ОП.14 **Основы функционирования UNIX - систем**

ЗАНЯТИЕ 09

Команды UNIX для работы с учетными записями

Учетные записи пользователей можно:

- создавать,
- изменять,
- удалять.

Для чего в системах UNIX предусмотрены специальные команды.

Напомню, что создание, удаление и изменение учетных записей может выполнять только суперпользователь `root`.

Для версий FreeBSD и System V эти команды несколько отличаются, поэтому рассмотрим их отдельно.

Команды UNIX для работы с учетными записями

Вначале остановимся на командах, используемых в системах System V:

- `useradd` — создает новую учетную запись пользователя или изменяет информацию о нем;
- `userdel` — удаляет регистрационное имя пользователя из системы;
- `passwd` — изменяет пароль пользователя;
- `su` — выполняет команду с заменой идентификатора пользователя и группы;

Команды UNIX для работы с учетными записями

- `login` — инициализирует сессию пользователя в системе;
- `id` — отображает реальный и эффективный идентификатор пользователя и группы;
- `pwconv`, `pwunconv`, `grpconv`, `grpunconv` — выполняют преобразование обычных и теневых файлов паролей и групп;
- `pwck` — проверяет целостность файла паролей.

Команды UNIX для работы с учетными записями

Команда `useradd`, вызванная без опции `-D`, создает новую учетную запись пользователя.

При этом эта команда использует параметры командной строки и **предполагает умолчание** для остальных пара метров.

Если команда завершается успешно, то в системе будет зарегистрирована новая учетная запись пользователя.

Для него будет создан домашний каталог, в который копируются файлы инициализации.

Команды UNIX для работы с учетными записями

Вот наиболее часто используемые опции команды `useradd`:

- `-u` *`идентификатор`* — указывает идентификатор пользователя (`uid`), представляющий собой неотрицательное целое число, меньшее по значению, чем системный параметр `MAXUID`.

По умолчанию обычно используется следующий доступный `uid` из указанного диапазона.

Например, если в системе используются `uid` с номерами от 100 до 105, то следующий будет равен 106 (идентификаторы, имеющие значения 0—99, зарезер вированы системой и не могут использоваться);

Команды UNIX для работы с учетными записями

- `-o` — эта опция позволяет создать дубликат `uid` — применять ее следует крайне осторожно, поскольку обеспечение безопасности системы из-за такой неоднозначности усложняется;
- `-g` *`группа`* — представляет собой целочисленный идентификатор или символьное имя существующей группы.

Эта группа устанавливается как основная (`primary`) для нового пользователя;

Команды UNIX для работы с учетными записями

- `-G` *`группа`* — представляет собой несколько элементов списка, разделенных запятыми/

Каждый элемент из этого списка является цело численным идентификатором или символьным именем существующей группы.

При этом список может состоять из одного элемента.

Содержимое списка устанавливает принадлежность пользователя к дополнительным группам, которые могут быть определены с помощью команды `newgrp`;

Команды UNIX для работы с учетными записями

- `-d` *`каталог`* — начальный (домашний) каталог нового пользователя.

По умолчанию в качестве начального используется каталог *`HOME/registration_name`*, где:

- *`HOME`* — базовый каталог для начальных каталогов новых пользователей,

- *`registration_name`* — регистрационное имя нового пользователя;

Команды UNIX для работы с учетными записями

- `-s shell` — полный путь к командному интерпретатору, используемому пользователем сразу же после регистрации.

По умолчанию этому полю значение не присваивается.

Поэтому система использует стандартный командный интерпретатор `/usr/bin/sh`.

Для командной оболочки `shell` нужно указывать существующий исполняемый файл;

Команды UNIX для работы с учетными записями

- `-c` *`комментарий`* — любая текстовая строка, кратко описывающая регистрационное имя.

Обычно указывает фамилию и имя реального пользователя.

Эта информация хранится в записи пользователя в файле `/etc/passwd`, а размер данного поля не должен превышать 128 символов;

- `-m` — создает домашний каталог для нового пользователя, если таковой отсутствует.

Если каталог уже существует, вновь созданный пользователь должен обладать правами доступа к указанному каталогу;

Команды UNIX для работы с учетными записями

- `-k skel_dir` — выполняет копирование содержимого каталога `skel_dir` в начальный каталог нового пользователя вместо использования стандартного "шаблонного" каталога `/etc/skel`, который содержит стандартные файлы, определяющие среду работы пользователя.

Каталог `skel_dir` должен существовать до выполнения операции;

Команды UNIX для работы с учетными записями

- `-f` *`активно_дней`* — максимально допустимый **интервал времени в днях** между использованиями регистрационного имени пользователя, когда это имя еще не объявляется недействительным.

Обычно в качестве значений указываются положительные целые числа;

Команды UNIX для работы с учетными записями

- `-e` *`дата`* — дата, начиная с которой регистрационное имя пользователя нельзя будет использовать.

После этой даты ни один пользователь не сможет войти в систему, введя данное регистрационное имя;

- `login` — строка символов, задающая регистрационное имя для нового пользователя.

В ней не должны присутствовать символы двоеточия и перевода строки, а первый символ не должен быть прописной буквой.

Команды UNIX для работы с учетными записями

Рассмотрим пример создания учетной записи пользователя с регистрационным именем `user1`, который будет работать в операционных системах Solaris и Linux.

Как обычно, для создания учетной записи пользователя необходимо зарегистрироваться в системе как суперпользователь `root`.

Вначале просмотрим опции по умолчанию для команды `useradd` — эта информация может оказаться полезной при создании и модификации учетных записей.

Команды UNIX для работы с учетными записями

Они могут быть такими:

```
# useradd -D
GROUP=100
HOME=/home
EXPIRE=
SHELL=/bin/bash
```

Команды UNIX для работы с учетными записями

Результат выполнения этой команды позволяет сделать несколько важных выводов:

- в качестве корневого каталога для вновь создаваемых пользователей выбран каталог `/home`;
- пустое поле значения параметра `EXPIRE` означает, что учетная запись пользователя никогда не будет заблокирована;
- в качестве командного интерпретатора для всех вновь создаваемых пользователей по умолчанию установлен `/bin/bash`.

Команды UNIX для работы с учетными записями

Для создания учетной записи пользователя `user1` введем команду:

```
# useradd user1
```

Если команда выполнена успешно, то учетная запись пользователя `user1` будет зарегистрирована в системе.

А в файл `/etc/passwd` будет добавлена примерно такая запись:

```
user1:x:2307:2307::/home/user1:/bin/bash
```

Команды UNIX для работы с учетными записями

Команда `useradd` автоматизирует процесс регистрации пользователя.

Но можно сделать это вручную, если нужно установить какие-либо индивидуальные параметры для пользователя.

Например, командную оболочку или домашний каталог.

Предположим, необходимо создать учетную запись пользователя с регистрационным именем `user2`.

Команды UNIX для работы с учетными записями

Вначале просмотрим файл `/etc/passwd/` на предмет поиска наибольшего значения идентификатора пользователя `uid`.

Наибольшее значение `uid`, равное 2307, имеет вновь созданный пользователь `user1`.

Поэтому следующим значением `uid` может быть 2308.

Добавим в файл `/etc/passwd` запись о пользователе `user2`, введя команду `echo`:

```
# echo user2:x:2308:2308::/home/user2:/bin/bash >>
/etc/passwd
```

Команды UNIX для работы с учетными записями

Далее создадим начальный каталог пользователя `user2`:

```
# mkdir /home/user2
```

Пользователя `user2` сделаем владельцем каталога `/home/user2`:

```
# chown user2  /home/user2
```

Приводим в соответствие записи файлов `/etc/passwd` и `/etc/shadow` с помощью команды `pwconv`:

```
# pwconv
```

Команды UNIX для работы с учетными записями

Команда `pwconv` создает файл `shadow` из `passwd`, при этом может использоваться и существующий файл `shadow` (он будет перезаписан).

Команда работает следующим образом:

1. Удаляются записи в теневом файле `shadow`, отсутствующие в основном файле паролей `passwd`.

2. Обновляются теневые записи, для которых в полях пароля в основном файле не стоит "x". Добавляются все недостающие теневые записи.

3. Пароли в основном файле заполняются символами "x".

Команды UNIX для работы с учетными записями

Удалить учетную запись пользователя в операционных системах System V можно с помощью команды `userdel`.

Она удаляет информацию о пользователе из системы, выполняя соответствующие изменения в регистрационных файлах и файловой системе.

Дополнительно `userdel` запоминает идентификатор `uid` удаляемого пользователя в файле `/etc/security/ia/ageduid`, чтобы исключить повторное использование этого идентификатора в течение определенного периода времени — такой механизм называется "устареванием идентификатора" (`uid aging`).

Команды UNIX для работы с учетными записями

Команда имеет синтаксис:

`userdel [-r] [-n месяцев] имя`

Опции имеют такой смысл:

- `-r` — удаление начального каталога пользователя из системы (каталог должен существовать).

При успешном выполнении команды файлы и подкаталоги в домашнем каталоге будут недоступны;

Команды UNIX для работы с учетными записями

- *-n_месяцев* — задает интервал времени в месяцах, указывающий, как долго идентификатор пользователя должен устаревать перед повторным использованием.

Если параметр равен –1, то идентификатор пользователя никогда не будет повторно использован/

Если он равен 0, то идентификатор пользователя можно использовать немедленно.

Если опция *-n* не задана, принимается значение устаревания по умолчанию.

Команды UNIX для работы с учетными записями

Изменить параметры учетной записи пользователя в системах System V можно при помощи команды `usermod`.

Эта команда модифицирует файлы, содержащие информацию об учетных записях пользователей.

Допустимы следующие опции:

- `-A` *`метод`*`|DEFAULT` — указывает новый метод идентификации пользователя и представляет собой имя программы, отвечающей за допустимую идентификацию пользователя. Строку `DEFAULT` можно использовать для установки стандартного метода идентификации;

Команды UNIX для работы с учетными записями

- `-c` *`комментарий`* — указывает на другой комментарий для записи пользователя в файле паролей;
- `-d` *`домашний_каталог`* — новый домашний каталог пользователя.

При указании опции `-m` содержимое текущего домашнего каталога будет перемещено в новый домашний каталог, который будет создан, если еще не существует;

- `-e` *`дата`* — дата, после которой учетная запись пользователя устареет.

Дата указывается в формате `MM/DD/YY`;

Команды UNIX для работы с учетными записями

- `-f` *`активно_дней`* — число дней между датой устаревания пароля и датой, когда учетная запись пользователя будет заблокирована.

Значение, равное `0`, блокирует учетную запись пользователя в момент устаревания пароля, а значение `–1` запрещает блокировку (значение по умолчанию);

- `-g` *`группа`* — имя группы или номер группы, которые будут присвоены пользователю после входа в систему, причем группа с указанным именем должна существовать.

Номер группы также должен ссылаться на существующую группу (по умолчанию равен `1`);

Команды UNIX для работы с учетными записями

- `-G` *`дополнительная_группа`* — список дополнительных групп.

Данный пользователь также является членом этих групп.

Каждая группа отделяется от следующей группы запятой, без пробелов.

Группы являются предметом для некоторых ограничений, например, группа, заданная с опцией `-g`.

Если пользователь является членом группы, которая не находится в списке, то пользователь будет удален из группы;

Команды UNIX для работы с учетными записями

- `-l` *`новое_имя`* — имя пользователя будет изменено с `имя` на `новое_имя`.

Ничего другого сделано не будет.

В частности, домашний каталог пользователя должен быть, вероятно, изменен;

- `-s shell` — имя командного интерпретатора, который будет использоваться новым пользователем при входе в систему.

Установка этого поля в пустое значение будет выбирать системный `shell` по умолчанию;

Команды UNIX для работы с учетными записями

- `-u` *`uid`* — числовое значение идентификатора пользователя *`uid`*. Это значение должно быть уникальным, исключение составляет использование опции `-o`.

Значение должно быть положительным. Как было сказано ранее, значения между **0** и **99** обычно зарезервированы для системных бюджетов. Для любых файлов, владельцем которых является пользователь, и которые находятся в домашнем каталоге пользователя, иден тификатор пользователя *`uid`* будет изменяться автоматически.

Для файлов вне домашнего каталога пользователя идентификатор пользователя должен быть изменен

Команды UNIX для работы с учетными записями

Важное замечание: если пользователь находится в системе, изменить его имя не удастся.

Вот пример использования команды `usermod`.

Предположим, требуется изменить регистрационное имя пользователя `user2`, созданного ранее, на `moduser2`, а его домашний каталог — на `/home/moduser2`.

Исходная запись для пользователя `user2` в файле `/etc/passwd` выглядит так:

```
user2:x:2308:2308::/home/user2:/bin/bash
```

Команды UNIX для работы с учетными записями

Следующая команда выполняет все необходимые изменения:

```
# usermod -l moduser2 -d /home/moduser2 -m user2
```

После выполнения этой команды запись для пользователя `moduser2` в файле `/etc/passwd` должна выглядеть примерно так:

```
moduser2:x:2308:2308::/home/moduser2:/bin/bash
```

Легко проверить и наличие домашнего каталога пользователя `moduser2`, задав команду:

```
#  ls -l /home
drwxr-xr-x  10 moduser2    4096 Aug   18 22:51 moduser2
```

Команды UNIX для работы с учетными записями

Здесь нужно сделать одно важное замечание: при изменении регистрационного имени пользователя его `uid` остается неизменным.

Это свидетельствует о том, что операционная система ра ботает с одной и той же учетной записью пользователя, несмотря на то, что регистрационное имя пользователя изменилось.

Таким образом, можно сделать очень важный вывод: для UNIX определяющим фактором при работе с пользователем является его идентификатор `uid`, а не регистрационное имя пользователя, которое может изменяться.

Команды UNIX для работы с учетными записями

Проанализируем команду `passwd` — с ее помощью можно изменить пароли пользователей.

При этом обычные пользователи могут изменить пароль только для своей учетной записи.

В то время как суперпользователь `root` может это сделать для любого пользователя.

Команды UNIX для работы с учетными записями

Кроме этого, `passwd` позволяет изменить информацию об учетной записи:

- полное имя пользователя,
- его командный интерпретатор,
- дату истечения срока используемого пароля,
- интервал времени, в течение которого пароль действует.

Команды UNIX для работы с учетными записями

Команда имеет синтаксис:

```
passwd [-f] имя
passwd [-g] [-r|-R] группа
passwd [-x max] [-n min] [-w warn] [-i inact] имя
passwd {-l|-u|-d|-S} имя
```

Команды UNIX для работы с учетными записями

Для пользователей, имеющих пароль, перед установкой нового пароля команда `passwd` предлагает ввести текущий пароль (он хранится в зашифрованном виде).

Обычному пользователю дается только одна попытка для ввода правильного пароля. Супер-пользователь `root` может пропустить этот шаг, что оказывается полезным, если пароль забыт, поскольку его можно изменить даже в этом случае.

После ввода пароля `passwd` проверяет наличие разрешения на изменение пароля в данное время — если это невозможно, команда завершает работу, не изменив пароль.

Команды UNIX для работы с учетными записями

Вот смысл некоторых опций команды `passwd`:

- `-g` — замена пароля для заданной группы — может быть выполнена только суперпользователем `root` или администратором группы.

Может быть использована вместе с опцией `-r` для удаления текущего пароля заданной группы, что делает группу доступной всем членам.

Вместе с опцией `-R` используется для ограничения доступа к группе всем пользователям;

Команды UNIX для работы с учетными записями

- `-x` — используется для установки максимального числа дней, в течение которых пароль остается допустимым, при этом после *max* дней требуется его изменение;
- `-n` — служит для установки минимального числа дней. После истечения этого срока пароль может быть изменен.

При этом пользователю запрещается изменять пароль в течение *min* дней;

Команды UNIX для работы с учетными записями

- `-w` — предназначена для установки числа дней.

В течение этих дней пользователь будет получать предупреждающее сообщение об истечении времени действия его пароля.

При этом сообщения будут выводиться в течении *warn* дней, напоминая пользователю, сколько дней осталось до момента устаревания его пароля;

Команды UNIX для работы с учетными записями

- `-i` — запрещает использование учетной записи пользователя по истечению промежутка времени после устаревания пароля.

При этом, если устаревший пароль остается неизменным в течение *inact* дней, он не будет вновь принят системой;

- `-l` — блокирует учетную запись, изменяя пароль таким образом, что он становится непригодным для шифрования;

Команды UNIX для работы с учетными записями

- `-u` — разблокирует учетную запись, изменяя пароль к его предыдущему значению;
- `-S` — вывод статусной информации учетной записи.

Статусная информация состоит из шести полей, первое из которых кодируется следующим образом:

- `L` — если бюджет пользователя заблокирован;
- `NP` — если не существует пароля для данной учетной записи;
- `P` — если пароль используется.

Команды UNIX для работы с учетными записями

Второе поле указывает дату последнего изменения пароля.

Следующие четыре поля:

— минимальное время до истечения срока действия пароля,

— максимальное время до истечения срока действия пароля,

— период вывода предупреждающего сообщения об истечении срока действия пароля,

— период неактивности для этого пароля;

- `-f` — требует от пользователя изменить пароль при следую

Команды UNIX для работы с учетными записями

От выбора пароля во многом зависит безопасность операционной системы.

Кроме того, существенную роль в этом играет алгоритм шифрования и размера ключа, используемый в данной UNIX-системе.

В большинстве операционных систем метод криптографии основывается на алгоритме NBS DES, который имеет очень высокую степень безопасности, при этом размер ключа зависит от выбранного пароля.

Команды UNIX для работы с учетными записями

Лучше **не выбирать** пароль, в котором используются литературные выражения, или основанный на личных данных (месяц, год рождения и т. д.).

Такой пароль злоумышленнику расшифровать несложно.

Конечно, пароль должен быть хорошо запоминаем.

Для этого одним из вариантов может быть знакомое слово, части которого разделены специальными символами.

Команды UNIX для работы с учетными записями

Пароль может представлять собой комбинацию из двух слов, объединенных вместе и разделенных специальными символами или цифрами.

Примерами таких паролей являются:

```
P!e%ter$sbu)rg
```

и

```
n*ew!Pas#s%w$ord.
```

Команды UNIX для работы с учетными записями

Организация учетных записей в системах, совместимых с BSD, принципиально не отличается от остальных.

Отличия заключаются в следующем:

- используется файл `/etc/master.passwd`, являющийся в некотором смысле аналогом файла `/etc/shadow`, используемого в системах, совместимых с System V.

Файл `/etc/master.passwd` хранит ту же информацию, что и `/etc/passwd`, хотя имеются и некоторые отличия.

Команды UNIX для работы с учетными записями

Здесь хранятся хеш-коды (шифры) пользовательских паролей, а также зашифрованные пароли пользователей, поэтому он доступен для чтения только суперполь зователю `root`;

- для управления учетными записями применяются команды с иной мнемоникой, чем в System V.

Для создания учетных записей пользователей применяется утилита `adduser`, которая выводит подсказки с предлагаемыми настройками, при этом синтаксис команды во многом напоминает тот, что используется для `useradd`.

Команды UNIX для работы с учетными записями

Команда `chpass` применяется для изменения учетных записей пользователей в FreeBSD.

Она позволяет изменять параметры учетной записи, включая пароль, срок действия учетной записи и стандартный интерпретатор команд.

Имеет следующий синтаксис:

```
chpass [-a список] [-p зашифрованный_пароль] [-e
срок_действия]
        [-s интерпретатор] [login]
```

Команды UNIX для работы с учетными записями

Опции команды означают следующее:

- `-a` *`список`* — позволяет суперпользователю определять полную запись в формате `/etc/passwd`;
- `-p` *`зашифрованный_пароль`* — разрешает изменить пароль, предварительно зашифрованный командой `crypt`.

Эта опция используется в командных файлах, содержащих команду `crypt` и передающих полученный результат команде `chpass`;

- `-e` *`срок_действия`* — задает срок действия учетной записи;

Команды UNIX для работы с учетными записями

- `-s` интерпретатор — обеспечивает смену стандартного интерпретатора команд на указанный;
- `login` — задает модифицируемую учетную запись.

Чаще всего команда `chpass` используется без параметров или с единственным параметром `login` — в этом случае запускается редактор, с помощью которого можно изменить параметры учетной записи.

Команды UNIX для работы с учетными записями

Учетные записи пользователей FreeBSD можно отредактировать вручную непосредственно в файле `/etc/master.passwd`.

После чего распространить изменения на другие файлы с помощью команды `pwd_mkdb`:

```
#pwd_mkdb   -p   /etc/master_passwd
```

Команды UNIX для работы с учетными записями

Еще одна команда — `rmuser` — служит для удаления пользователя и информации, связанной с данной учетной записью.

Имеет такой синтаксис:

```
rmuser [-y] login
```

Команды UNIX для работы с учетными записями

Команда выполняет последовательность действий:

- уничтожает процессы, инициированные пользователем;
- удаляет задания демона `cron`, запланированные пользователем;
- удаляет задания команды `at`, запланированные пользователем;
- удаляет относящиеся к пользователю записи из файлов паролей (`/etc/passwd`, `/etc/master.passwd`);

Команды UNIX для работы с учетными записями

- удаляет почтовую очередь пользователя из каталога `/var/mail`;
- удаляет файлы пользователя из каталогов `/tmp`, `/var/tmp`, `/var/tmp/vi.recover`;
- удаляет учетную запись пользователя из всех групп в файле `/etc/group` и саму группу, если пользователь является ее единственным членом;
- интерактивно позволяет удалить начальный каталог пользователя.

Команды UNIX для работы с учетными записями

Группы пользователей в системе FreeBSD можно создавать либо с помощью программы `sysinstall`, либо вручную, редактируя файл `/etc/group`.

Как видно из обзора, команды управления учетными записями пользователей System V и FreeBSD очень похожи и используют однотипные параметры.

Рассмотренные здесь команды являются основными для управления учетными записями пользователей, хотя кроме них имеется целый ряд других утилит, позволяющих выполнить более узкие задачи. Дополнительную информацию о таких командах можно получить из man-страниц операционной системы.

Список литературы:

1. Юрий Магда. UNIX для студентов, Санкт-Петербург «БХВ-Петербург», 2007.
2. Unix и Linux: руководство системного администратора, 4-е издание, 2012, Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли
3. Организация UNIX систем и ОС Solaris 9, Торчинский Ф.И., Ильин Е.С., 2-е издание, исправленное, 2016.

Спасибо за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru