Общая версия Linux. Уровень 1

Пользователи. Управление пользователями и группами





# На этом уроке

1. Разберём типы пользователей в ОС Linux.
2. Научимся создавать пользователей и группы пользователей, используя различные способы.
3. Разберём понятия владелец и группа владельца файла или каталога, научимся менять владельца и группу владельца файла или каталога.
4. Изучим утилиты, при помощи которых мы сможем выполнять административные действия или действия от другого пользователя в системе.

# Оглавление

[Типы пользователей в Linux](#_2s8eyo1)

[UID](#_gltrm6h8sw8u)

[GID](#_hzefxz8fibm7)

[Суперпользователь (root)](#_u1f21zgtwsrc)

[Системные пользователи (пользователи-демоны, технологические пользователи)](#_jllei2u7j07w)

[Обычные пользователи](#_k72l1zf8k9do)

[Управление пользователями](#_ghx5wvtlruuf)

[Создание пользователей и групп](#_rogyf6abyy8c)

[Добавление пользователей](#_dxrw0r87alvd)

[Примеры использования команды и параметров](#_xoui0haugyqc)

[Добавление группы](#_vmaf3cd9wb8e)

[Изменение параметров пользователя](#_ysjinrppz2p3)

[Изменение владельца и группы владельца файлов и каталогов](#_cbw8tpvu1i4x)

[Утилиты sudo, su](#_v7qjdac9g9n)

[Практическое задание](#_1v1yuxt)

[Дополнительные материалы](#_bjcdpahtyoqf)

[Используемые источники](#_qp22ogdddnar)

# Глоссарий

[**Пользователь**](http://heap.altlinux.org/modules/linux_users/index.html)— ключевое понятие организации системы доступа в Linux. Когда пользователь регистрируется в системе, то есть проходит процедуру авторизации, например, вводя системное имя и пароль, он идентифицируется с учётной записью. В ней система хранит информацию о каждом пользователе: его системное имя и некоторые другие сведения, необходимые для работы с ним. Именно с учётными записями, а не с самими пользователями, и работает система. Ниже приведён список этих сведений.

[**Учётная запись**](https://ru.wikipedia.org/wiki/%D0%A3%D1%87%D1%91%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C) — хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и [п](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B0_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0)редоставления доступа к его личным данным и настройкам.

[**Права доступа**](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B0_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0) — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы.

**Группа пользователей** — именованное множество пользователей с одинаковыми правами доступа к тем или иным объектам.

# Типы пользователей в Linux

Пользователь — ключевое понятие организации системы доступа к ресурсам ОС Linux. У пользователей есть два основных атрибута: UID и GID.

## UID

UID— идентификатор пользователя. Операционная система различает пользователей именно по UID, а не, например, по логину. Есть возможность создать двух пользователей с разными логинами, но одинаковым UID, что позволит обоим пользователям иметь одинаковые права доступа в системе. Это нарушение безопасности. **Важно:** UIDу каждого пользователя должен быть уникальным, в ОС не должно быть двух пользователей с одинаковым UID.

UID — это число из диапазона от 0 до 65535, при этом UID 0 назначается суперпользователю. Во многих ОС диапазон от 1 до 499 используется под системные нужды, всё остальное — обычные пользователи.

## GID

GID— идентификатор группы пользователей. Каждый пользователь в ОС Linux принадлежит как минимум к одной группе — группе по умолчанию, которая создаётся одновременно с учётной записью пользователя и как правило совпадает с именем пользователя. У пользователя может быть несколько групп. Пользователь может входить в группу с GID 0 (группа суперпользователя), и это не будет нарушением безопасности. Группы необходимы для регулирования доступа нескольких пользователей к различным ресурсам.

Условно можно разделить пользователей ОС Linux на три типа: суперпользователь, системные пользователи и обычные пользователи.

## Суперпользователь (root)

Это пользователь с неограниченными правами, он имеет UID и GID, равные 0. В системе больше не должно быть пользователей с таким UID, но другие пользователи могут входить в группу суперпользователя. Этот пользователь предназначен для выполнения команд и действий с файлами, которые могут влиять на работу как отдельных служб, так и всей системы. Суперпользователем осуществляется конфигурация ключевых служб операционной системы, установка и удаление программного обеспечения, конфигурация устройств и т. д.

Неосторожная работа от имени суперпользователя может привести к критическому повреждению операционной системы, вплоть до её уничтожения. Поэтому работа из-под root не рекомендуется, лучше использовать данную возможность только в тех случаях, когда без неё не обойтись.

## Системные пользователи (пользователи-демоны, технологические пользователи)

Онипредназначены для обеспечения работы запущенных процессов. Обычно такие пользователи не имеют оболочки, а также не могут никаким образом авторизоваться в системе. Создаются системой автоматически при установке приложений или вручную, в случае запуска какого-то приложения, не имеющегося в стандартных репозиториях ОС. Во многих ОС UID таких пользователей рекомендуется использовать с числами от 1 до 499.

## Обычные пользователи

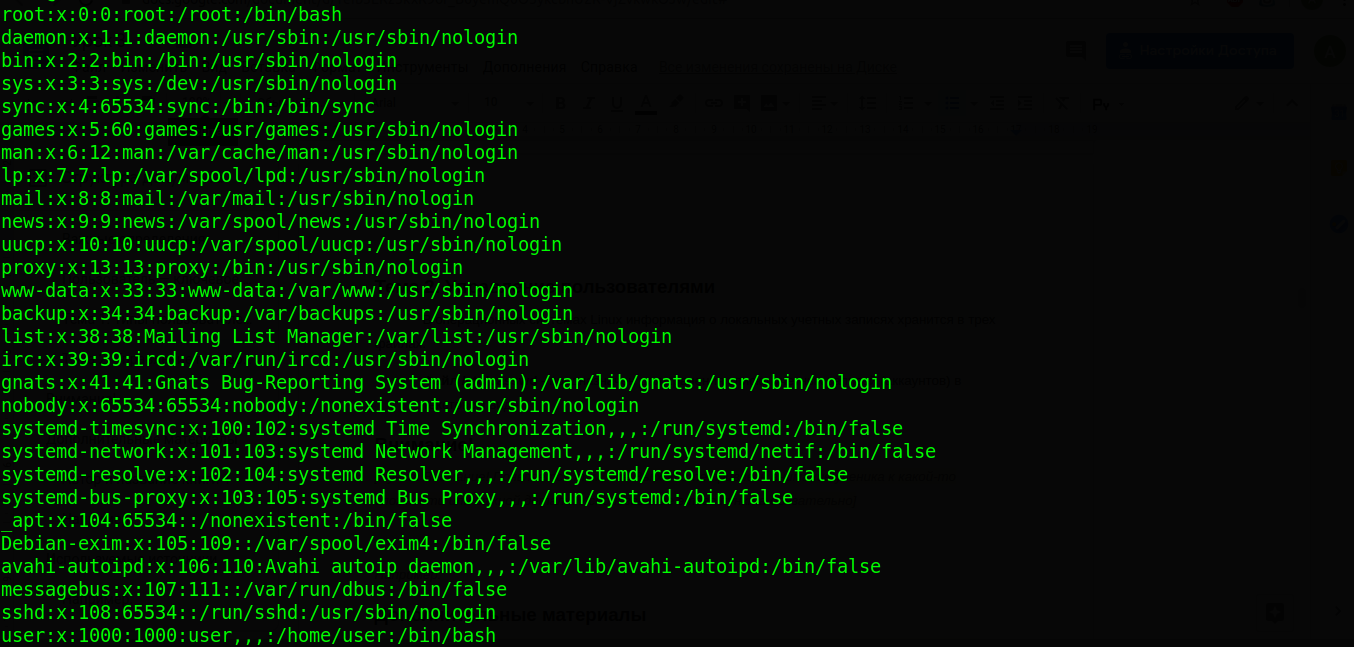
Это учётные записи, которые используются для работы в ОС, создаются администратором системы. Они могут быть локальными — созданными непосредственно на сервере, либо сетевыми, например, если сведения об учётной записи хранятся в домене LDAP (аналог службы Active Directory в Windows). Такой тип учётных записей может использоваться не только людьми, но и программным обеспечением, предназначенным для управления конфигурациями (например, Ansible). Важно разграничивать возможности данного типа пользователей для совершения административных действий, например использования утилиты sudo.

## 

# Управление пользователями

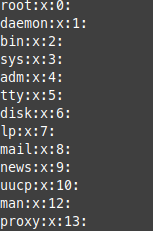
В операционных системах Linux информация о локальных учётных записях хранится в трёх файлах:

**1. Файл /etc/passwd.** Предназначен для хранения списка учётных записей (аккаунтов) в текстовом виде. На скриншоте вы видите содержимое файла /etc/passwd:



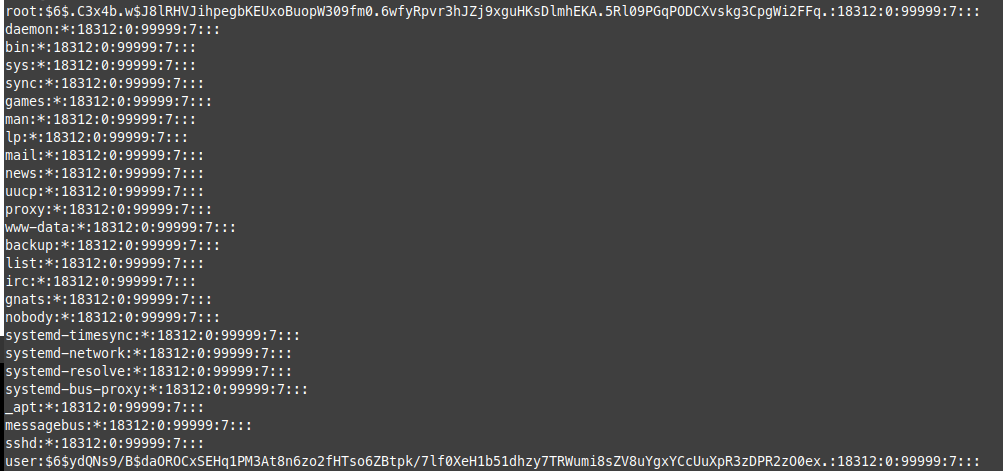
Файл можно разделить на несколько столбцов. В качестве разделителя используется символ «:». Первый столбец — имя учётной записи (логин), второй столбец предназначался для хранения хеша паролей, но сейчас хранение паролей вынесено в отдельный файл, о нём мы поговорим ниже. Третий и четвёртый столбцы — это UID и GID пользователя. Пятый столбец — комментарии к учётной записи. Шестой — домашний каталог пользователя. Если он не указан, будет использоваться корневой каталог (/), и при логине в ОС будет выдано сообщение об ошибке. И последний седьмой столбец — это оболочка, запускаемая при входе в систему. У системных пользователей оболочка всегда /usr/sbin/nologin или /bin/false. Зайти в систему с такой учётной записью не получится. У обычных пользователей стандартная оболочка — /bin/bash.

**2. Файл /etc/group** хранит информацию о группах и пользователях, состоящих в этих группах. Вывод информации о группах имеет следующий вид:



Файл можно разделить на несколько столбцов. Первый столбец — имя группы. Второй столбец аналогичен второму столбцу в файле passwd и предназначался для хранения паролей. **X** означает, что пароли хранятся в файле gshadow. Пароли в группах используются крайне редко, поэтому рассматривать их мы не будем. Третий столбец — ID группы. Четвёртый — пользователи, состоящие в группе. В группе может быть несколько пользователей, они перечисляются через запятую.

**3. Файл /etc/shadow** хранит информацию о паролях пользователей из файла etc/passwd. Во многих системах файл доступен только для чтения пользователю root.



Файл изменяется командой passwd. Он разделён на несколько столбцов. Первый столбец — имя пользователя, по этому столбцу связаны файлы /etc/passwd и /etc/shadow. Второй столбец — пароль в зашифрованном виде. Третий — дата последнего изменения, заполняется командой passwd. Четвёртый — минимальное число дней между изменениями паролей, то есть количество дней, спустя которое пользователь сможет снова изменить пароль. Пятый — максимальное время жизни пароля, значение по умолчанию — 99999. Шестой — количество дней до истечения срока действия пароля пользователь получит предупреждающее сообщение об этом. Седьмой — количество дней после истечения срока действия пароля, когда учётная запись будет отключена. Восьмой — срок действия учетной записи. Девятый зарезервирован.

**Внимание!** *Если во втором столбце вместо хеша пароля стоит символ «! или \*», пользователь не сможет залогиниться в системе. Столбцы 7, 8 и 9 обычно пустые. Изменение файла вручную не рекомендуется!*

## Создание пользователей и групп

В Linux есть несколько способов создать пользователя или группу. Команды useradd или adduser используются для создания пользователей, groupadd или addgroup — для создания групп. Изменить атрибуты пользователя можно при помощи утилиты usermod, для изменения атрибутов группы есть утилита groupmod, а для изменения паролей — passwd.

### Добавление пользователей

**useradd** — стандартная команда Linux, она предназначена для создания пользователя в системе. Имеет небольшие различия по результату работы в RHEL- и Debian-подобных системах. В Debian-подобных системах useradd без использования каких-либо параметров создаст пользователя и группу пользователя. Она не создаст домашний каталог, и в качестве оболочки по умолчанию будет назначена /bin/sh. В RHEL-подобных системах useradd без использования каких-либо параметров создаст пользователя и группу пользователя, создаст домашний каталог в /home, и в качестве оболочки по умолчанию будет назначена /bin/bash.

### Примеры использования команды и параметров

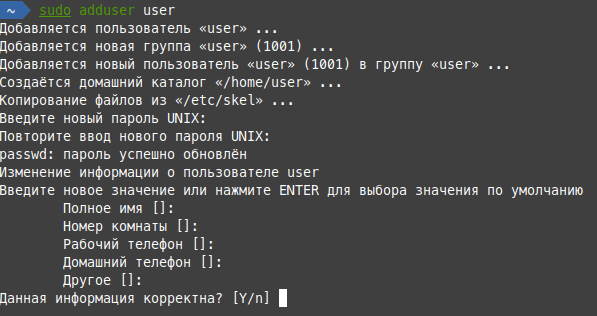
useradd -s /bin/bash -d /home/user -m user\_name создаст пользователя с именем user\_name. Параметр -s /bin/bash говорит, что в качестве оболочки нужно установить bash, -d /home/user указывает домашний каталог пользователя, параметр -m— создать домашний каталог. Подобный вариант команды используется для создания обычных пользователей.

useradd -s /usr/sbin/nologin -d /path\_to\_file -M user\_name создаст пользователя с именем user\_name. Параметр -s /usr/sbin/nologin говорит, что в качестве оболочки нужно использовать nologin, это позволит ограничить вход пользователя. -D /path\_to\_file указывает домашний каталог пользователя, параметр -M— не создавать домашний каталог. Подобный вариант используется для создания системных или технологических учётных записей, от имени которых будет работать разработанное приложение.

Дополнительные параметры и возможности мы можем посмотреть, вызвав страницу справочного руководства **man useradd**.

**Внимание!** *После того, как пользователь был добавлен, по необходимости ему назначается пароль командой passwd.*

adduser— Perl-скрипт, реализующий в более удобном и интерактивном виде функционал команды useradd. Он рекомендуется к использованию в Debian-подобных системах. Одна из особенностей данной команды — отсутствие каких-либо дополнительных действий с учётной записью после её создания. Пример работы команды:



#### **Добавление группы**

**groupadd** — стандартная утилита Linux, предназначенная для создания групп. Чаще всего используется без параметров groupadd group\_name. Обычно группы создаются сразу при создании пользователя, но довольно часто бывают ситуации, когда в одну группу должны входить сразу несколько пользователей, и здесь на выручку придёт команда groupadd. Например, мы можем предварительно создать общую группу: groupadd dev**,** а потом создать пользователей, входящих в эту группу, командой adduser username --gid GID, adduser user1 --gid 1001.

**addgroup** — скрипт, использующий функционал команды groupadd.

Дополнительную информацию о параметрах и возможностях **groupadd/addgroup** можно прочитать в справочном руководстве **man groupadd** или **man addgroup.**

Удаление пользователей рекомендуется выполнять командой deluser — это скрипт, использующий функционал команды userdel. Аналогично для удаления групп из системы рекомендуется применять delgroup — скрипт, использующий функционал команды groupdel. Параметры и дополнительные возможности предлагаем рассмотреть самостоятельно, используя утилиту manс названиями соответствующих команд.

#### **Изменение параметров пользователя**

1. **passwd user\_name** изменит пароль пользователя с именем **user\_name**. Такое действие требует прав суперпользователя, поэтому данная команда используется с командой **sudo**.
2. **passwd** без указания пользователя изменит или задаст пароль текущему пользователю.
3. **chage user\_name** позволит изменить политики для паролей конкретного пользователя. Действие требует прав суперпользователя, поэтому данная команда также используется с командой **sudo**.
4. **usermod** изменяет атрибуты пользователя. Например, нам необходимо добавить пользователя в группу sudo. Это группа, которая имеет административные права на ОС. Используем usermod -aG sudo user\_name, где параметр -G— имя дополнительной группы, а параметр -aдобавляет пользователя в дополнительные группы, не исключая из основной. Чтобы просто сменить группу, достаточно выполнить usermod -g new\_group user\_name.

Дополнительно к вышеперечисленному существует ещё ручной способ добавления пользователей и групп пользователей путём редактирования файлов **/etc/passwd** и **/etc/group**. При редактировании этих файлов важно учитывать следующие вещи:

1. Обязательно соблюдайте синтаксис файла.
2. В файле **/etc/group** пользователи и участники группы добавляются через запятую.
3. После заполнения информации о пользователе и группе в случае необходимости пользователю задаётся пароль командой **passwd**.
4. Домашний каталог пользователя создаётся вручную, и ему присваиваются соответствующие разрешения.
5. Изменять эти файлы вручную — не лучшая идея, поскольку существует множество мест, где можно ошибиться. Лучше пользоваться утилитами, указанными выше.

## Изменение владельца и группы владельца файлов и каталогов

Для изменения владельца файла или каталога есть две команды:

1. **chown** —изменяет владельца и группу владельца файлов и каталогов. Самый распространённый способ применения: chown user\_name:group\_name file\_name. Здесь user\_name — имя пользователя, владельца файла или каталога, group\_name — имя группы, которая будет владельцем файла или каталога. Если нам необходимо поменять владельцев на каталог со всем содержимым, используем параметр **-R** (рекурсивно): chown -R user\_name:group\_name dir\_name. Дополнительную информацию можно посмотреть на странице справочного руководства **man chown**.
2. **chgrp** — изменяет группу владельца на файл или каталог: chgrp group\_name file\_name. Для каталога с содержимым — chgrp -R group\_name dir\_name**.** Дополнительную информацию можно получить в страницах справочного руководства **man** **chgrp**.

# Утилиты sudo, su

Как известно, в ОС Linux всегда есть один суперпользователь (администратор системы) **root**. У этого пользователя абсолютно неограниченные права на всю систему, начиная от установки пакетов, заканчивая удалением файлов и каталогов. Ограничить свободу действий в системе пользователя root практически невозможно. Во избежание ошибочных действий, которые могут привести к краху системы, работа под пользователем root не рекомендуется. А для выполнения административных действий обычным пользователем используют две утилиты: **su** и **sudo.**

**su** — команда, которая позволяет переключаться в пользователя (switch user) или делает пользователя суперпользователем, при этом не завершая сеанс. Синтаксис: su - user\_name — далее вводится пароль и меняется ID текущего пользователя. Su -без параметров переключит текущего пользователя в суперпользователя. Данный метод работы под суперпользователем не очень хорош, так как нет никаких ограничений.

**sudo** — утилита, которая позволит выполнять административные действия в системе согласно настройкам в файле /etc/sudoers. Файл /etc/sudoers редактируется только пользователем, имеющим права администратора системы. В этом файле перечисляется набор административных команд, которые разрешено выполнять пользователю или группе пользователей. В Ubuntu пользователи, входящие в группу sudo, могут выполнять административные действия без каких-либо ограничений. Не рекомендуется злоупотреблять количеством участников данной группы.

Файл /etc/sudoers может редактироваться или командой **sudoedit**, которая является встроенным механизмом для редактирования файлов в утилиту sudo, или утилитой **visudo**, обе эти команды запускают текстовый редактор и позволяет избежать большинства синтаксических ошибок. **sudoedit -**вызывает редактор по умолчанию (во многих современных системах это nano), a **visudo -** проверяет синтаксис записи, использует для редактирования файла редактор **vi**, имеет преимущество в . Синтаксис записи:

1. User\_name ALL= full\_path\_to\_command.Например, запись user All= /usr/sbin/adduser позволит пользователю с именем user, используя sudo, добавлять учётные записи в системе.
2. User\_name ALL=(ALL) ALLпозволит пользователю, используя утилиту **sudo,** выполнять административные действия без ограничений.
3. %sudo ALL=(ALL) NOPASSWD:ALLпозволит всем пользователям, входящим в группу sudo, выполнять любые административные действия в системе без подтверждения паролем. В целях безопасности не рекомендуется использовать в многопользовательских решениях.

# 

# Практическое задание

1. Управление пользователями:
   1. создать пользователя, используя утилиту useradd;
   2. удалить пользователя, используя утилиту userdel;
   3. создать пользователя в ручном режиме.
2. Управление группами:
   1. создать группу с использованием утилит и в ручном режиме;
   2. попрактиковаться в смене групп у пользователей;
   3. добавить пользователя в группу, не меняя основной;
   4. удалить пользователя из группы.
3. Добавить пользователя, имеющего право выполнять команды/действия от имени суперпользователя. Сделать так, чтобы sudo не требовал пароль для выполнения команд.
4. \* Используя дополнительные материалы, выдать одному из созданных пользователей право на выполнение ряда команд, требующих прав суперпользователя (команды выбираем на своё усмотрение).

# Дополнительные материалы

[Администратор в Ubuntu, или Что такое sudo](https://help.ubuntu.ru/wiki/%D1%81%D1%83%D0%BF%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C_%D0%B2_ubuntu)

[su или sudo?](https://habr.com/ru/post/44783/)

[Sudo](https://ru.hexlet.io/courses/cli-basics/lessons/sudo/theory_unit)

# 

# Используемые источники

[Робачевский А. Операционная система Unix](https://it.wikireading.ru/6490)

[Ubuntu управление пользователями и группами](https://help.ubuntu.ru/wiki/%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%B8_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%8B)

[Костромин В. Linux для пользователя](http://www.linuxcenter.ru/lib/books/kostromin/)