**Лабораторная работа №2. Права, пользователи, su и sudo**

**Становимся root**

Станьте суперпользователем (root-ом) с помощью утилиты sudo -i. Так как пароль root не задан - мы пока не можем стать им с помощью su.

к сведению

**Root** (англ. *root* — корень; читается "рут"), или **суперпо́льзователь** — это специальный аккаунт и группа пользователей в UNIX-подобных системах с идентификатором UID 0 (User IDentifier), владелец которого имеет право на выполнение всех без исключения операций. Суперпользователь UNIX-систем имеет логин "root" только по умолчанию и легко переименовывается при необходимости, часто встречается переименование в "toor" для усложнения подбора паролей автоматическими сканерами.

**su** (англ. **S**ubstitute **U**ser, **S**et **U**ID, **S**witch **U**ser\*, **S**uper **U**ser\* — замена пользователя, переключение пользователя, суперпользователь) — команда Unix-подобных операционных систем, позволяющая пользователю войти в систему под другим именем, не завершая текущий сеанс. Обычно используется для временного входа суперпользователем для выполнения административных работ. По умолчанию предполагается работа от имени пользователя root. Если первый аргумент su — дефис - , среда будет установлена такой же, как при регистрации заданного пользователя. Иначе передается текущая среда, за исключением значения $PATH, которое задается переменными PATH и SUPATH в файле /etc/default/su.

**sudo** (англ. **S**ubstitute **U**ser and **do**, дословно "подменить пользователя и выполнить") — программа для системного администрирования UNIX-систем, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы.

**Основная идея** — дать пользователям как можно меньше прав, но при этом достаточных для решения поставленных задач.

**Редактируем sudoers[​](https://iu5edu.ru/wiki/devops/docs/labs/linux/sudo/" \l "%D1%80%D0%B5%D0%B4%D0%B0%D0%BA%D1%82%D0%B8%D1%80%D1%83%D0%B5%D0%BC-sudoers" \o "Прямая ссылка на Редактируем sudoers)**

Далее с помощью утилиты visudo можно отредактировать файл /etc/sudoers(через утилиту - чтобы ничего не сломать, она создает временный файл и перед применением изменений проверяет синтаксис) - разрешить группе wheel делать sudoс паролем.

к сведению

В GNU/Linux CTRL часто обозначается как ^:

* Сохранить в nano: ^O.
* Выйти из nano: ^X.
* Поиск по файлу: ^W.

Этого можно добиться добавив строку %wheel ALL=(ALL:ALL) ALL:

* **%wheel** ALL=(ALL:ALL) ALL

Первое поле показывает имя пользователя или группы, к которым будет применяться правило, в данном случае к группе **wheel**, для пользователя нужно убрать %.

* %wheel **ALL=**(ALL:ALL) ALL

Первое "ALL" означает, что данное правило применяется ко всем хостам.

* %wheel ALL=(**ALL**:ALL) ALL

Данное "ALL" означает, что пользователь группы **wheel** может запускать команды от лица всех пользователей.

* %wheel ALL=(ALL:**ALL**) ALL

Данное "ALL" означает, что пользователь группы **wheel** может запускать команды от лица всех групп.

* %wheel ALL=(ALL:ALL) **ALL**

Последнее "ALL" означает, что данные правила применяются всем командам.

Хорошая статья о sudoers файле [тут](https://www.digitalocean.com/community/tutorials/how-to-edit-the-sudoers-file-ru).

**Добавим пользователя, группу и изменим права**[**​**](https://iu5edu.ru/wiki/devops/docs/labs/linux/sudo/#%D0%B4%D0%BE%D0%B1%D0%B0%D0%B2%D0%B8%D0%BC-%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F-%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%83-%D0%B8-%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B8%D0%BC-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0)

к сведению

Материал для дополнительного изучения: [Пользователи в Linux](https://github.com/iu5git/linux-course/blob/master/Wiki.md#%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D0%B8-%D0%B2-gnulinux).

1. Создаем пользователя ansible с домашней директорией /home/ansible/. Например, с помощью утилиты adduser.

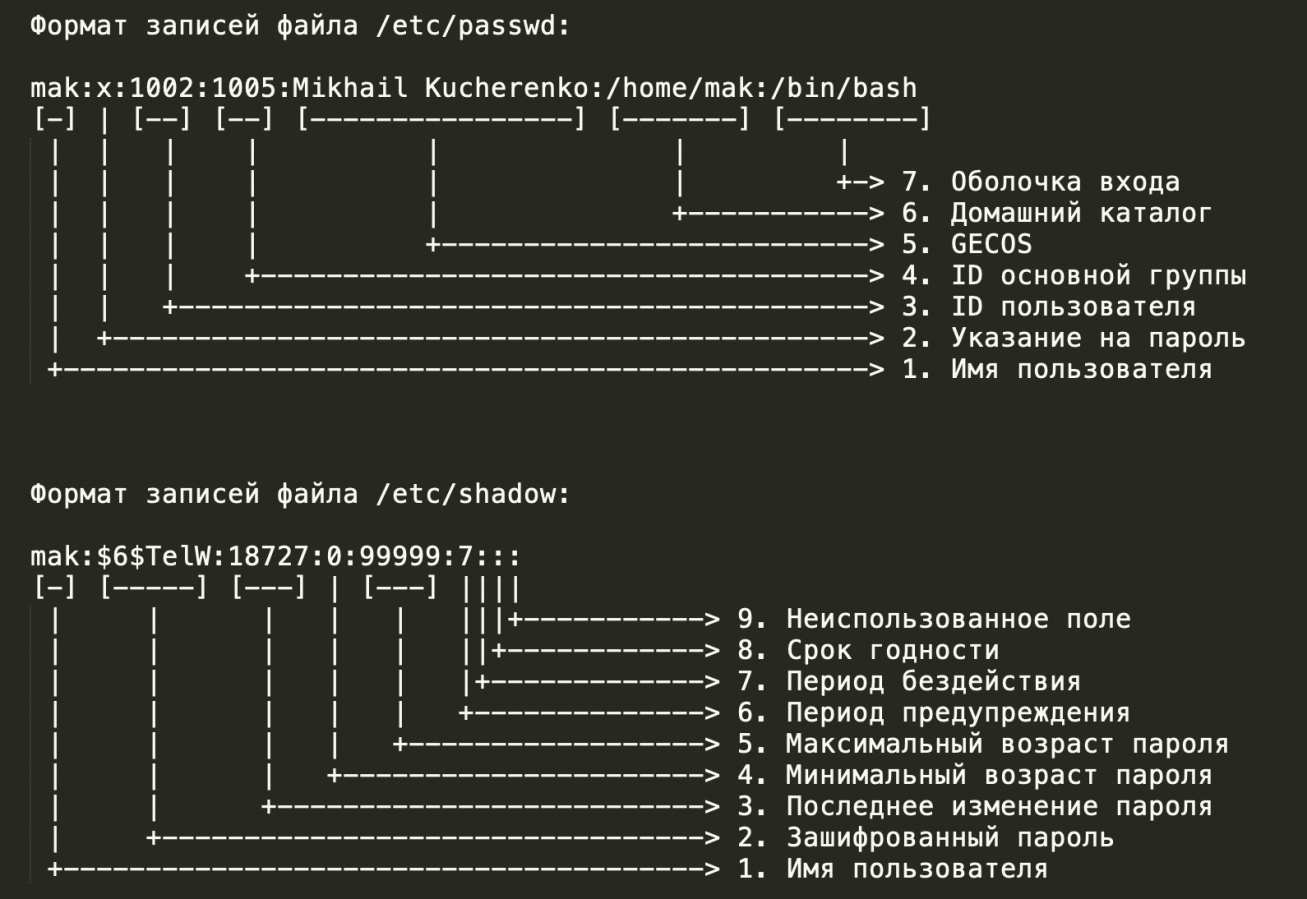
к сведению

Хорошая [статья](https://andreyex.ru/linux/komandy-linux-i-komandy-shell/useradd-protiv-adduser-v-chem-raznitsa/) о создании пользователей.

1. Меняем пользователю ansible пароль с помощью passwd ansible.
2. Меняем root пароль с помощью passwd.
3. Создаем группу wheel с помощью groupadd wheel.

предупреждение

В GNU/Linux нет магии, все происходит максимально логично. Так, добавление пользователя сводится к изменению файлов /etc/passwd и /etc/shadow. Исторически файл /etc/passwd содержал информацию о пользователях и их зашифрованные (чаще всего - хешированные) пароли. Однако, для того,чтобы пользователь мог взаимодействовать с системой - запускать программы от лица других пользователей, просматривать права доступа и так далее, нам необходимо, чтобы этот файл был доступен для чтения всем. А значит, в теории, пароли других пользователей можно было бы подобрать перебором, ведь они нам были бы тоже доступны. Для того, чтобы избежать проблем с утечкой паролей - их вынесли в отдельный файл /etc/shadow. Больше о формате этих файлов стоит узнать в справочных материалах.



1. Создать директорию /admin c помощью mkdir /admin.
2. [Читаем про систему прав](https://github.com/iu5git/linux-course/blob/master/Wiki.md#%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-%D0%BF%D1%80%D0%B0%D0%B2-%D0%B2-gnulinux).
3. Сделать owner-ом директории /admin пользователя ansible и выдать права группе wheel:

chown ansible:wheel /admin

1. Выдать на права на чтение и редактирование пользователю ansible,а группе wheel только не чтение:

chmod 640 /admin

**History[​](https://iu5edu.ru/wiki/devops/docs/labs/linux/sudo/" \l "history" \o "Прямая ссылка на History)**

Настроим для root сохранение истории, добавим это в конец /root/.bashrc, чтобы история незамедлительно сливалась в файл (а не при завершении сессии):

shopt -s histappend  
PROMPT\_COMMAND="history -a;$PROMPT\_COMMAND"

Аналогичное действие проведите для .bashrc вашего пользователя, с помощью которого вы подключаетесь на хост.

Для синхронизации history между сессиями можно добавить в текущий env (либо также добавить в .bashrc, но не советую, т.к. при вводе нескольких команд с разных консолей одновременно - может перетирать историю, которая не успела сохраниться на диск, но если вас не очень заботит мультипоточность можно):

export PROMPT\_COMMAND='history -a;history -c;history -r'

**А теперь перестаньте уже быть root, это вредно** - наберите команду exit или нажмите комбинацию ^D (CTRL+D).

Демонстрация некоторых командна некотором сервере, просто для ознакомления, не руководство к действию:

