

## Лабораторная работа №2

---

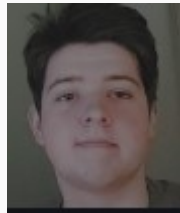
Артём Дмитриевич Петлин

1970-01-01



## 1.1 Докладчик

- Петлин Артём Дмитриевич
- студент
- группа НПИбд-02-24
- Российский университет дружбы народов
- 1132246846@pfur.ru
- [https://github.com/hikrim/study\\_2025-2026\\_os2](https://github.com/hikrim/study_2025-2026_os2)



## 2. Цель работы

Получить представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

### 3. Задание

1. Находясь под учётной записью пользователя `alice`, создайте группы `main` и `third`:  
`sudo groupadd main sudo groupadd third`
2. Используйте `usermod` для добавления пользователей `alice` и `bob` в группу `main`, а `carol`, `dan`, `dave` и `david` — в группу `third`:  
`sudo usermod -aG main alice sudo usermod -aG main bob sudo usermod -aG third carol`
3. Убедитесь, что пользователь `carol` правильно добавлен в группу `third`:  
`id carol`  
Пользователю `carol` должна быть назначена основная группа с идентификатором `gid = 100 (users)`. Определите, в какие вторичные группы входит `carol`.
4. Определите, участниками каких групп являются другие созданные вами пользователи. Укажите эту информацию в отчёте.

## 4. Теоретическое введение

В операционных системах типа Linux чаще всего применяется дискреционное управление доступом субъектов к объектам системы. В качестве субъектов системы чаще всего выступают пользователи или группы пользователей, а в качестве объектов — файлы (в том числе системные), каталоги, устройства и т.п. В качестве особого субъекта выделяется суперпользователь (пользователь root), имеющий право устанавливать права владения для всех остальных субъектов системы. Под доступом к ресурсу системы понимают чтение (read), запись (write) и выполнение (execute). Тот или иной тип доступа может быть применён к пользователю и/или группе, владеющими тем или иным ресурсом операционной системы, а также ко всем остальным субъектам, не являющимся владельцами ресурса.

## 5. Выполнение лабораторной работы

```
adpetlin@adpetlin:~$ whoami
adpetlin
adpetlin@adpetlin:~$ id
uid=1000(adpetlin) gid=1000(adpetlin) groups=1000(adpetlin),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
adpetlin@adpetlin:~$ su
Password:
root@adpetlin:/home/adpetlin# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рисунок 1: whoami

Входим в систему как обычные пользователи и открываем терминал. Определяем, какую учётную запись мы используем, вводя команду **whoami**. Выводим на экран более подробную информацию, используя команду **id**. Используем команду **su** для переключения к учётной записи **root**. При запросе пароля вводим пароль пользователя **root**. Набираем **id**.

## 6. Ход работы

Просматриваем в безопасном режиме файл `/etc/sudoers`, используя `sudo -i visudo`. Используем `visudo` так как он не даст потерять весь механизм `sudo`, лишив всех пользователей возможности получать права суперпользователя (включая `root`).

```
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias    FILESERVERS = fs1, fs2
# Host_Alias    MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias    ADMINS = jsmith, mikem
```

Рисунок 2: `/etc/sudoers`



```
## Allows people in group wheel to run all commands  
%wheel  ALL=(ALL)        ALL
```

Рисунок 3: %wheel

Убеждаемся, что в открытом с помощью **visudo** файле присутствует строка **%wheel ALL=(ALL) ALL**. Все пользователи входящие в группу wheel, могут выполнять любые команды на этом компьютере, получая права любого пользователя, предварительно введя свой собственный пароль.

```
adpetlin@adpetlin:~$ sudo -i useradd -G wheel alice
[sudo] password for adpetlin:
adpetlin@adpetlin:~$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel)
```

Рисунок 4: alice

Создаём пользователя **alice**, входящего в группу **wheel**. Убеждаемся, что пользователь **alice** добавлен в группу **wheel**, введя **id alice**.

```
adpetlin@adpetlin:~$ sudo -i passwd alice
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
adpetlin@adpetlin:~$
```

Рисунок 5: alice passwd

Задаём пароль для пользователя `alice`.

Переключаемся на учётную  
запись пользователя  
**alice**. Создаём  
пользователя **bob**

```
alice@adpetlin:/home/adpetlin$ sudo useradd bob
```

```
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:
```

```
#1) Respect the privacy of others.
```

```
#2) Think before you type.
```

```
#3) With great power comes great responsibility.
```

```
For security reasons, the password you type will not be visible.
```

```
[sudo] password for alice:
```

Рисунок 6: su alice

## 11. Ход работы

```
alice@adpetlin:/home/adpetlin$ sudo passwd bob
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: password updated successfully
alice@adpetlin:/home/adpetlin$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob)
alice@adpetlin:/home/adpetlin$
```

Рисунок 7: bob passwd

Устанавливаем пароль для пользователя **bob**. Просматриваем, в какие группы входит пользователь **bob**.



```
CREATE_HOME          yes
```

Рисунок 8: /etc/login.defs

Переключаемся в терминале на учётную запись пользователя **root**. Открываем файл конфигурации **/etc/login.defs** для редактирования, используя, например, **vim**. Изменяем несколько параметров. Например, находим параметр **CREATE\_HOME** и убеждаемся, что он установлен в значение **yes**. Также устанавливаем параметр **USERGROUPS\_ENAB no**.

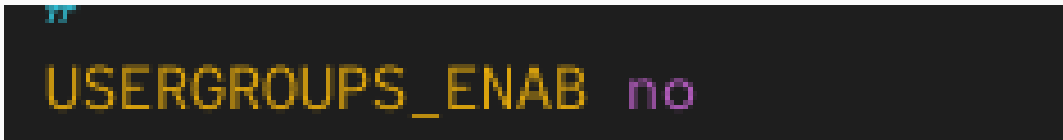


Рисунок 9: /etc/skel

Также устанавливаем параметр **USERGROUPS\_ENAB no**. Переходим в каталог **/etc/skel**. Создаём каталоги **Pictures** и **Documents**, это позволяет добавить эти каталоги по умолчанию во все домашние каталоги пользователей.

Изменяем содержимое  
файла `.bashrc`.

```
/etc/skel/.bashrc
# .bashrc
export EDITOR=/usr/bin/vim
# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi
```

Рисунок 10: `.bashrc`



## 15. Ход работы

Переключаемся в терминале на учётную запись пользователя **alice**, Используя утилиту **useradd**, создаём пользователя **carol**, Устанавливаем пароль для пользователя **carol**. Смотрим информацию о пользователе **carol**, проверяем, в какую первоначальную группу входит пользователь **carol**; также убеждаемся, что каталоги **Pictures** и **Documents** были созданы в домашнем каталоге пользователя **carol**.

```
root@adpetlin:/etc/skel# su alice
alice@adpetlin:/etc/skel$ sudo -i useradd carol
[sudo] password for alice:
alice@adpetlin:/etc/skel$ sudo passwd carol
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
alice@adpetlin:/etc/skel$ su carol
Password:
carol@adpetlin:/etc/skel$ id
uid=1003(carol) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
carol@adpetlin:/etc/skel$ cd
carol@adpetlin:~$ ls -Al
total 12
-rw-r--r--. 1 carol users 18 Oct 29 2024 .bash_logout
-rw-r--r--. 1 carol users 144 Oct 29 2024 .bash_profile
-rw-r--r--. 1 carol users 548 Sep 13 21:22 .bashrc
drwxr-xr-x. 2 carol users 6 Sep 13 21:20 Documents
drwxr-xr-x. 4 carol users 39 Sep 5 15:14 .mozilla
drwxr-xr-x. 2 carol users 6 Sep 13 21:20 Pictures
carol@adpetlin:~$
```

Рисунок 11: carol

## 16. Ход работы

переключаемся в терминале на учетную запись пользователя **alice**. Сначала представлен зашифрованный пароль, потом параметры: срок действия пароля 99999 дней, за 7 дней до истечения срока пользователь получит предупреждение, пароль можно менять бесконечно подряд, то есть без какого-либо периода действия установленного пароля. Изменяем свойства пароля пользователя **carol** следующим образом.срок действия пароля истекает через 90 дней . За три дня до истечения срока действия пользователь получает предупреждение . Пароль должен использоваться как минимум за 30 дней до того, как его можно будет изменить. Убеждаемся в изменении в строке с данными о пароле пользователя **carol** в файле `/etc/shadow`.

```
carol@adpetlin:~$ su alice
Password:
alice@adpetlin:/home/carol$ sudo cat /etc/shadow | grep carol
sudo: cat: command not found
alice@adpetlin:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$3Na3LxTab3j3d8a3bXe640$6Yc5Rm/B36KyHtK1RQOE.XyYzkLUKE058c1QKV6zA/:20344:0:99999:7:::
alice@adpetlin:/home/carol$ sudo passwd -n 30 -w 3 -x 90 carol
passwd: password changed.
alice@adpetlin:/home/carol$ sudo cat /etc/shadow | grep carol
carol:$y$j9T$3Na3LxTab3j3d8a3bXe640$6Yc5Rm/B36KyHtK1RQOE.XyYzkLUKE058c1QKV6zA/:20344:30:90:3:::
```

Рисунок 12: passwd -n ...

## 17. Ход работы

```
alice@adpetlin:/home/carol$ sudo grep alice /etc/passwd /etc/shadow /etc/group
/etc/passwd:alice:x:1001:1001::/home/alice:/bin/bash
/etc/shadow:alice:$y$j9T$B1cetZ4YsaVSewYNcb0hF/$0wd1DSvAw0VURaBEdwG8wjHgZWiI572JMGk.Eh6qQjA:20344:0:99999:7:::
/etc/group:wheel:x:10:adpetlin,alice
/etc/group:alice:x:1001:
alice@adpetlin:/home/carol$ sudo grep carol /etc/passwd /etc/shadow /etc/group
/etc/passwd:carol:x:1003:100::/home/carol:/bin/bash
/etc/shadow:carol:$y$j9T$3No3LxTsb3j3dBs3bXeG40$6cYcSRm/B36KyhTk1RG0E.XyYzkiUkE058crQKV6zA/:20344:30:90:3:::
alice@adpetlin:/home/carol$
```

Рисунок 13: alice | carol

Убеждаемся, что идентификатор **alice** существует во всех трёх файлах и убеждаемся, что идентификатор **carol** существует не во всех трёх файлах.

## 18. Ход работы

Находясь под учётной записью пользователя **alice**, создаём группы **main** и **third**. Используем **usermod** для добавления пользователей **alice** и **bob** в группу **main**, а **carol** — в группу **third**. Убеждаемся, что пользователь **carol** правильно добавлен в группу **third**. Определяем, участниками каких групп являются другие созданные нами пользователи. Указываем эту информацию в отчёте.

```
alice@adpetlin:/home/carol$ sudo groupadd main
alice@adpetlin:/home/carol$ sudo groupadd third
alice@adpetlin:/home/carol$ sudo usermod -aG main alice
alice@adpetlin:/home/carol$ sudo usermod -aG main bob
alice@adpetlin:/home/carol$ sudo usermod -aG third carol
alice@adpetlin:/home/carol$ id carol
uid=1003(carol) gid=100(users) groups=100(users),1004(third)
alice@adpetlin:/home/carol$ id adpetlin
uid=1000(adpetlin) gid=1000(adpetlin) groups=1000(adpetlin),10(wheel),980(vboxsf)
alice@adpetlin:/home/carol$ id bob
uid=1002(bob) gid=1002(bob) groups=1002(bob),1003(main)
alice@adpetlin:/home/carol$ id alice
uid=1001(alice) gid=1001(alice) groups=1001(alice),10(wheel),1003(main)
alice@adpetlin:/home/carol$
```

Рисунок 14: main | third

Мы получили представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

1. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010.
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — (Системный администратор).
3. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 4. — (Классика Computer Science).
5. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
6. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.