

Учетные записи в LINUX

В операционной системе Linux существуют три типа пользователей:

- пользователь root (по умолчанию неактивен в Ubuntu)
- системные пользователи
- обычные пользователи

Система регистрирует следующую информацию о каждом пользователе:

Имя пользователя (username) - Это имя должно быть уникальным в рамках системы. В именах могут быть использованы только английские буквы, числа и символы _ и . (точка).

- Идентификационный номер пользователя (UserID) - Этот номер, сокращённо обозначаемый как UID, является уникальным идентификатором пользователя в системе. Система отслеживает пользователей по их номерам UID, а не по именам.
- Идентификационный номер группы (groupID) - Этот номер (сокращённо GID) обозначает группу, к которой по умолчанию относится пользователь. Группы позволяют регулировать доступ многих пользователей к различным ресурсам. Каждый пользователь принадлежит одной или нескольким группам, и эту принадлежность устанавливает системный администратор.
- Пароль (password) - Это зашифрованный (encrypted) пароль пользователя. Для создания и изменения пароля используется команда **passwd**.

- Полное имя (fullname) - Помимо системного имени пользователя, в систему заносится и хранится имя (фамилия и т. д.) “реального” пользователя. Например, пользователю petriv в реальной жизни может соответствовать человек по имени Ivan Petrov.
- Домашний каталог (homedirectory) - Это название каталога, в который попадает пользователь после того, как он вошёл в систему (зарегистрировался, login), и где хранятся его собственные файлы. Такой каталог имеется у каждого пользователя, и все такие каталоги собраны в один каталог, обычно называемый /home.

- Начальная оболочка (loginshell) - Командная оболочка, которая запускается при входе в систему. Например, /bin/bash или /bin/zsh.

Вся эта информация хранится в файле **/etc/passwd**.

Каждая строка в файле имеет формат:

Имя пользователя: зашифрованный пароль: UID:

GID: полное имя: домашний каталог: оболочка
например:

*kiwi:Xv8Q981g71oKK:102:100:LauraPoole:/home/kiwi
:/bin/bash*

В этом примере на первом месте стоит имя пользователя, kiwi. В следующем поле помещается пароль в зашифрованном виде: Xv8Q981g71oKK. Пароли в системе хранятся не в “читаемом” формате, а в зашифрованном. Для того, чтобы расшифровать пароль, его нужно знать. Эта форма шифрования является достаточно надёжной.

Третье поле — 102 — UID. Это число должно быть уникальным.

Четвёртое поле — 100 — GID, т. е. пользователь принадлежит к группе с номером 100. Информация о группах хранится в файле **/etc/group**.

Пятое поле — реальное имя пользователя, в данном случае — LauraPoole. Последние два поля — домашний каталог пользователя (/home/kiwi) и начальная оболочка (/bin/bash). Не требуется, чтобы имена пользователя и домашнего каталога совпадали, однако такая организация помогает устанавливать принадлежность каталога.

Для управления пользователями служат команды :

Команда	Описание
useradd	добавить нового пользователя
passwd	установить пароль пользователя
usermod	изменить параметры учетной записи пользователя
userdel	удалить учетную запись пользователя

Ключ	Описание
-b	Базовый каталог. Это каталог, в котором будет создана домашняя папка пользователя. По умолчанию /home
-c	Комментарий. В нем вы можете напечатать любой текст.
-d	Название домашнего каталога. По умолчанию название совпадает с именем создаваемого пользователя.
-e	Дата, после которой пользователь будет отключен. Задается в формате ГГГГ-ММ-ДД. По умолчанию отключено.
-f	Количество дней, которые должны пройти после устаревания пароля до блокировки пользователя, если пароль не будет изменен (период неактивности). Если значение равно 0, то запись блокируется сразу после устаревания пароля, при -1 - не блокируется. По умолчанию -1.
-g	Первичная группа пользователя. Можно указывать как GID, так и имя группы. Если параметр не задан будет создана новая группа название которой совпадает с именем пользователя.
-G	Список вторичных групп в которых будет находиться создаваемый пользователь
-k	Каталог шаблонов. Файлы и папки из этого каталога будут помещены в домашнюю папку пользователя. По умолчанию /etc/skel.
-m	Ключ, указывающий, что необходимо создать домашнюю папку. По умолчанию домашняя папка не создается.
-p	Зашифрованный пароль пользователя. По умолчанию пароль не задается, но учетная пользователь будет заблокирован до установки пароля
-s	Оболочка, используемая пользователем. По умолчанию /bin/sh.
-u	Вручную задать UID пользователю.

Если требуется временно запретить пользователю вход в систему, но не удалять его домашний каталог и прочие сделанные установки, можно просто поставить звёздочку (символ *) в то поле файла `/etc/passwd`, где находится пароль. Например, таким образом, изменённая строка для пользователя `kiwi` будет выглядеть как

```
kiwi:*Xv8Q981g71oKK:102:100:LauraPoole:/home/  
kiwi:/bin/bash
```

При этом вход в систему пользователя `kiwi` станет невозможным.

Каждый пользователь принадлежит одной либо нескольким группам.

Имеется несколько групп, определённых системой, например, *bin*, *mail*, *sys*. Эти группы созданы для оформления прав доступа к системным файлам, и пользователи не должны принадлежать к этим группам. Для пользователей создаются специальные группы, например, *users*.

Для управления группами служат команды :

Команда	Описание
<code>groupadd</code>	создать новую группу
<code>grpasswd</code>	установить пароль группы
<code>groupmod</code>	изменить параметры группы
<code>groupdel</code>	удалить группу

Информация о группах содержится в файле /etc/group. Формат каждой строки:

имя группы: пароль:GID:другие члены группы

Команда groups перечисляет список групп, к которым относится (имеет доступ) данный пользователь.

Команда **login** используется при входе в систему. Она проверяет правильность ввода имени и пароля пользователя, меняет каталог на домашний, выстраивает окружение и запускает командный интерпретатор. Команду login нельзя запускать из командной строки – это вызовет ошибку и может привести к завершению сеанса.

Команда **su** позволяет сменить идентификатор пользователя уже в процессе сеанса. Синтаксис ее прост: `su username`, где `username` — имя пользователя, которое будет использоваться. После этого программа запросит пароль. При правильно введенном пароле, `su` запустит новый командный интерпретатор с правами пользователя, указанного `su` и присвоит сеансу его идентификаторы. Если имя пользователя опущено, то команда `su` использует имя `root`.

При использовании команды `su` пользователем `root` она никогда не запрашивает пароль.

Команда **newgrp** аналогична по своим возможностям **su** с той разницей, что происходит смена группы. Пользователь должен быть включен в группу, которая указывается в командной строке **newgrp**. При использовании команды **newgrp** пользователем **root** она никогда не запрашивает пароль. Синтаксис команды аналогичен синтаксису команды **su**: **newgrp groupname**, где **groupname** – имя группы, на которую пользователь меняет текущую.

Команда `chage` управляет информацией об устаревании пароля и учетной записи. Обычный пользователь (не `root`) может использовать команду только для просмотра своих параметров устаревания пароля:

```
gserg@ADM:/$ chage -l gserg
Last password change           : May 03, 2014
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```