top
КОМПЬЮТЕРНАЯ АКАДЕМИЯ

Основы системного администрирования и сетевых технологий

УРОК №1

Управление пользователями в Linux

Linux является многозадачной операционной системой. Это означает, что с ней одновременно могут работать несколько пользователей. Поэтому одной из функций операционной системы является изоляция пользователей и защита их друг от друга. Система следит за каждым пользователем и определяет, можно ли ему предоставить доступ к тому или иному файлу или разрешить выполнение той или иной программы.

Каждому пользователю ставится в соответствие уникальное имя (регистрационное имя пользователя). Имя пользователя важно, но система определяет права пользователя не на основании его, а на основании идентификатора пользователя (user ID, UID). В отличие от имени пользователя UID может и не быть уникальным, в этом случае для сопоставления ему имени пользователя берется первое найденное имя, UID которого совпадает с данным.

Каждому регистрируемому в системе пользователю ставятся в соответствие определенные элементы системы. Обычно это домашний каталог и командная оболочка. Домашний каталог отдается в полное распоряжение пользователя.

Пользователи

При добавлении нового пользователя в систему ему выделяется идентификатор пользователя - UID. UID может иметь значения от 0 до 65534.

Выделение UID начинается с некоторого номера, разного для разных дистрибутивов (например, 500 или 1000) и продолжается в сторону увеличения. Тот факт, что номера, например, до 500 зарезервированы для системы, просто является общепринятым соглашением. Эти номера соответствуют непривилегированным учетным записям, пользователи которых не обладают никакими специальными привилегиями.

Однако существует особенный UID=0. Любой пользователь с нулевым идентификатором является привилегированным. Такой пользователь имеет неограниченную власть над системой, ему разрешено все. Учетная запись root, UID которой равно 0, называемая учетной записью суперпользователя, делает ее владельца полным хозяином системы, поскольку он может все и никто не может ему воспрепятствовать в этом.

Группы

Каждый пользователь является членом какой-то группы. Он может входить и в несколько групп, но в одну он входит обязательно.

Механизм групп позволяет выбрать одну из двух различных схем управления группами: группа по умолчанию или частные группы пользователей.

В случае схемы с группой по умолчанию любой пользователь может читать (и изменять) файлы другого пользователя.

С частными же группами чтение и запись файла, созданного другим пользователем, возможны лишь если его владелец явно предоставил это право другим пользователям.
Если требуется, чтобы пользователи могли присоединиться или покинуть группу без вмешательства системного администратора, то группе можно назначить пароль.

Пользователь может пользоваться привилегиями определенной группы только в том случае, если он принадлежит к ней. Существуют два варианта: либо пользователь принадлежит группе с момента входа в систему, либо он становится членом группы впоследствии, после того, как он начал работать с системой.

Частные группы пользователей обладают именами, совпадающими с именами пользователей. Частная группа делается группой входа в систему.

Способы управления учетными записями

Управление учетными записями пользователей в Linux может осуществляться тремя способами.

Во-первых, можно использовать инструменты с графическим интерфейсом, предоставляемые дистрибутивом. Внешний вид и принцип работы этих инструментов зависит от используемого дистрибутива. Такой подход гарантированно позволит избежать проблем.

Другим вариантом является использование инструментов с интерфейсом командной строки, таких как useradd, usermod, gpasswd, passwd и т.д.

Третий способ управления учетными записями пользователей заключается в непосредственном редактировании локальных файлов конфигурации.

Использование инструментов командной строки для управления пользователями и группами

Добавление пользователя осуществляется при помощи команды useradd. Для вызовы команды необходимы права суперпользователя.

Пример использования:
useradd stu

Эта команда создаст в системе нового пользователя stu. Чтобы изменить настройки создаваемого пользователя, используются следующие ключи:

Ключ	Описание
-b	Базовый каталог. Это каталог, в котором будет создана домашняя папка пользователя. По умолчанию /home
-c	Комментарий. В нем может быть любой текст.
-d	Имя 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.

Ключ	Описание
-G	Список вторичных групп в которых будет находится 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.

Параметры создания пользователя по умолчанию

Если при создании пользователя не указываются дополнительные ключи, то берутся настройки по умолчанию. Эти настройки можно посмотреть, выполнив команду **useradd -D**

Результат может быть следующим:

```
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

Если вас не устраивают такие настройки, вы можете поменять их выполнив
useradd -D -s /bin/bash

Здесь - s это ключ из таблицы выше. Таким образом могут быть заданы параметры, определяемые только ключами:
-b -e -f -g -s

Изменение пользователя

Изменение параметров пользователя происходит с помощью утилиты **usermod.**

Пример использования:

usermod -c «комментарий пользователю» stu
Команда usermod использует те же опции, что и команда useradd.

Изменение пароля

Изменить пароль пользователю можно при помощи утилиты passwd. Для ее выполнения необходимы права суперпользователя.
passwd stu

Команда passwd может использоваться и обычным пользователем для смены собственного пароля. Для этого пользователю надо ввести
passwd
и ввести старый и новый пароли.

Основные ключи passwd:

Ключ	Описание
-d	Удалить пароль пользователя. После этого пароль станет пустым, и пользователь сможет войти в систему без ввода пароля.
-e	Сделать пароль устаревшим. Это заставит пользователя изменить пароль при следующем входе в систему.
-i	Заблокировать учетную запись пользователя по прошествии указанного количества дней после устаревания пароля.
-n	Минимальное количество дней между сменами пароля.
-x	Максимальное количество дней, после которого необходимо обязательно сменить пароль.
-l	Заблокировать учетную запись пользователя.
-u	Разблокировать учетную запись пользователя.

Установка пустого пароля пользователя

Суперпользователь с помощью утилит командной строки **passwd** и **usermod** может удалить пароль пользователь, дав возможность входить в систему без указания пароля.

passwd -d stu или **usermod -p "" stu**

Если учетная запись пользователя в этот момент была заблокирована командой **passwd -l,** то указанные выше команды снимут эту блокировку.
Установка пустого пароля может быть полезна как временное решение проблемы в ситуации, когда пользователь забыл свой пароль или не может его ввести из-за проблем с раскладкой клавиатуры. После этого имеет смысл принудить пользователя установить себе новый пароль при следующем входе в систему с помощью команды **passwd -e stu**

Удаление пользователя

Для удаления пользователя используется команда userdel.
Для её использования необходимы права суперпользователя.
Пример использования:
userdel stu
Команда userdel имеет два основных ключа:

Ключ	Описание
-f	Принудительно удалить пользователя, даже если он сейчас работает в системе.
-r	Удалить домашний каталог пользователя.

Проверка учётной записи

Перед тем, как передать новому пользователю реквизиты и начальный пароль для входа в свою учётную запись, её необходимо проверить. Для этого нужно завершить текущий сеанс и войти в систему под именем нового пользователя (учётную запись которого необходимо проверить). И последовательно выполнить следующие команды:

pwd
ls -al

Первая выведет домашний каталог для текущего пользователя, вторая список всех (в том числе и скрытых) файлов и подкаталогов в домашнем каталоге с указанием их владельца и режимов доступа.

Получение информации о пользователях

Часто в процессе работы необходимо получить информацию о пользователях системы. Для этого используются следующие команды.

w – вывод информации (имя пользователя, рабочий терминал, время входа в систему, информацию о потребленных ресурсах CPU и имя запущенной программы) о всех вошедших в систему пользователях.

who – вывод информации (имя пользователя, рабочий терминал, время входа в систему) о всех вошедших в систему пользователях.

whoami или id – вывод имени пользователя, выполнившего команду.

users – вывод имен пользователей, работающих в системе. id имя_пользователя – вывод информации о пользователе: его uid, имя_пользователя, gid (идентификационный номер группы) и имя первичной группы, список групп в которых состоит пользователь.

groups имя_пользователя – вывод списка групп, в членом которых является пользователь.

Создание группы

Команда groupadd создаёт новую группу согласно указанным значениям командной строки и системным значениям по умолчанию. Для выполнения команды необходимы права суперпользователя. Пример использования:
groupadd testgroup

Основные ключи:

Ключ	Описание
-g	Установить собственный GID.
-p	Пароль группы.
-r	Создать системную группу.

Изменение группы

Сменить название группы, ее идентификационный номер (GID) или пароль можно при помощи команды groupmod. Для выполнения команды необходимы права суперпользователя. Пример использования:

groupmod -n newtestgroup testgroup

#Имя группы изменено с testgroup на newtestgroup
Опции команды groupmod:

Ключ	Описание
-g	Установить другой GID.
-n	Новое имя группы.
-p	Изменить пароль группы.

Удаление группы

Удаление группы производится с помощью команды groupdel. Для выполнения команды необходимы права суперпользователя.

Пример использования:

groupdel testgroup
Команда groupdel не имеет параметров.

Управления учетными записями пользователей непосредственным редактированием локальных файлов конфигурации

Информация о пользователях и группах хранится в следующих файлах.

passwd (etc/passwd) – содержит информацию о пользователях.
group (etc/group) – информация о группах.

У файлов **/etc/passwd** и **/etc/group** следующие права доступа: чтение и запись для root, для остальных – только чтение.
shadow (etc/shadow) – в этом файле хранятся "теневые пароли", информация о паролях пользователей в зашифрованном виде.
Файл **/etc/passwd** может читать любой пользователь, а файл **/etc/shadow** может читать только root.
gshadow (etc/gshadow) – то же самое что и shadow, только для паролей групп.
Помимо основных, в системе присутствуют дополнительные файлы.
useradd (etc/default/useradd) – файл задающий свойства по умолчанию для всех добавляемых пользователей. Содержимое этого файла выводится командой - useradd -D.
login.defs (/etc/login.defs) – содержит настройки для создания новых пользователей.
/etc/skel – каталог с файлами по умолчанию, которые копируются в домашний каталог каждого пользователя при его создании.

Файл /etc/passwd

Вся информация об учетной записи пользователя хранится в файле /etc/passwd. Чтобы просмотреть список пользователей, можно использовать команду:

cat /etc/passwd

Каждая строка файла описывает некоторого пользователя (рис. 1).

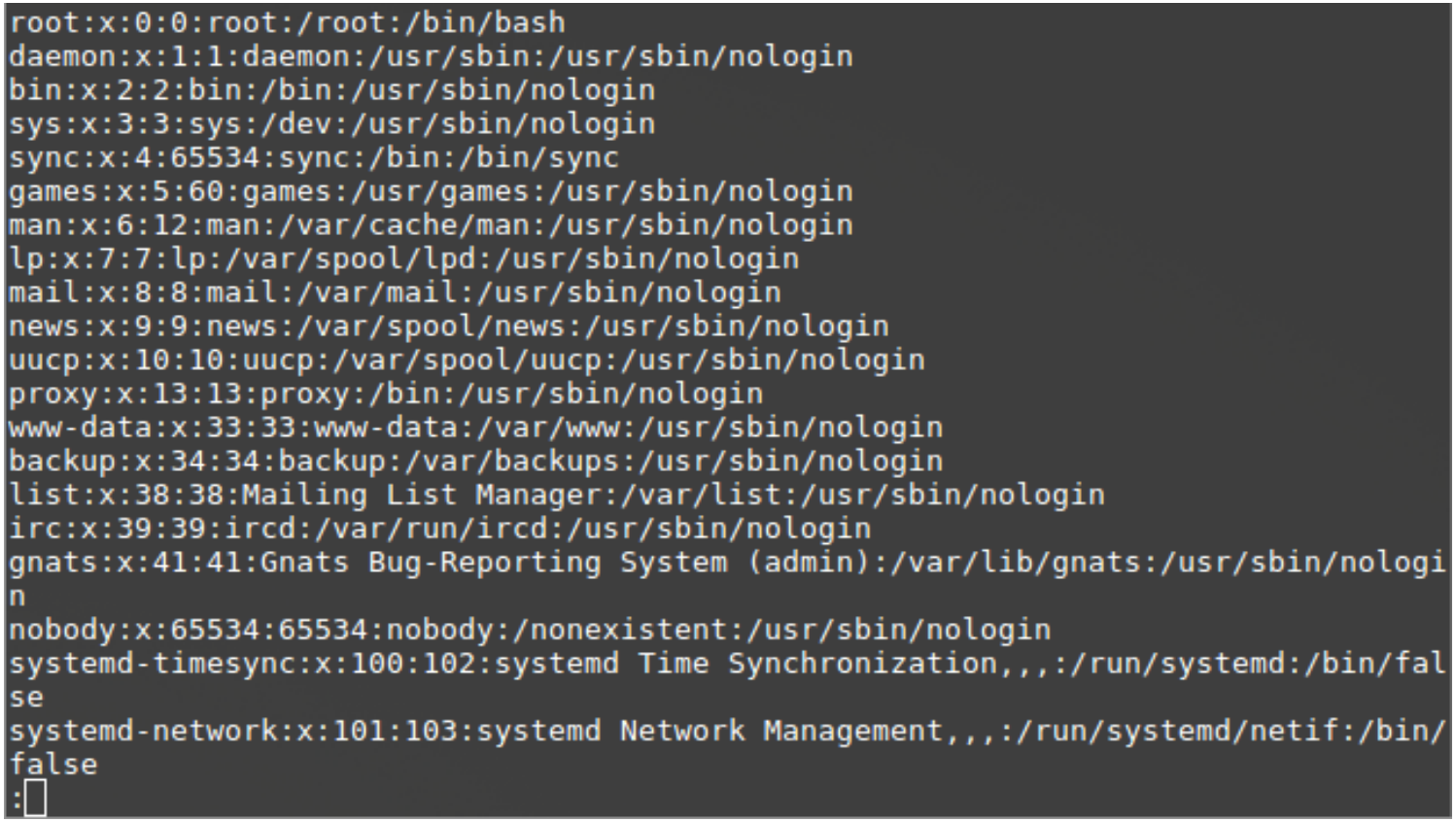
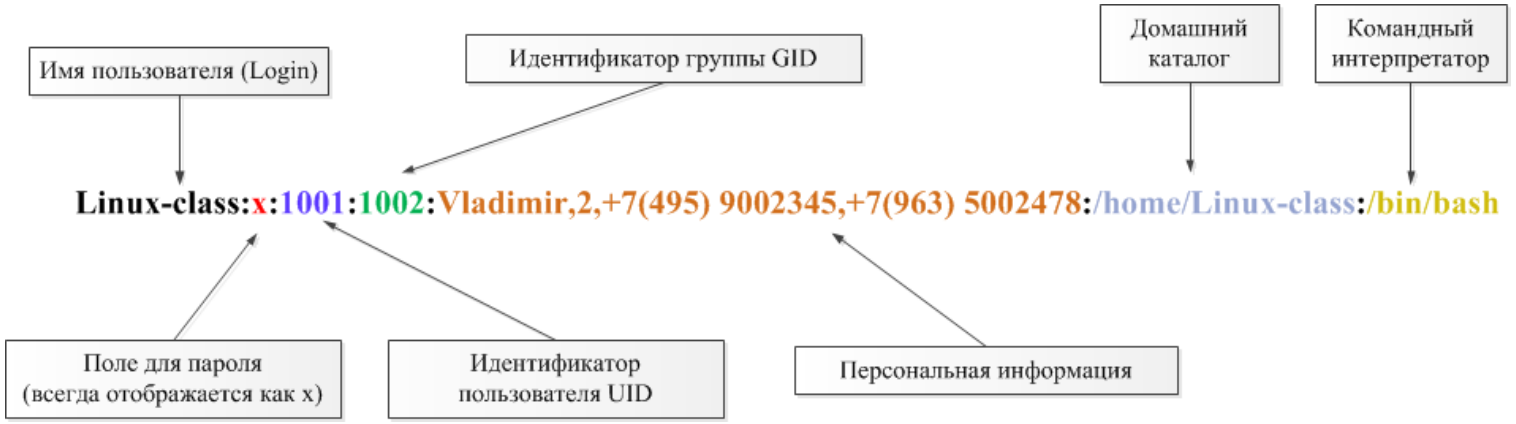


Рисунок 1. Пример содержимого файла /etc/passwd

Строка имеет следующий формат (рис. 2):

account:password:UID:GID:GECOS:directory:shell
где:
– account – имя пользователя;
– password – пароль пользователя;
– UID – идентификационный номер пользователя;
– GID – идентификационный номер основной группы пользователя;
– GECOS – необязательное поле, используемое для указания дополнительной информации о пользователе (например, полное имя пользователя);
– directory – домашний каталог ($HOME) пользователя;
– shell – командный интерпретатор пользователя (часто /bin/sh).
Символ «x» в поле пароля означает, что в системе используются теневые пароли и пароль пользователя хранится в файле **etc/shadow.**

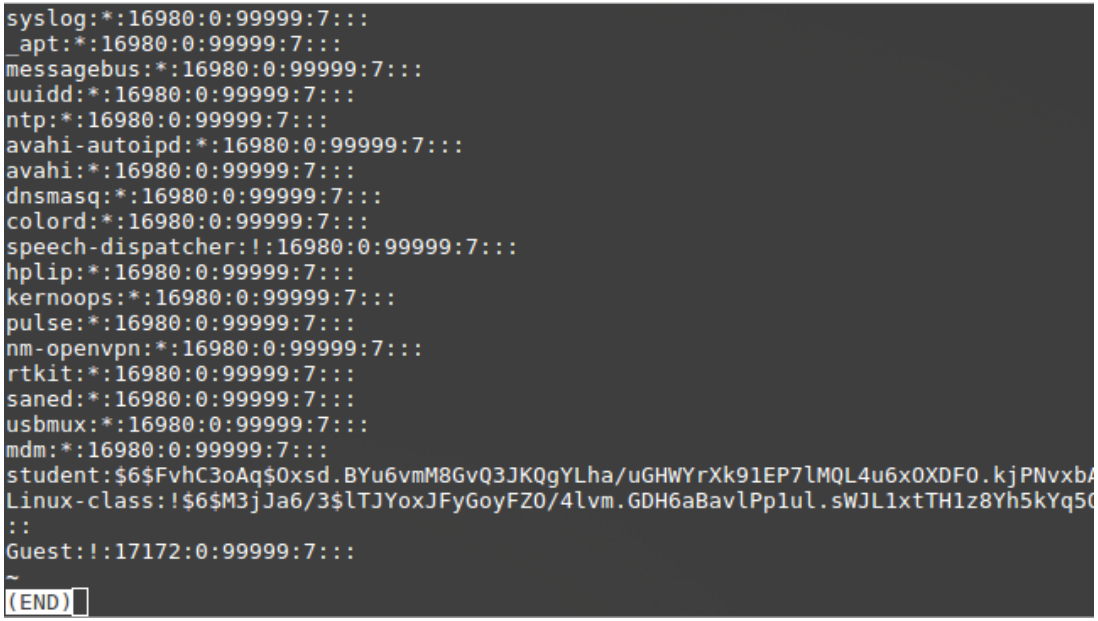
Рисунок 2.
Формат строки
файла /etc/passwd



Файл /etc/shadow

Этот файл содержит информацию о паролях пользователей. Пароли хранятся в цифрованном виде, то есть когда вводится новый пароль его шифрует хэш-функция и в дальнейшем уже сравниваются лишь хэши.
Пример файла /etc/shadow показан на рис. 3.

Рисунок 3.
Пример содержимого файла /etc/shadow



Каждая строка файла содержит поля (рис. 4):
– регистрационное имя;
– пароль в зашифрованном виде;
– дата последнего изменения пароля;
– минимальное количество дней между изменениями пароля;
– максимальное количество дней между изменениями пароля;
– количество дней до выдачи сообщения об окончании срока действия пароля;
– количество дней (по истечению срока действия пароля) до автоматического аннулирования учётной записи;
– период действия учётной записи;
– зарезервированное поле.

Рисунок 4.
Формат строки файла /etc/shadow

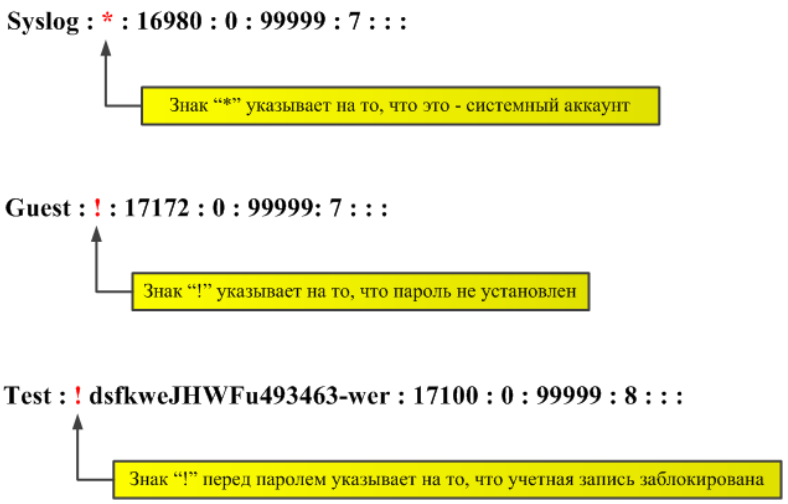


Рисунок 5. Символы «*» и «!» в строках файла /etc/shadow

Обязательными являются первые два поля. Формат полей дат соответствует количеству дней, прошедших с первого января 1970 года. Поле с регистрационным именем заполняется соответствующим значением из файла /etc/passwd. Седьмое поле содержит значение, которое определяет по истечении какого времени (в днях) после устаревания пароля учётная запись будет автоматически отключена. В восьмом поле, для установки даты истечения срока действия учётной записи можно использовать команду usermod в формате гггг-мм-чч.

Символ «*» в поле пароля устанавливается только у системных пользователей и означает, что нельзя войти в систему от имени системного пользователя (рис. 5).

Если перед хэшем пароля расположен символ «!», то это означает, что пароль и учетная запись заблокированы и пользователь не сможет войти в систему (рис. 5).

Если после знака “!” нет хэша, то пароль не установлен и учетная запись временно заблокирована до тех пор, пока не установят пароль (рис. 5).

Файл etc/group

Файл etc/group предназначен для хранения сведений о группах. Пример файла etc/group показан на рис. 6.

Рисунок 6. Пример файла etc/group

Информация о каждой группе содержится в отдельной строке. Строка имеет следующий формат (рис. 7):

– имя группы;
– идентификатор группы (GID);
– список пользователей, входящих в группу.

Рисунок 7.
Формат строки файла
etc/group

Файл /etc/gshadow

Файл предназначен для хранения паролей групп. Пример файла приведен на рис. 8.

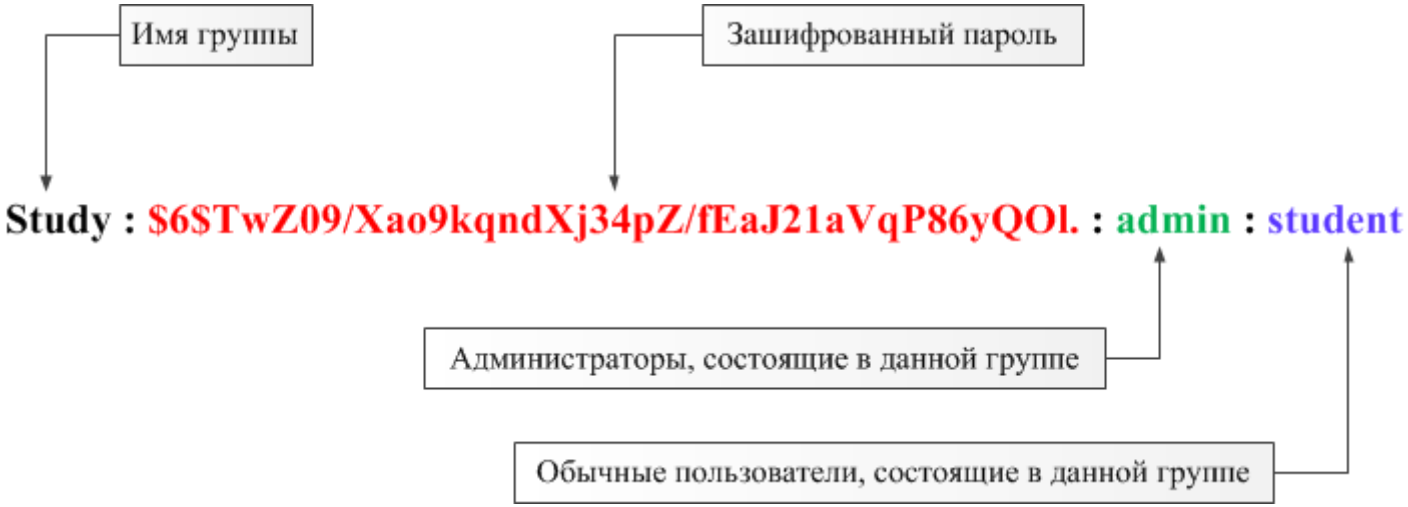
Рисунок 8. Пример файла /etc/gshadow

```
root:*::
daemon:*::
bin:*::
sys:*::
adm:*::syslog
tty:*::
disk:*::
lp:*::
mail:*::
news:*::
uucp:*::
man:*::
proxy:*::
kmem:*::
dialout:*::
fax:*::
voice:*::
cdrom:*::
floppy:*::
tape:*::
sudo:$6$/A1W33qrGd$40hOfbsYxNe9sQGakFcEIM.m6ZEVtN7bNEiaXHOMIi3x/7RVw3EBxP3e7VTs6
XtdRitDoZmh.t5yCi2Ai4HQK.::
audio:*::pulse
/etc/gshadow
```

Каждая строка файла содержит информацию о пароле группы в формате:

– имя группы;
– зашифрованный пароль;
– администраторы через запятую;
– обычные пользователи через запятую.

Рисунок 9.
Формат строки файла
/etc/gshadow



Каталог /etc/skel/

Символ «*» присутствует в поле пароля у системных групп. Пароли этих групп может менять только суперпользователь. Когда пароль устанавливается для системных групп, то знак «*» сменяется на зашифрованный пароль.

В каталоге хранятся файлы, которые необходимы каждому пользователю, имеющему свой домашний каталог. При создании учетной записи все файлы данного каталога автоматически копируются в домашний каталог нового пользователя. Все файлы скрытые.

Ручное создание пользователей и групп

Редактирование /etc/passwd

Чтобы вручную добавить нового пользователя в систему в файл /etc/passwd, добавьте следующую строку:

testuser:x:3000:3000:test user:/home/testuser:/bin/bash

Добавлен пользователь «testuser» с идентификатором 3000. Пользователь добавлен в группу с таким же идентификатором, которая еще не создана. У пользователя установлен комментарий, гласящий **«test user»**, домашний каталог установлен как **"/home/testuser"**, а командная оболочка – как **"/bin/bash".** Сохраните файл.

Редактирование /etc/shadow

Необходимо добавить запись в /etc/shadow для этого пользователя. Скопируйте строку какого-нибудь существующего пользователя, например

drobbins: $1$12345678901234567890123456789O1:11664:0:-1:-1:-1:-1:0

Замените имя пользователя в скопированной строке на имя вашего пользователя и убедитесь что все поля (особенно старый пароль) установлены:

testuser: $1$12345678901234567890123456789O1:11664:0:-1:-1:-1:-1:0
Сохраните внесенные изменения.

Установка пароля

Теперь необходимо определить пароль для нового пользователя. Введите в командной строке команду
passwd testuser
и определите пароль пользователя.

Редактирование /etc/group

Если решено добавить созданного пользователя к уже имеющейся группе, то не понадобиться создавать новую группу в /etc/groups. Если это не так, то необходимо добавить новую группу для этого пользователя, введя в файл следующую строку:
testuser:x:3000:

Создание домашней директории

Для создания домашнего каталога нового пользователя выполните следующие команды:
cd /home
mkdir testuser
chown testuser:testuser testuser
chmod o-rwx testuser

Вход пользователя в систему

Во время входа пользователя в систему, до появления у него командной строки, происходит целый ряд событий. После ввода регистрационного имени и пароля система проверяет, может ли пользователь войти в систему. С этой целью используется содержимое файла /etc/passwd.

После успешной регистрации выполняются два файла: /etc/profile и файл .profile, расположенный в домашнем каталоге пользователя. Существуют и другие исполняемые файлы инициализации.

Файл /etc/profile

Информация файла профиля /etc/profile используется при входе в систему каждого пользователя. Этот файл обычно содержит:
- глобальные или локальные переменные среды;
- информацию о пути к файлам в переменной PATH;
- параметры терминала;
- меры безопасности;
- советы дня или сведения о причинах отказа.

Файл $HOME/.profile

После выполнения /etc/profile пользователь попадает в свой домашний каталог $HOME. В этом каталоге хранится вся личная информация пользователя. Если в $HOME имеется файл .profile, система использует его в качестве исходного файла. Установки /etc/profile могут быть переопределены при добавлении в файл .profile нового элемента с другим значением либо при выполнении команды unset. Настройка файла .profile остается в распоряжении пользователя.

top
КОМПЬЮТЕРНАЯ АКАДЕМИЯ

Основы системного администрирования и сетевых технологий