:~/hw_03$ chmod u=rw,g=rw,o=r file1
joker@joker-vbox:~/hw_03$
```

Права доступа на файл file2 права на чтение и запись только для владельца

```
joker@joker-vbox: ~/hw_03
joker@joker-vbox:~/hw_03$ chmod u=rw,g=-,o=- file2
joker@joker-vbox:~/hw_03$ ll
итого 8
drwxrwxr-x  2 joker joker 4096 янв 23 15:51 ./
drwxr-x--- 19 joker joker 4096 янв 23 15:50 ../
-rw-rw-r--  1 joker joker   0 янв 23 15:51 file1
-rw-----  1 joker joker   0 янв 23 15:51 file2
joker@joker-vbox:~/hw_03$
```

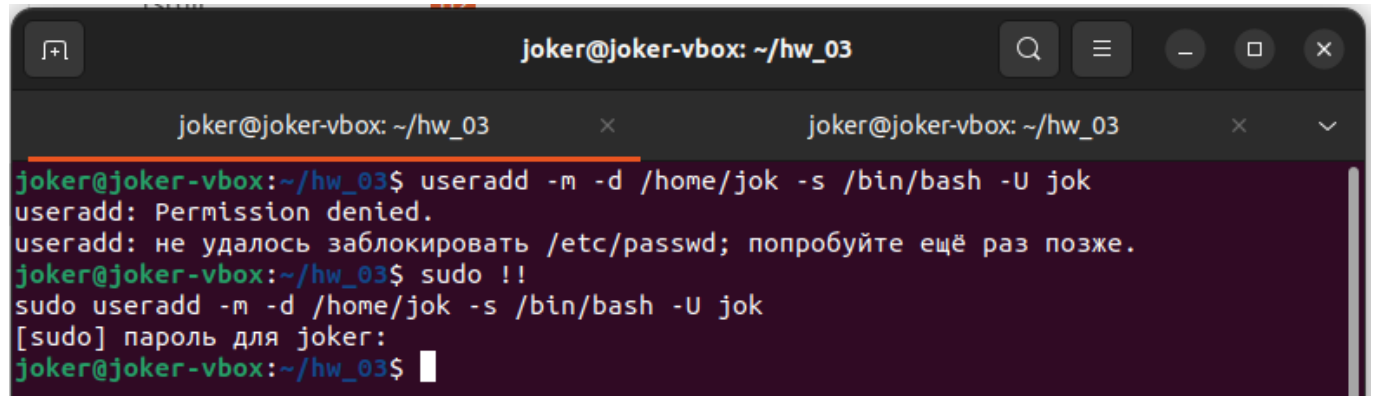
Вернем права rw для всех пользователей обоим файлам, повторим те же операции в числовом формате

```
joker@joker-vbox: ~/hw_03
joker@joker-vbox: ~/hw_03
joker@joker-vbox:~/hw_03$ chmod a=rw file1 file2
joker@joker-vbox:~/hw_03$ ll
итого 8
drwxrwxr-x  2 joker joker 4096 янв 23 15:51 ./
drwxr-x--- 19 joker joker 4096 янв 23 15:50 ../
-rw-rw-rw-  1 joker joker   0 янв 23 15:51 file1
-rw-rw-rw-  1 joker joker   0 янв 23 15:51 file2
joker@joker-vbox:~/hw_03$ chmod 664 file1
joker@joker-vbox:~/hw_03$ chmod 600 file2
joker@joker-vbox:~/hw_03$ ll
итого 8
drwxrwxr-x  2 joker joker 4096 янв 23 15:51 ./
drwxr-x--- 19 joker joker 4096 янв 23 15:50 ../
-rw-rw-r--  1 joker joker   0 янв 23 15:51 file1
-rw-----  1 joker joker   0 янв 23 15:51 file2
joker@joker-vbox:~/hw_03$
```

Управление пользователями

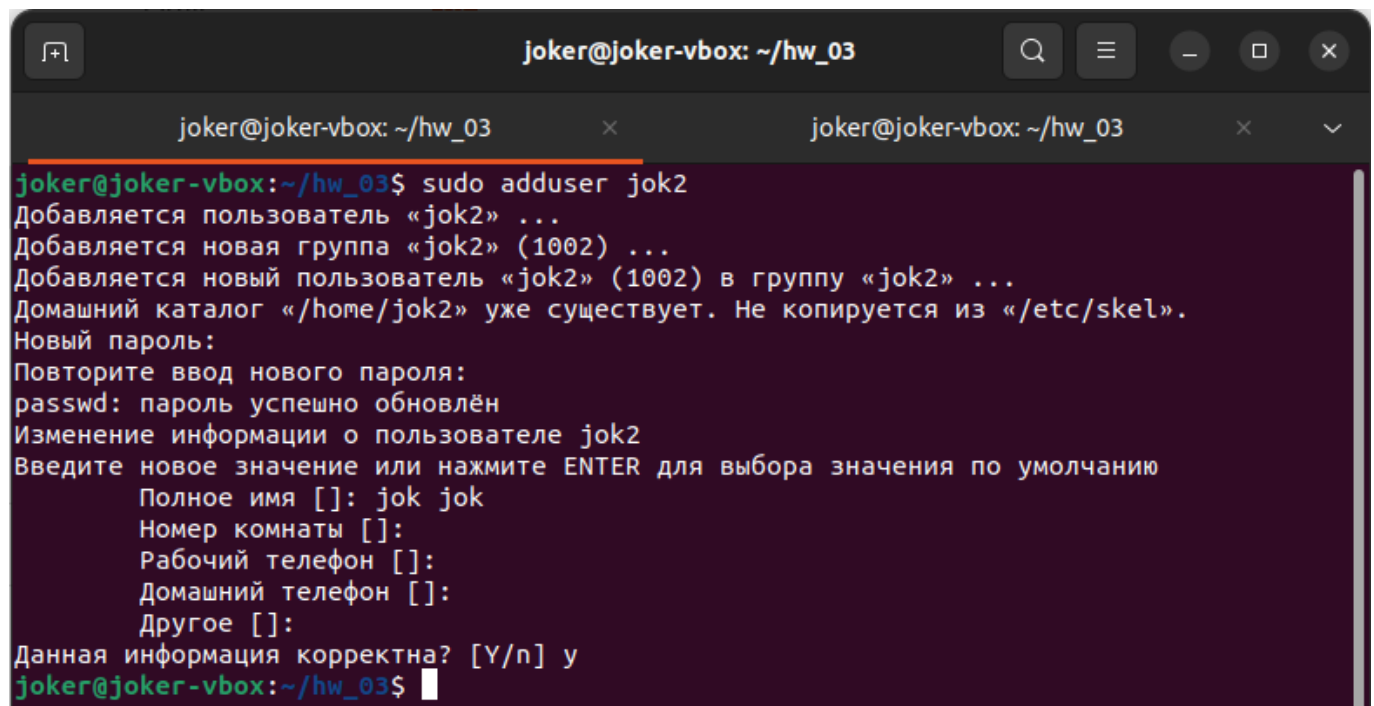
Создание пользователя командой `useradd`.

Создадим нового пользователя `jok` с указанием домашнего каталога, оболочки и одновременным созданием одноименной группы.



```
joker@joker-vbox: ~/hw_03
joker@joker-vbox: ~/hw_03
joker@joker-vbox:~/hw_03$ useradd -m -d /home/jok -s /bin/bash -U jok
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
joker@joker-vbox:~/hw_03$ sudo !!
sudo useradd -m -d /home/jok -s /bin/bash -U jok
[sudo] пароль для joker:
joker@joker-vbox:~/hw_03$
```

Создадим пользователя `jok2` при помощи `adduser`



```
joker@joker-vbox: ~/hw_03
joker@joker-vbox: ~/hw_03
joker@joker-vbox:~/hw_03$ sudo adduser jok2
Добавляется пользователь «jok2» ...
Добавляется новая группа «jok2» (1002) ...
Добавляется новый пользователь «jok2» (1002) в группу «jok2» ...
Домашний каталог «/home/jok2» уже существует. Не копируется из «/etc/skel».
Новый пароль:
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
Изменение информации о пользователе jok2
Введите новое значение или нажмите ENTER для выбора значения по умолчанию
    Полное имя []: jok jok
    Номер комнаты []:
    Рабочий телефон []:
    Домашний телефон []:
    Другое []:
Данная информация корректна? [Y/n] y
joker@joker-vbox:~/hw_03$
```

Просмотрим информацию о пользователях

```
joker@joker-vbox: ~/hw_03

joker@joker-vbox: ~/hw_03

joker@joker-vbox:~/hw_03$ tail /etc/passwd
gnome-initial-setup:x:125:65534::/run/gnome-initial-setup:/bin/false
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
joker:x:1000:1000:joker,,,:/home/joker:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
postgres:x:129:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
fwupd-refresh:x:130:137:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
jok:x:1001:1001::/home/jok:/bin/bash
jok2:x:1002:1002:jok jok,,,:/home/jok2:/bin/bash
joker@joker-vbox:~/hw_03$
```

Удалим пользователя jok2

```
joker@joker-vbox: ~

joker@joker-vbox:~$ sudo userdel -r jok2
userdel: почтовый ящик jok2 (/var/mail/jok2) не найден
joker@joker-vbox:~$ sudo tail /etc/passwd
pulse:x:124:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:65534::/run/gnome-initial-setup:/bin/false
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
joker:x:1000:1000:joker,,,:/home/joker:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
postgres:x:129:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
fwupd-refresh:x:130:137:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
jok:x:1001:1001::/home/jok:/bin/bash
joker@joker-vbox:~$ ll /home
итого 16
drwxr-xr-x  4 root  root  4096 янв 24 11:21 ./
drwxr-xr-x 20 root  root  4096 янв 13 09:40 ../
drwxr-x---  2 jok   jok   4096 янв 23 16:51 jok/
drwxr-x--- 19 joker joker 4096 янв 24 11:08 joker/
joker@joker-vbox:~$ _
```

Создадим группы пользователей group1 и group2

```
joker@joker-vbox: ~

joker@joker-vbox:~$ sudo addgroup group1
[sudo] пароль для joker:
Добавляется группа «group1» (GID 1003) ...
Готово.
joker@joker-vbox:~$ groupadd group2
groupadd: Permission denied.
groupadd: не удалось заблокировать /etc/group; попробуйте ещё раз позже.
joker@joker-vbox:~$ sudo !!
sudo groupadd group2
joker@joker-vbox:~$ _
```

отобразим список последних созданных групп в системе

```
joker@joker-vbox: ~  
joker@joker-vbox:~$ sudo tail /etc/group  
lxd:x:134:joker  
joker:x:1000:  
sambashare:x:135:joker  
vboxsf:x:999:  
vboxdrmpc:x:998:  
postgres:x:136:  
fwupd-refresh:x:137:  
jok:x:1001:  
group1:x:1003:  
group2:x:1004:  
joker@joker-vbox:~$ _
```

Добавим пользователя jok группу group1

```
joker@joker-vbox: ~  
joker@joker-vbox:~$ sudo usermod -aG group1 jok  
joker@joker-vbox:~$ sudo group jok  
sudo: group: команда не найдена  
joker@joker-vbox:~$ sudo groups jok  
jok : jok group1  
joker@joker-vbox:~$
```

Сменим основную группу пользователю jok на group2

```
joker@joker-vbox: ~  
joker@joker-vbox:~$ sudo usermod -g group2 jok  
joker@joker-vbox:~$ sudo groups jok  
jok : group2 group1  
joker@joker-vbox:~$
```

Уберем запрос пароля для sudo этого откроем для редактирования sudoers командой `sudo visudo` и внесем следующие изменения для группы sudo

```
joker@joker-vbox: ~
GNU nano 6.2 /etc/sudoers.tmp *

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) NOPASSWD:ALL

# See sudoers(5) for more information on "@include" directives:

@include /etc/sudoers.d

^G Справка      ^O Записать     ^W Поиск       ^K Вырезать    ^T Выполнить   ^C Позиция
^X Выход        ^R ЧитФайл     ^\ Замена      ^U Вставить    ^J Выровнять   ^_ К строке
```