Лабораторная работа №4
Управление пользователями и группами

Введение

Из этой лабораторной работы вы узнаете от том, что такое POSIX идентификаторы и чем они отличаются от SID'ов из мира Windows. Мы посмотрим, в каких файлах хранится информация о локальных пользователях и группах и как редактировать эти файлы с помощью стандартных утилит.

Аутентификация в системе Linux

В операционной системе Linux функция аутентификации вынесена отдельно от приложений и реализована в виде подключаемых модулей аутентификации (*от англ. Pluggable Authentication Modules, PAM*). Поэтому приложениям, таким как login, достаточно получить у пользователя учетные данные и передать их библиотеке libpam.

Этот подход хорошо зарекомендовал себя, так как позволяет встраивать в систему новые способы *аутентификации*, не изменяя исходного кода прикладных приложений. И, более того, для разных приложений можно использовать разный состав модулей и запускать их с разными параметрами — за эти настройки отвечают файлы из каталога `/etc/pam.d`

Возможности PAM-стека отлично дополняются функциями Диспетчера службы имен (*от англ. Name Service Switch, NSS*). Если PAM-стек обеспечивает разные способы аутентификации, то система NSS позволяет подключать различные источники для извлечения информации о пользователях, паролях и группах.

Сравнивая содержимое файлов `/etc/nsswitch.conf` на разных компьютерах, вы сможете заметить, что на обычном компьютере используются только локальные базы, которые обозначаются как *file* и *db*, а на доменных компьютерах появляется дополнительный источник *sss*, который позволяет извлекать информацию из домена через службу SSSD:

```
sa@astra:~$ cat /etc/nsswitch.conf

passwd:         files sss
group:          files sss
shadow:         files sss

hosts:          files dns
networks:       files
```

```
protocols:      db files
services:       db files sss
ethers:         db files
rpc:            db files

netgroup:       nis sss
sudoers:        files sss

automount:      sss
```

Источники NSS строго формализованы и должны предоставлять типовой набор данных, например, база пользователей passwd должна содержать: имя пользователя, хеш пароля, идентификатор пользователя UID, идентификатор первичной группы GID, атрибут GECOS, пути к домашнему каталогу и оболочке командной строки.

Это не означает, что все атрибуты должны быть «заполнены». Например, PAM-модулю службы SSSD не требуется прямой доступ к хешам паролей всех пользователей, т.к. аутентификация может быть выполнена через контроллер домена по сетевому протоколу Kerberos V5. Однако информация об идентификаторах UID/GID и участии пользователей в группах нужна системе обязательно, т.к. без нее не будет работать авторизация доступа к локальным ресурсам.

Примечание

В системе Windows аналогом технологий PAM и NSS является система аутентификации, которая включает в себя такие компоненты, как Локальный центр безопасности (Local Security Authority, LSA), Интерфейс поставщика поддержки безопасности (Security Support Provider Interface, SSPI) и другие.

Подсистема LSA управляет аутентификацией пользователей, авторизацией и контролем доступа, а программный интерфейс SSPI обеспечивает различные методы аутентификации, включая Kerberos, NTLM и др.

Компоненты Windows тоже имеют модульную архитектуру, что позволяет расширять их функциональность. Например, довольно часто разработчики средств защиты информации встраивают в Windows LSA свои фильтры паролей для их проверки на соответствие дополнительным требованиям.

Идентификаторы SID, UID и GID

В Windows у всех субъектов безопасности (пользователей, групп, служебных учетных записей и т.д.) есть уникальный идентификатор безопасности, который представляет собой строку вида:

```
S-R-IA-SA-SA-RID
```

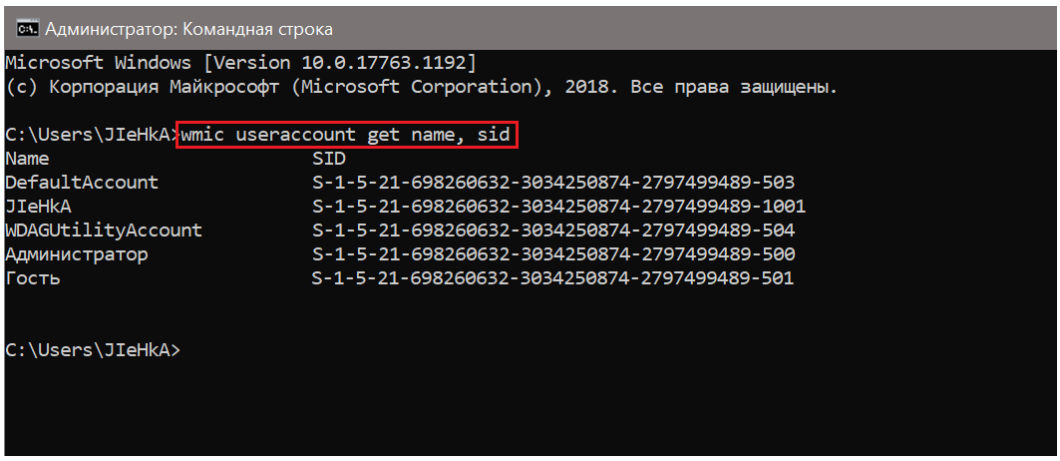
Например, идентификатор доменного пользователя *iivanov@ALD.COMPANY.LAN*:

```
S-1-5-21-2174213541-4214376712-4023651427-1006
```

Именно по этим идентификаторам, а не по именам, обеспечивается доступ пользователей к ресурсам. Рассмотрим подробно, что означает каждая из частей идентификатора:

- **S** — указывает на то, что строка является идентификатором безопасности Windows.
- **R** — первое число является номером редакции (revision). До второй версии дело так и не дошло, поэтому у всех SID'ов в этой части будет указана единица.
- **IA** — источник выдачи (issuing authority). Практически все идентификаторы безопасности в операционной системе Windows указывают NT Authority номер 5. Исключением являются универсальные широко известные (universal well-known) учётные записи групп и пользователей, например, идентификатор создателя объекта S-1-3-X (англ. SECURITY_CREATOR_SID_AUTHORITY).
- **SA** — идентификатор уполномоченного центра (sub-authority), который выдал идентификатор безопасности. Первое число определяет специальные группы и функции, например, 21 указывает, что идентификатор безопасности был выдан контроллером домена или изолированным компьютером. Далее идут три числа, которые идентифицируют компьютер/домен. Эти числа генерируются автоматически в момент установки ОС, поэтому в домене недостаточно просто клонировать машину и обязательно требуется выполнить процедуру sysprep, которая повторно генерирует это значение.
- **RID** — относительный идентификатор (Relative Identifier). Это целое число в диапазоне от 0 до 2^{31} (до 2 млрд.), которое уникально идентифицирует субъект безопасности в пределах компьютера или домена. Относительные идентификаторы обычных пользователей начинаются с 1 000. В нашем примере это значение равно 1 006.

Чтобы посмотреть значения SID на Windows, нужно запустить командную строку с правами администратора и выполнить команду `wmic useraccount get name, sid`:



Теперь разберем несколько особенностей идентификаторов Linux:

- Если в Windows идентификатор SID используется для всех субъектов, то в Linux для пользователей и групп используются разные идентификаторы. Идентификаторы пользователей называются UID (от англ. User Identifier), идентификаторы групп называются GID (*от англ. Group Identifier*), а все вместе они называются POSIX-идентификаторами по названию стандартов, которым следуют *nix-подобные системы (*англ. Portable Operating System Interface — переносимый интерфейс операционных систем*).
- Оба вида идентификаторов представляют собой целые числа в диапазоне от 0 до 2^{32} (4 294 967 296). Идентификаторы в диапазоне 0-99 обычно резервируются под систему, в диапазоне 100-999 используются для разного рода служб (например, Apache). А все, что начинается с 1000, отдается пользователям. Astra Linux следует этой практике, но в других дистрибутивах подходы могут отличаться, поэтому смотрите файл /etc/login.defs, какие значения там определены для переменных UID_MIN, UID_MAX, GID_MIN и GID_MAX.
- Как вы можете заметить, максимальный размер идентификаторов в 4 млрд сопоставим с емкостью относительных идентификаторов Windows. Однако у POSIX-идентификаторов нет уникальной доменной части, поэтому получается, что все пользователи и группы Linux находятся как бы в одном большом домене. Это может стать проблемой при необходимости объединения двух инфраструктур, но есть разные способы решения этой проблемы. Например, служба каталога ALD Pro (FreeIPA) выделяет для каждого нового домена 200 тыс. идентификаторов в случайном месте этого диапазона, что значительно снижает вероятность конфликта.
- Обе системы имеют так называемые широко известные идентификаторы (*от англ. well-known identifiers*). Например, у администратора Windows SID заканчивается на `...-500`, а у группы администраторов на `...-512`. В системе Linux у суперпользователя root и его первичной группы идентификаторы всегда равны 0. И эти значения желательно помнить наизусть.
- Еще одним существенным отличием Linux от Windows являются первичные группы пользователей. Дело в том, что в Linux при создании файлов и папок нужно обязательно указать не только пользователя-владельца, но и группу, которая будет считаться владельцем этого объекта. По этой причине пользователям был добавлен атрибут «первичная группа», значение которого проставляется у новых объектов файловой системы.

Однако использовать какую-нибудь общую группу Users в качестве первичной группы для всех новых пользователей будет небезопасно. В этом случае пользователи смогут получить доступ к личным файлам друг друга, что крайне нежелательно в многопользовательских системах. Поэтому в Linux при создании нового пользователя

система автоматически создает одноименную группу, идентификатор которой записывает в качестве первичной группы пользователя.

Примечание

Идентификаторы пользователей иногда совпадают с идентификаторами их первичных групп. Например, у пользователя root идентификатор UID равен 0, и у группы root идентификатор GID тоже равен 1. Но следует понимать, что это не считается какой-то лучшей практикой и для большинства обычных пользователей эти значения будут расходиться. Например, в системе Astra Linux автоматически создается группа astra-admin с GID=1001, поэтому при создании нового пользователя ему будет присвоен первый свободный UID=1001, а идентификатор его группы будет GID=1002.

Формат хранения информации об учетных записях пользователей и групп

В Windows данные об учетных записях хранятся в реестре Windows NT, а именно в файле SAM (от англ. Security Account Manager). Этот файл находится на жестком диске в каталоге `%windows%/system32/config`. Система имеет единоличный доступ к этому файлу, и пока она загружена, доступа к нему нет даже у администраторов.

В Linux для хранения данных об учетных записях локальных пользователей, их паролей и групп используется несколько баз данных, которые представляют собой обычные текстовые файлы:

- `/etc/passwd` — база пользователей
- `/etc/shadow` — база паролей пользователей
- `/etc/group` — база групп
- `/etc/gshadow` — база паролей групп

Рассмотрим каждую их этих баз данных отдельно.

Хранение учетных записей пользователей (/etc/passwd)

В файле `/etc/passwd` хранятся данные об учетных записях пользователей. Это текстовый файл, информация в котором хранится в табличном виде, а разделителем столбцов является символ двоеточия «:». Первая строка, как правило, содержит учетную запись суперпользователя root, а новые учетные записи добавляются в конец файла.

```
sa@astra:~$ cat /etc/passwd | head
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
...
sa@astra:~$ grep 1000 /etc/passwd
sa:x:1000:1000:sa,,,:/home/sa:/bin/bash
```

Формат полей файла хранения учетных данных пользователей:

Поле в таблице	Значение
Имя пользователя	sa
Хеш пароля	x
UID	1000
GID	1000
GECOS	sa,,,
Домашний каталог	/home/sa
Оболочка	/bin/bash

1. **Имя пользователя** — это строка, которую пользователь вводит при входе в систему в качестве своего имени. Имя не должно начинаться с цифр, содержать большие буквы или буквы кириллицы. Максимальная длина не более 32 символов.
2. **Хеш пароля** — уникальная строка символов, полученная после применения к исходному тексту пароля специальной хеш-функции (от англ. hash - фарш). Как фарш невозможно провернуть назад, так и хеш невозможно превратить обратно в исходные данные. Проще всего хеш-функцию представить в виде синусоиды, где бесконечному значению X соответствуют значения Y строго в интервале от -1 до 1, т.е. хеширование всегда идет с потерей данных. Например, MD5-хеш любого файла всегда будет длиной 32 символа, и не важно, была ли это PNG-картинка на пару килобайт или ISO-образ размером 5 ГБ.

В первых системах Unix хеш пароля находился непосредственно в `/etc/passwd`, но к этому файлу должен быть доступ на чтение у всех пользователей, поэтому такой подход не был защищен от взлома методом перебора. Первым, кто реализовал атаку на хеш пароля, стал Ричард Столман, основатель проекта GNU, после чего хеши перенесли в файл `/etc/shadow`, к которому есть доступ только у суперпользователя.

В этой колонке сейчас указывают значение «x», если пароль задан и находится в файле shadow, и значение «!», если пароль не задан и интерактивный вход запрещен.

3. **UID** — идентификатор пользователя.
4. **GID** — идентификатор первичной группы пользователя. Эта группа проставляется владельцем для файлов и каталогов, которые будут созданы пользователем.
5. **GECOS** — содержит несколько атрибутов, разделенных запятой:

- Полное имя пользователя или название приложения.
- Номер комнаты.
- Рабочий номер телефона.

- Домашний телефон.
- Другая контактная информация.

6. **Домашний каталог** — абсолютный путь к домашнему каталогу пользователя, в котором находятся его личные файлы. По умолчанию домашние каталоги называются по имени пользователя и располагаются в каталоге `/home`.

7. **Оболочка** — абсолютный путь к оболочке, которая запускается для пользователя при входе в терминал. В большинстве дистрибутивов Linux оболочкой входа по умолчанию является Bash, в том числе и в Astra Linux. Список установленных в системе оболочек можно посмотреть в файле `/etc/shells`.

Примечание

Изначально атрибут GECOS был добавлен для совместимости с операционной системой General Comprehensive Operating System, которую часто использовали в качестве принт-сервера. Уже и системы той нет, а атрибут остался, поэтому в него обычно записывают полное имя пользователя.

Хранение паролей пользователей. Файл /etc/shadow

Файл `/etc/shadow` содержит хеши паролей пользователей, поэтому доступ к нему должен быть только у суперпользователя. Для просмотра файла необходимо воспользоваться командой повышения привилегий `sudo`.

```
sa@astra:~$ sudo -i
[sudo] пароль для sa:
root@astra:~# cat /etc/shadow | head
root:!:19493:0:99999:7:::
daemon:*:19493:0:99999:7:::
bin:*:19493:0:99999:7:::
sys:*:19493:0:99999:7:::
sync:*:19493:0:99999:7:::
games:*:19493:0:99999:7:::
man:*:19493:0:99999:7:::
lp:*:19493:0:99999:7:::
mail:*:19493:0:99999:7:::
news:*:19493:0:99999:7:::
root@astra:~# cat /etc/shadow | grep sa
```

Строка найденная в базе по имени sa:

```
sa:$gost12512hash$Ag32kwCZw/YI1iaX$7d6oorvJr4EnfprtlXzeA6IUJzAaZ0yab1ghPbQbVGGixLxhWgI3K1qOG9W
Kkw4sh0ov/Fe4OUWZ0.p.j1oC91:19493:0:99999:7:::
```

Синтаксис файла такой же, как у passwd — информация хранится в табличном виде, разделителем столбцов является символ двоеточие «:». Как правило, первая строка в файле содержит учетную запись суперпользователя root, а для новых учетных записей информация добавляется в виде новых строк в конец файла.

Формат полей файла `/etc/shadow`:

Поле в таблице	Значение
Имя пользователя	sa
Хеш пароля	$gost12512hash$Ag32…
Последнее изменение пароля	19493
Минимальный возраст пароля	0
Максимальный возраст пароля	99999
Период предупреждения	7
Период бездействия	пусто
Срок действия уч. записи	пусто
Резерв	пусто

1. **Имя пользователя** — строка, которую вы вводите при входе в систему. Учетная запись пользователя должна существовать в системе.
2. **Хеш пароля** — уникальная строка символов, полученная после применения специальной хеш-функции исходному тексту пароля.

Хеш задается в формате $type$salt$hashed:

- **Подстрока $type** — это метод криптографического алгоритма хеширования, который может принимать следующие значения:

- **1** — алгоритм хеширования MD5
- **$2a$** — алгоритм хеширования Blowfish
- **$2y$** — алгоритм хеширования Eksblowfish
- **5** — алгоритм хеширования SHA-256
- **6** — алгоритм хеширования SHA-512
- **$gost12512hash$** — алгоритм хеширования ГОСТ Р 34.11-2012

В Astra Linux при генерации пароля применяется алгоритм защищенного преобразования ГОСТ Р 34.11.-2012.

- **Подстрока $salt$** — задает набор случайных символов, который объединяется с паролем при хешировании для усложнения взлома паролей с использованием радужных таблиц (от англ. rainbow table).
- **hashed** — само значение хеша в кодировке base64

Однако, вместо хеша ($type$salt$hashed) поле может содержать следующие специальные символы:

- Символ «*» – Если поле пароля начинается с символа звёздочка (*), то пользователь не сможет войти в систему с использованием аутентификации по паролю. Другие методы входа, такие как аутентификация на основе ключей или переключение на пользователя, по-прежнему разрешены.
- Символ «!» – Если поле пароля начинается с символа восклицательный знак (!), то пользователь вообще не сможет войти в систему даже по ключу. Пароль в этом случае считается заблокированным.

3. **Последнее изменение пароля** — это дата последнего изменения пароля в количестве дней, прошедших с 1 января 1970 года, как начала эпохи Unix. Преобразовать это значение в реальную дату можно командой: `date -d @$((19493*24*3600))`
4. **Минимальный срок действия пароля** — количество дней, которое должно пройти, прежде чем пароль пользователя может быть изменен. Как правило, минимальный срок действия пароля не задан, поэтому в этой колонке будет 0.
5. **Максимальный срок действия пароля** — количество дней, по истечении которых пароль будет считаться истекшим. Как правило, максимальный срок не задан, поэтому в этой колонке будет установлено значение 99999.
6. **Период предупреждения** — количество дней до истечения срока действия пароля, в течение которых пользователь будет получать предупреждение о необходимости изменить пароль.
7. **Период бездействия** — количество дней после истечения срока действия пароля, во время которых пароль всё ещё будет приниматься. Это поле обычно остается пустым.
8. **Срок действия учетной записи** — дата истечения срока действия учётной записи в формате timestamp, после которой учетная запись будет заблокирована. Обратите внимание, если истек срок действия учетной записи, то пользователь не сможет войти в систему. Если же закончился срок пароля, то пользователь сможет сменить его и продолжить работу.
9. **Резерв** — это поле было зарезервировано для использования в будущем. В настоящий момент не используется.
10.

Важно

Крайне не рекомендуется редактировать файл `/etc/passwd` вручную, т.к. это может привести к повреждению данных.Используйте специальные команды, например:

- `passwd` — для смены пароля;
- `fly-passwd` — для смены пароля в графическом интерфейсе;
- `chage` — для изменения срока действия пароля.

Хранение групп (/etc/group)

Файл `/etc/group` содержит информацию о группах, зарегистрированных в системе, включая информацию об участниках этих групп.

```
sa@astra:~$ cat /etc/group | head -n 25 | tail
fax:x:21:
voice:x:22:
cdrom:x:24:sa
floppy:x:25:sa
tape:x:26:
sudo:x:27:
audio:x:29:pulse,sa
dip:x:30:sa
www-data:x:33:
backup:x:34:
sa@astra:~$ grep astra-admin /etc/group
sa:x:1001:sa
```

Это текстовый файл, информация в котором хранится в табличном виде, а разделителем столбцов является символ двоеточие «:».

Формат полей файла информации о группах `/etc/group`:

Поле в таблице	Значение
Имя группы	sa
Хеш пароля	x
GID	1001
Список участников группы	sa

1. **Имя группы** — набор символов, по которым можно уникально идентифицировать группу.
2. **Хеш пароля** — аналогично с паролем пользователя хеши перенесены в файл `/etc/group`. Пароль группы позволяет пользователю самостоятельно присоединиться к группе для расширения своих прав доступа.
3. **GID** – идентификатор группы.
4. **Список участников группы** — список пользователей, разделенный запятыми без пробелов.

Хранение паролей групп (/etc/gshadow)

Файл `/etc/gshadow` хранит информацию о паролях локальных групп. Доступ к этому файлу есть только у суперпользователя, поэтому для его просмотра необходимо воспользоваться командой повышения привилегий sudo.

```
sa@astra:~$ sudo cat /etc/gshadow | head
```

```
root:*::
daemon:*::
bin:*::
sys:*::
adm:*::loaches
tty:*::
disk:*::
lp:*::
mail:*::
news:*::

sa@astra:~$ sudo cat /etc/gshadow | grep astra-admin
astra-admin:!::sa
```

Это текстовый файл, информация в котором хранится в табличном виде, а разделителем столбцов является символ двоеточие «:». Как правило первая строка в файле содержит учетную запись группы суперпользователя root, а для новых учетных записей информация добавляется в виде новых строк в конец файла.

Формат полей файла информации о паролях локальных групп `/etc/gshadow`:

Поле в таблице	**Значение**
Имя группы	astra-admin
Хеш пароля	!
Администраторы	
Участники группы	sa

1. **Имя группы** — должно содержать имя группы, которая зарегистрирована в системе.
2. **Хеш пароля** - позволяет пользователю самостоятельно присоединиться к группе для расширения своих прав доступа. Если поле содержит символ «!» или «*», то пользователь не сможет использовать пароль для доступа в группу.
3. **Администраторы** — список имён пользователей, перечисленных через запятую. Администраторы имеют те же права, как у обычных участников, и дополнительно могут изменять список участников группы и назначать новый пароль.
4. **Участники группы** — список имён пользователей, перечисленных через запятую. Участники группы могут иметь доступ к группе без ввода пароля.

Изменение файлов /etc/passwd, /etc/group и /etc/shadow

Если вы хотите изменить указанные файлы с помощью обычного текстового редактора, рекомендуется использовать специальные утилиты, которые проверяют корректность файла в момент сохранения данных:

- `vipw` – редактирование базы пользователей `/etc/passwd`
- `vipw -g` – редактирование базы групп пользователей `/etc/group`
- `vipw -s` – редактирование базы паролей пользователей `/etc/shadow`

При этом не важно, какой именно редактор вы выберете для работы – это может быть `vim`, `nano`, `mcedit`.

Резервные копии файлов /etc/passwd, /etc/group и /etc/shadow

В системе существуют резервные копии рассмотренных выше файлов (со знаком тире в конце имени файла):

- `/etc/shadow-` – резервный файл хешей паролей пользователей
- `/etc/passwd-` – резервный файл базы пользователей
- `/etc/group-` – резервный файл базы групп пользователей
- `/etc/gshadow-` – резервный файл паролей групп пользователей

Резервные копии хранят предыдущую версию файлов. Когда утилиты управления меняют пользователя или группу, они создают резервные копии основных файлов. В этом можно убедиться командой `diff`. Например, после создания пользователя выполните в терминале команду `diff /etc/passwd /etc/passwd-`.

Управление учетными записями пользователей из командной строки

Просмотр учетных записей пользователей

Список учетных записей можно посмотреть в файле `/etc/passwd`:

```
sa@astra:~$ less /etc/passwd
```

Проверить, существует ли пользователь, и вывести по нему информацию можно командой `id`:

```
sa@astra:~$ id sa
uid=1000(sa) gid=1000(sa)
группы=1000(sa),24(cdrom),25(floppy),29(audio),30(dip),44(video),46
(plugdev),109(netdev),113(lpadmin),114(scanner),333(astra-console),1001(astra-admin)
```

Команда `getent` отображает записи из любой базы данных, которая поддерживается библиотеками NSS. С помощью неё можно получить информацию как о пользователе, так и о группе или пароле:

```
sa@astra:~$ getent passwd sa
sa:x:1000:1000:sa,,,:/home/sa:/bin/bash
```

Утилита `lslogins` позволяет вывести информацию об учетных записях пользователей, атрибутах паролей и информацию о сеансах:

```
sa@astra:~$ lslogins | tail -n 5
998 vboxadd               0
 999 systemd-coredump     0                            systemd Core Dumper
1000 sa                  37                      09:29 sa,,,
1001 student              0                 2024-map05 student,,,
65534 nobody              0                            nobody...
```

Создание учетных записей пользователей

Для создания учетных записей пользователей из консоли используются команды `useradd/adduser`.

Команда `useradd` — это встроенная команда Linux, которую можно найти в любой системе Linux. А вот `adduser` не является стандартной командой Linux, это дружественный интерфейс к программам useradd и usermod.

Утилита useradd

Команда `useradd` регистрирует нового пользователя или изменяет информацию по умолчанию о новых пользователях. Команда для работы требует привилегий до суперпользователя.

Синтаксис команды: `useradd <опции> <имя_пользователя>`

Все доступные опции и описание команды можно найти в справке `man useradd`. Далее рассмотрим наиболее часто используемые сценарии применения этой команды.

Утилита useradd имеет свой собственный конфигурационный файл `/etc/default/useradd`, в котором определены следующие параметры:

- **SHELL** — задает командную оболочку `/bin/sh`, которая будет назначаться пользователям по умолчанию, если значение не было задано явно в момент вызова команды.
- **SKEL** — задает директорию с шаблонами по умолчанию `/etc/skel`. Шаблоны — это директории и файлы, которые копируются в домашний каталог пользователя при его создании.
- **HOME** — указывает на директорию, в которой будут создаваться домашние папки пользователей.
- **CREATE_MAIL_SPOOL** — определяет, будет ли создаваться файл для хранения локальной почты пользователя. По умолчанию он не создается. Это можно увидеть,

запустив команду `useradd -D`. В выводе команды будут отражены настройки по умолчанию, применяемые при создании пользователя.

```
sa@astra:~$ sudo useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

```
sa@astra:~$ cat /etc/default/useradd
```

Результат вывода:

```
# Default values for useradd(8)
#
# The SHELL variable specifies the default login shell on your
# system.
# Similar to DHSELL in adduser. However, we use "sh" here because
# useradd is a low level utility and should be as general
# as possible
SHELL=/bin/sh
#
# The default group for users
# 100=users on Debian systems
# Same as USERS_GID in adduser
# This argument is used when the -n flag is specified.
# The default behavior (when -n and -g are not specified) is to create a
# primary user group with the same name as the user being added to the
# system.
# GROUP=100
#
# The default home directory. Same as DHOME for adduser
# HOME=/home
#
# The number of days after a password expires until the account
# is permanently disabled
# INACTIVE=-1
#
# The default expire date
# EXPIRE=
#
# The SKEL variable specifies the directory containing "skeletal" user
# files; in other words, files such as a sample .profile that will be
# copied to the new user's home directory when it is created.
# SKEL=/etc/skel
#
# Defines whether the mail spool should be created while
# creating the account
# CREATE_MAIL_SPOOL=yes
```

Для простого создания нового пользователя достаточно выполнить команду:

```
sudo useradd username
```

Пользователь будет создан с параметрами по умолчанию. Для явного выбора оболочки необходимо использовать параметр `-s` и полный путь до исполнимого файла, например, `sudo useradd username -s /bin/bash`

Для того чтобы пользователь смог войти в систему, необходимо также задать пароль:

```
sudo passwd username
```

Для создания пользователя с домашним каталогом в стандартной директории `/home` необходимо воспользоваться ключом `-m`. При этом будет создан новый каталог `/home/username`:

```
sudo useradd -m username
```

При необходимости домашний каталог может быть создан не в стандартной директории /home, а в любой другой. Для этого необходимо:

1. Опционально: создать родительский каталог для домашнего каталога будущего пользователя (пустой каталог):

```
sudo mkdir -p /users
```

2. Создать пользователя с домашним каталогом в требуемой директории:

```
sudo useradd -d /users/username -m username
```

```
sa@astra:~$ sudo mkdir -p /users
sa@astra:~$ sudo useradd -d /users/user1 -m user1
```

Для создания пользователя с определенным UID и с определенной группой по умолчанию необходимо воспользоваться ключами -u и -g соответственно (группа с таким GID должна быть уже предварительно создана):

```
sa@astra:~$ sudo useradd -u 1111 -g 1222 username
```

Чтобы создать пользователя и добавить его в дополнительные группы, используется ключ `-G`, например:

```
sa@astra:~$ sudo useradd -G sudo,ssh username
```

Таким образом, команда для создания нового пользователя с домашним каталогом в стандартной директории /home, включенного в группы sudo и ssh, и оболочкой bash будет выглядеть так:

```
sa@astra:~$ sudo useradd -m -G sudo,ssh -s /bin/bash username
```

Не стоит забывать, что требуется еще задать пароль пользователю, чтобы он смог войти в систему:

```
sa@astra:~$ sudo passwd username
```

Создадим несколько новых пользователей с заданными параметрами. Пароль для тестовых пользователей зададим *P@ssw0rd*.

Создадим простого пользователя user1:

```
sa@astra:~$ sudo useradd -m -u 1002 -s /bin/bash user1
sa@astra:~$ sudo passwd user1
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
```

Создадим простого пользователя user2:

```
sa@astra:~$ sudo useradd -m -s /bin/bash user2
sa@astra:~$ sudo passwd user2
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
```

Создадим администратора admin1:

```
sa@astra:~$ sudo useradd -m -G astra-admin -s /bin/bash admin1
sa@astra:~$ sudo passwd admin1
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
```

Создадим группу developers (подробнее о создании групп будет рассказано далее) с GID 1200:

```
sa@astra:~$ sudo groupadd developers -g 1200
```

Создадим пользователя user3 с заданными UID и GID

```
sa@astra:~$ sudo useradd -m -u 1150 -g 1200 -s /bin/bash user3
sa@astra:~$ sudo passwd user3
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
```

Посмотрите содержимое файлов `/etc/passwd` и `/etc/group`, чтобы ответить на вопросы:

- Была ли группа user3 создана для пользователя user3 и почему?
- Какая оболочка была выбрана для пользователя user3 и почему?

Утилита adduser

Команда `adduser` – это Perl-скрипт для команд `useradd` и `usermod`, убедиться в этом поможет команда `file /usr/sbin/adduser`. У этого скрипта есть свои конфигурационные файлы:

- `/etc/adduser.conf` – основной конфигурационный файл;

• `/usr/local/sbin/adduser.local` – по своей сути является скриптом sh для настройки нового пользователя. Если этот файл существует, то он будет запущен сразу после создания учётной записи пользователя, чтобы выполнить необходимые локальные настройки.

Команда `adduser` в отличие от `useradd` по умолчанию назначает пользователю командную оболочку `/bin/bash` (параметр DSHELL). В параметре EXTRA_GROUPS указываются дополнительные группы, в которые должен быть включен новый пользователь. При использовании `useradd` группы надо указывать явно с помощью параметра `-G`.

```
sa@astra:~$ cat /etc/adduser.conf

# /etc/adduser.conf: 'adduser' configuration.
# See adduser(8) and adduser.conf(5) for full documentation.

# The DSHELL variable specifies the default login shell on your
# system.
DSHELL=/bin/bash

# The DHOME variable specifies the directory containing users' home
# directories.
DHOME=/home

# If GROUPHOMES is "yes", then the home directories will be created as
# /home/groupname/user.
GROUPHOMES=no

# If LETTERHOMES is "yes", then the created home directories will have
# an extra directory - the first letter of the user name. For example:
# /home/u/user.
LETTERHOMES=no

# The SKEL variable specifies the directory containing "skeletal" user
# files; in other words, files such as a sample .profile that will be
# copied to the new user's home directory when it is created.
SKEL=/etc/skel

# FIRST_SYSTEM_[GU]ID to LAST_SYSTEM_[GU]ID inclusive is the range for UIDs
# for dynamically allocated administrative and system accounts/groups.
# Please note that system software, such as the users allocated by the base-passwd
# package, may assume that UIDs less than 100 are unallocated.
FIRST_SYSTEM_UID=100
LAST_SYSTEM_UID=999

FIRST_SYSTEM_GID=100
LAST_SYSTEM_GID=999

# FIRST_[GU]ID to LAST_[GU]ID inclusive is the range of UIDs of dynamically
# allocated user accounts/groups.
FIRST_UID=1000
LAST_UID=59999

FIRST_GID=1000
LAST_GID=59999

# The USERGROUPS variable can be either "yes" or "no". If "yes" each
# created user will be given their own group to use as a default. If
# "no", each created user will be placed in the group whose gid is
# USERS_GID (see below).
USERGROUPS=yes

# If USERGROUPS is "no", then USERS_GID should be the GID of the group
# `users' (or the equivalent group) on your system.
USERS_GID=100
```

```
# If DIR_MODE is set, directories will be created with the specified
# mode. Otherwise the default mode 0755 will be used.
DIR_MODE=0700

# If SETGID_HOME is "yes" home directories for users with their own
# group the setgid bit will be set. This was the default for
# versions << 3.13 of adduser. Because it has some bad side effects we
# no longer do this per default. If you want it nevertheless you can
# still set it here.
SETGID_HOME=no

# If QUOTAUSER is set, a default quota will be set from that user with
# `edquota -p QUOTAUSER newuser'
QUOTAUSER=""

# If SKEL_IGNORE_REGEX is set, adduser will ignore files matching this
# regular expression when creating a new home directory
SKEL_IGNORE_REGEX="dpkg-(old|new|dist|save)"

# Set this if you want the --add_extra_groups option to adduser to add
# new users to other groups.
# This is the list of groups that new non-system users will be added to
# Default:
EXTRA_GROUPS="fuse weston-launch dialout cdrom floppy audio video plugdev users"

# If ADD_EXTRA_GROUPS is set to something non-zero, the EXTRA_GROUPS
# option above will be default behavior for adding new, non-system users
ADD_EXTRA_GROUPS=1

# check user and group names also against this regular expression.
#NAME_REGEX="^[a-z][-a-z0-9_]*\$"
```

При запуске `adduser` запрашивает дополнительную информацию о пользователе:

```
sa@astra:~$ sudo adduser testuser
Добавляется пользователь «testuser» ...
Добавляется новая группа «testuser» (1007) ...
Добавляется новый пользователь «testuser» (1006) в группу «testuser» ...
Создаётся домашний каталог «/home/testuser» ...
Копирование файлов из «/etc/skel» ...
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
Изменение информации о пользователе testuser
Введите новое значение или нажмите ENTER для выбора значения по умолчанию
      Полное имя []:
      Номер комнаты []:
      Рабочий телефон []:
      Домашний телефон []:
      Другое []:
Данная информация корректна? [Y/n]
Добавляется новый пользователь «testuser» в дополнительные группы ...
adduser: Группа «fuse» не существует.
adduser: Группа «weston-launch» не существует.
Добавляется пользователь «testuser» в группу «dialout» ...
Добавляется пользователь «testuser» в группу «cdrom» ...
Добавляется пользователь «testuser» в группу «floppy» ...
Добавляется пользователь «testuser» в группу «audio» ...
Добавляется пользователь «testuser» в группу «video» ...
Добавляется пользователь «testuser» в группу «plugdev» ...
Добавляется пользователь «testuser» в группу «users» ...
```

Изменение учетных записей пользователей

С помощью команды `usermod` мы можем изменять параметры учетных записей пользователей, задаваемые утилитой `useradd`, и управлять дополнительными параметрами. Как и команда `useradd`, команда `usermod` требует прав суперпользователя.

Синтаксис команды: `useradd <опции> <имя_пользователя>`

Все доступные опции и описание команды можно найти в справке `man usermod`. Далее рассмотрим наиболее часто используемые сценарии применения этой команды.

Изменение основной группы

Для изменения основной группы необходим ключ `-g`. Создадим группу user3 с GID=1150 и назначим её в качестве основной для пользователя user3.

```
sa@astra:~$ sudo groupadd -g 1150 user3
sa@astra:~$ sudo usermod -g user3 user3
sa@astra:~$ id user3
uid=1150(user3) gid=1150(user3) группы=1150(user3)
```

Вместо имени группы можно указать её GID: `sudo usermod -g 1150`.

Добавление и исключение из группы

Командой `usermod` можно добавить пользователя в дополнительную группу.

Добавим пользователя user3 в группы developers и adm. Когда мы используем ключ `-G`, нам необходимо перечислить все текущие группы пользователя, кроме группы по умолчанию, и добавить к этому списку все группы, в которые его необходимо включить. В противном случае пользователь будет исключен из всех текущих групп, т.к. они не были перечислены. Но если в дополнение к ключу `-G` использовать ключ `-a`, то можно будет не указывать список текущих групп, и пользователь не будет из них исключен.

Для наглядности сделаем это в 2 этапа. У пользователя user3 сейчас нет ни одной дополнительной группы, и мы применим ключ `-G` для добавления его в группу developers, а затем добавим его еще и в группу adm, воспользовавшись ключами `-a` и `-G`:

```
sa@astra:~$ sudo usermod -G developers user3
sa@astra:~$ id user3
uid=1150(user3) gid=1150(user3) группы=1150(user3),1200(developers)
sa@astra:~$ sudo usermod -a -G adm user3
sa@astra:~$ id user3
uid=1150(user3) gid=1150(user3) группы=1150(user3),4(adm),1200(developers)
```

Командой `usermod` можно исключить пользователя из группы в явном виде. Для этого используем ключи `-r`, `-G` и имя дополнительной группы, из которой надо исключить пользователя.

Чтобы исключить пользователя из некоторых дополнительных групп, необходимо выполнить команду `usermod -G` и перечислить только те группы, в которых пользователь должен остаться.

Для исключения пользователя из всех дополнительных групп необходимо задать пустые кавычки после ключа `-G`:

```
sa@astra:~$ sudo usermod -G developers,adm user3
sa@astra:~$ id user3
uid=1150(user3) gid=1150(user3) группы=1150(user3),4(adm),1200(developers)
sa@astra:~$ sudo usermod -r -G adm user3
sa@astra:~$ id user3
uid=1150(user3) gid=1150(user3) группы=1150(user3),1200(developers)
sa@astra:~$ sudo usermod -G "" user3
sa@astra:~$ id user3
uid=1150(user3) gid=1150(user3) группы=1150(user3)
```

Исключить пользователя из группы в явном виде также можно командой `deluser` и синтаксис команды в таком случае будет: `deluser <пользователь> <группа>`

```
sa@astra:~$ groups user3
user3: user3 developers
sa@astra:~$ sudo deluser user3 developers
Удаляется пользователь «user3» из группы «developers» …
Готово.
sa@astra:~$ groups user3
user3: user3
```

Изменение домашнего каталога пользователя

Перед изменением домашнего каталога пользователя во избежание потери данных в случае сбоя лучше сделать его резервное копирование с сохранением прав доступа командой `cp -rp <источник>/ <назначение>/`. Сделаем резервную копию домашнего каталога пользователя user3:

```
sa@astra:~$ sudo cp -rp /home/user3 /home/user3_bkp
sa@astra:~$ sudo ls -l /home/user3_bkp/
итого 4
drwxr-xr-x 2 user3 user3 4096 мар 22  2023 Desktop
```

Для изменения домашнего каталога пользователя необходим ключ `-d`. Для создания нового домашнего каталога необходимо просто указать полный путь до него. Зададим новый каталог `/home/new_dir` для пользователя user3:

```
sa@astra:~$ grep user3 /etc/passwd
user3:x:1150:1150::/home/user3:/bin/bash
sa@astra:~$ sudo usermod -d /home/new-dir user3
sa@astra:~$ grep user3 /etc/passwd
```

```
user3:x:1150:1150::/home/new-dir:/bin/bash
sa@astra:~$ ls -l /home
итого 32
drwx------  3 admin1   admin1   4096 фев 23 09:41 admin1
drwx------ 26 sa       sa       4096 фев 23 10:57 sa
drwx------ 16 student  student  4096 мар  5  2024 student
drwx------  3 testuser testuser 4096 фев 23 09:57 testuser
drwx------  3 user2    user2    4096 фев 23 09:40 user2
drwx------  3 user3    user3    4096 фев 23 09:43 user3
drwx------  3 user3    user3    4096 фев 23 09:43 user3_bkp
drwx------  3 username username 4096 фев 23 09:38 username
```

Как видим, в конфигурационный файл /etc/passwd были внесены изменения, был создан новый каталог `/home/new-dir`, файлы из старого каталога были скопированы в новый, а старый каталог удалился.

Изменение оболочки пользователя

Изменить оболочку пользователя можно ключом `-s`. Список доступных оболочек хранится в файле `/etc/shells`. Назначим пользователю user3 оболочку bash.

```
sa@astra:~$ cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/bin/dash
/usr/bin/dash
sa@astra:~$ sudo usermod -s /bin/sh user3
sa@astra:~$ getent passwd user3
user3:x:1150:1150::/home/new-dir:/bin/sh
```

Обычный пользователь может изменить свою оболочку командой `chsh -s имя_интерпретатора` (но только на то, что перечислено в `/etc/shells`).

Изменение UID пользователя

Для изменения UID пользователя необходимо воспользоваться ключом `-u`. Изменим UID пользователя user3 на 1010.

```
sa@astra:~$ id user3
uid=1150(user3) gid=1150(user3) группы=1150(user3)
sa@astra:~$ sudo usermod -u 1010 user3
sa@astra:~$ id user3
uid=1010(user3) gid=1150(user3) группы=1150(user3)
```

Если необходимо задать не уникальный UID (UID, принадлежащий уже какому-то пользователю, например, 1003), необходимо добавить ключ `-o`: `sudo usermod -o -u 1003 user3`. Как вы понимаете, назначать один и тот же идентификатор двум и более субъектам возможно, но крайне не рекомендуется из соображений безопасности.

Изменение имени пользователя

Изменить имя пользователя можно ключом `-l` (строчная L). Изменим имя пользователя admin1 на admin:

```
sa@astra:~$ sudo usermod -l admin admin1
sa@astra:~$ ls /home
admin1  sa  student  testuser  user2  user3  user3_bkp  username
```

Однако при этом не происходит изменения имени домашнего каталога и группы по умолчанию.

Имя каталога может быть изменено сразу при выполнении команды или после, как рассматривалось выше с помощью ключей `-m` и `-d`:

```
sa@astra:~$ sudo usermod -l admin1 admin
sa@astra:~$ sudo usermod -l admin admin1 -m -d /home/admin1
sa@astra:~$ ls /home
admin1  sa  student  testuser  user2  user3  user3_bkp  username
sa@astra:~$ sudo groupmod -n admin admin1
sa@astra:~$ id admin
uid=1005(admin) gid=1006(admin) группы=1006(admin),1001(astra-admin)
```

Блокировка пользователя

Чтобы блокировать пользователю вход по паролю, необходимо воспользоваться ключом -L. При этом перед зашифрованным паролем пользователя в файле /etc/shadow добавляется восклицательный знак. Заблокируем пользователя user3:

```
sa@astra:~$ sudo grep user3 /etc/shadow
user3:$gost12512hash$…20142:0:99999:7:::
sa@astra:~$ sudo usermod -L user3
sa@astra:~$ sudo grep user3 /etc/shadow
user3:$gost12512hash$…20142:0:99999:7:::
```

Еще пользователя можно заблокировать командой `sudo passwd -l username`, а вывести информацию о состоянии учетной записи командой `sudo passwd -S username`:

```
sa@astra:~$ sudo passwd -l user3
passwd: информация об истечении срока действия пароля изменена.
sa@astra:~$ sudo passwd -S user3
user3 L 02/23/2025 0 99999 7 -1
```

Однако другие способы входа, например, по сертификату все еще доступны пользователю. Чтобы полностью заблокировать пользователя, необходимо добавить параметр `--expiredate` со значением 1. Полностью заблокируем пользователя user3:

```
sa@astra:~$ sudo usermod -L --expiredate 1 user3
sa@astra:~$ sudo grep user3 /etc/shadow
user3:!$gost12512hash$t…:20142:0:99999:7::1:
```

Для разблокировки входа по паролю необходимо воспользоваться ключом -U, а для полной разблокировки ключом –expiredate с пустыми кавычками “”. Разблокируем пользователя user3:

```
sa@astra:~$sudo usermod -U --expiredate "" user3
sa@astra:~$sudo grep user3 /etc/shadow
user3:$gost12512hash$…20142:0:99999:7:::
sa@astra:~$ sudo usermod -U --expiredate "" user3
sa@astra:~$ sudo grep user3 /etc/shadow
user3:$gost12512hash$…20142:0:99999:7:::
```

Можно задать определенную дату блокировки учетной записи с помощью ключа `--expiredate` в формате ГГГГ-ММ-ДД, а с помощью команды `chage` с опцией `-l` (строчная L) посмотреть срок действия учетной записи и другие параметры:

```
sa@astra:~$ sudo usermod --expiredate 2025-12-31 user3
sa@astra:~$ sudo chage -l user3
Последний раз пароль был изменён                                    : фев 23, 2025
Срок действия пароля истекает                                       : никогда
Пароль будет деактивирован через                                    : никогда
Срок действия учётной записи истекает                               : дек 31, 2025
Минимальное количество дней между сменой пароля                     : 0
Максимальное количество дней между сменой пароля                    : 99999
Количество дней с предупреждением перед деактивацией пароля        : 7
```

Изменение информационного поля GECOS

Для изменения информационных полей GECOS мы можем воспользоваться ключом `-c` команды `usermod` или специальной командой `chfn` (change finger information). Рассмотрим оба варианта.

Запустим команду `sudo chfn admin` и в интерактивной форме заполним поля GECOS для учетной записи admin. Пользователь может самостоятельно менять эти поля у своей собственной учетной записи. Прав суперпользователя при этом не требуется:

```
sa@astra:~$ sudo chfn admin
Изменение информации о пользователе admin
Введите новое значение или нажмите ENTER для выбора значения по умолчанию
       Полное имя []: Иван Иванов
       Номер комнаты []: 10
       Рабочий телефон []: 123-45-67
       Домашний телефон []: 98-76-54
       Другое []: Администратор Linux
chfn: имя «Иван Иванов» содержит не ASCII-символы
chfn: в «Администратор Linux» содержатся не ASCII-символы
sa@astra:~$ getent passwd admin
admin:x:1005:1006:Иван Иванов,10,123-45-67,98-76-54,Администратор Linux:/home/admin1:/bin/bash
```

Как видим, в файл `/etc/passwd` были внесены соответствующие изменения. Командой `chfn` можно менять и отдельные поля в GECOS. Например, ключом `-f` можно изменить полное имя, а ключом -o изменить поле «Другое». Полная справка по этой команде доступна через `man chfn`.

```
sa@astra:~$ sudo chfn -o "Linux администратор" admin
chfn: имя «Иван Иванов» содержит не ASCII-символы
```

```
chfn: в «Linux администратор» содержатся не ASCII-символы
sa@astra:~$ getent passwd admin
admin:x:1005:1006:Иван Иванов,10,123-45-67,98-76-54,Администратор Linux:/home/admin1:/bin/bash
```

Теперь изменим значение GECOS с помощью ключа `-c` команды `usermod`. При этом нам необходимо передавать в кавычках 5 полей, разделенных запятой без пробелов, со следующими значениями соответственно: ФИО, номер комнаты (или офиса), номер рабочего телефона, номер домашнего телефона, дополнительная информация. Добавим GECOS для учетной записи user3:

```
sa@astra:~$ sudo usermod -c "Петр Петров,202,555-1233,555-1122,Разработчик" user3
sa@astra:~$ getent passwd user3
user3:x:1010:1150:Петр Петров,202,555-1233,555-1122,Разработчик:/home/new-dir:/bin/sh
```

Изменение параметров пароля учетной записи

Изменить параметры срока действия пароля учетной записи можно командой `chage`. Мы уже применяли её, когда просматривали этот параметр. Выведем текущие параметры пароля у пользователя admin:

```
sa@astra:~$ sudo chage -l admin
Последний раз пароль был изменён                                    : фев 23, 2025
Срок действия пароля истекает                                       : никогда
Пароль будет деактивирован через                                    : никогда
Срок действия учётной записи истекает                               : никогда
Минимальное количество дней между сменой пароля                     : 0
Максимальное количество дней между сменой пароля                    : 99999
Количество дней с предупреждением перед деактивацией пароля        : 7
```

Посмотрим те же параметры в файле `/etc/shadow`:

```
sa@astra:~$ sudo grep -E ^admin /etc/shadow
admin:$gost12512hash$hG5F9o[...].:20142:0:99999:7:::
```

Чтобы поменять дату последнего изменения пароля, применяется ключ `-d` со значением в количестве дней с начала эпохи Unix (01.01.1970) или в формате ГГГГ-ММ-ДД.

```
sa@astra:~$ sudo chage -d 2025-02-2 admin
sa@astra:~$ sudo chage -l admin
Последний раз пароль был изменён                                    : фев 23, 2025
Срок действия пароля истекает                                       : никогда
Пароль будет деактивирован через                                    : никогда
Срок действия учётной записи истекает                               : никогда
Минимальное количество дней между сменой пароля                     : 0
Максимальное количество дней между сменой пароля                    : 99999
Количество дней с предупреждением перед деактивацией пароля        : 7
```

Дату устаревания учетной записи можно задать с помощью ключа `-E` со значением в количестве дней с начала эпохи (01.01.1970) или в формате ГГГГ-ММ-ДД. Для отключения устаревания необходимо задать значение -1.

```
sa@astra:~$ sudo chage -E 2025-12-31 admin
```

```
sa@astra:~$ sudo chage -l admin
Последний раз пароль был изменён                                      : фев 23, 2025
Срок действия пароля истекает                                         : никогда
Пароль будет деактивирован через                                      : никогда
Срок действия учётной записи истекает                                 : дек 31, 2025
Минимальное количество дней между сменой пароля                       : 0
Максимальное количество дней между сменой пароля                      : 99999
Количество дней с предупреждением перед деактивацией пароля          : 7
```

Посмотрим, как изменилась строка для пользователя admin в файле `/etc/shadow`:

```
sa@astra:~$ sudo grep -E ^admin /etc/shadow
admin:$gost12512hash$hG5F9o[...].:20142:0:99999:7::20453:
```

Полный список ключей доступен в справке `man chage`.

Удаление учетных записей пользователей

С помощью команды `userdel` мы можем удалить пользователя из системы. Как и команда `useradd`, команда `usermod` требует прав суперпользователя.

Синтаксис команды: `userdel <опции> <имя_пользователя>`

Все доступны е опции и описание команды можно найти в справке: `man userdel`. Далее рассмотрим частые сценарии применения этой команды.

Если дать команду без ключей, учетная запись выбранного пользователя будет удалена, однако домашний каталог пользователя и его почтовый ящик в каталоге /var/mail (если он существует) останутся. Если пользователь уже вошел в систему, эта команда не будет выполнена.

Войдем в систему в консоли tty1 под пользователем user3 и попробуем его удалить. Повторим то же действие после выхода пользователя user3 из сессии.

Войдите в tty1 под user3, нажав `Ctrl + Alt + F1`, и переключитесь обратно на tty7 `Ctrl + Alt + F7`, затем выполните команду в терминале:

```
sa@astra:~$ sudo userdel user3
userdel: user user3 is currently used by process 3190
```

Выйдите из сессии в tty1 `Ctrl + Alt + F1` и `exit`. После закрытия сессии в tty1 переключитесь обратно на tty7 `Ctrl + Alt + F7` и выполните удаление повторно:

```
sa@astra:~$ sudo userdel user3
sa@astra:~$ id user3
id: «user3»: такого пользователя нет
sa@astra:~$ ls -l /home
итого 32
drwx------  3 admin    admin    4096 фев 23 09:41 admin1
drwx------ 26 sa       sa       4096 фев 23 10:57 sa
drwx------ 16 student  student  4096 мар  5  2024 student
```

```
drwx------  3 testuser testuser 4096 фев 23 09:57 testuser
drwx------  3 user2    user2    4096 фев 23 09:40 user2
drwx------  3     1150     1150 4096 фев 23 09:43 user3
drwx------  3     1150     1150 4096 фев 23 09:43 user3_bkp
drwx------  3 username username 4096 фев 23 09:38 username
```

Как видим, в первом случае учетная запись не была удалена из-за активной сессии, а во втором - удалена успешно, однако домашний каталог остался нетронутым. Вместо имени пользователя и группы в правах на домашний каталог мы видим их UID и GID. Для удаления домашнего каталога и почтового ящика необходимо применить параметр `-r`. Удалим пользователя user2 и его домашний каталог:

```
sa@astra:~$ sudo userdel -r user2
userdel: почтовый ящик user2 (/var/mail/user2) не найден
sa@astra:~$ ls -l /home
итого 28
drwx------  3 admin    admin    4096 фев 23 09:41 admin1
drwx------ 26 sa       sa       4096 фев 23 10:57 sa
drwx------ 16 student  student  4096 мар  5  2024 student
drwx------  3 testuser testuser 4096 фев 23 09:57 testuser
drwx------  3     1150     1150 4096 фев 23 09:43 user3
drwx------  3     1150     1150 4096 фев 23 09:43 user3_bkp
drwx------  3 username username 4096 фев 23 09:38 username
```

Для удаления пользователя, даже если у него открыта активная сессия в системе или если другой пользователь использует его домашний каталог или его первичную группу, необходимо воспользоваться ключом `-f`. Войдем в систему под пользователем user1 и после этого удалим его.

Войдите в tty1 под user1 и переключитесь обратно на tty7:

```
sa@astra:~$ sudo userdel -f -r user1
userdel: user user1 is currently used by process 3240
userdel: почтовый ящик user1 (/var/mail/user1) не найден
sa@astra:~$ id user1
id: «user1»: такого пользователя нет
sa@astra:~$ ls /home
admin1  sa  student  testuser  user3  user3_bkp  username
```

Удалим домашние каталоги user3 и user3-new.

```
sa@astra:~$ rm -rf /home/user3*
```

Управление учетными записями групп из командной строки

Просмотр групп

Список всех учетных записей групп можно посмотреть в файле `/etc/group`:

```
sa@astra:~$ less /etc/group
```

Создание учетных записей групп

Для создания учетных записей групп в консоли используются две команды: `groupadd` и `addgroup`. `Groupadd` — это встроенная команда Linux, которую можно найти в любой системе Linux. Команда `addgroup` не является стандартной командой Linux. Это дружественный интерфейс к программам groupadd и groupmod.

Команда `groupadd` создает новую группу в системе. Команда для успешного выполнения требует привилегий суперпользователя.

Синтаксис команды: `groupadd <имя_группы> <опции>`

Все доступные опции и описание команды можно найти в справке: `man groupadd`. Далее рассмотрим наиболее используемые сценарии применения этой команды.

Чтобы просто создать новую группу, необходимо выполнить команду `sudo groupadd groupname`, где groupname - имя новой группы.

```
sa@astra:~$ sudo groupadd programmers
sa@astra:~$ grep programmers /etc/group
programmers:x:1201:
```

Создадим группу с заданным GID, для этого воспользуемся ключом `-g`:

```
sa@astra:~$ sudo groupadd managers -g 1100
sa@astra:~$ grep managers /etc/group
managers:x:1100:
```

Изменение учетных записей групп

С помощью утилиты `groupmod` можно изменить параметры группы, например, GID, имя или пароль.

Синтаксис команды: `groupmod <опции> <имя_группы>`

Изменим имя созданной нами группы programmers:

```
sa@astra:~$ sudo groupmod -n programmers_grp1 programmers
sa@astra:~$ cat /etc/group | grep programmers
programmers_grp1:x:1201:
```

Создание пароля группы

Чтобы создать пароль группы, используйте утилиту `gpasswd`.

Синтаксис команды: `gpasswd [<опции>] <имя_группы>`

Если команда дана без опций, появится запрос на изменение пароля группы:

```
sa@astra:~$ sudo gpasswd programmers_grp1
Изменение пароля для группы programmers_grp1
Новый пароль:
Повторите пароль:
```

Применяя опции, можно создать администратора группы (пользователь с правом добавления членов группы), добавить пользователей группы и т.д.

Создайте нового пользователя user 4.

```
sa@astra:~$ sudo useradd -m -s /bin/bash user4
sa@astra:~$ sudo passwd user4
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
```

Пользователь может присоединиться к группе, применив команду `newgrp`. Если группе назначен пароль, пользователь получит приглашение его ввести:

```
sa@astra:~$ sudo login user4
Пароль:
user4@astra:~$ newgrp programmers_grp1
Пароль:
user4@astra:~$ groups
programmers_grp1 user4
user4@astra:~$ exit
exit
user4@astra:~$ groups
user4
```

С помощью команды `newgrp` пользователь присоединяется к группе лишь на время. Набрав команду `exit` либо выйдя из системы, пользователь выйдет и из группы, к которой он присоединился командой `newgrp`.

Удаление учетных записей групп

С помощью команды `groupdel` можно удалить учетные записи групп.

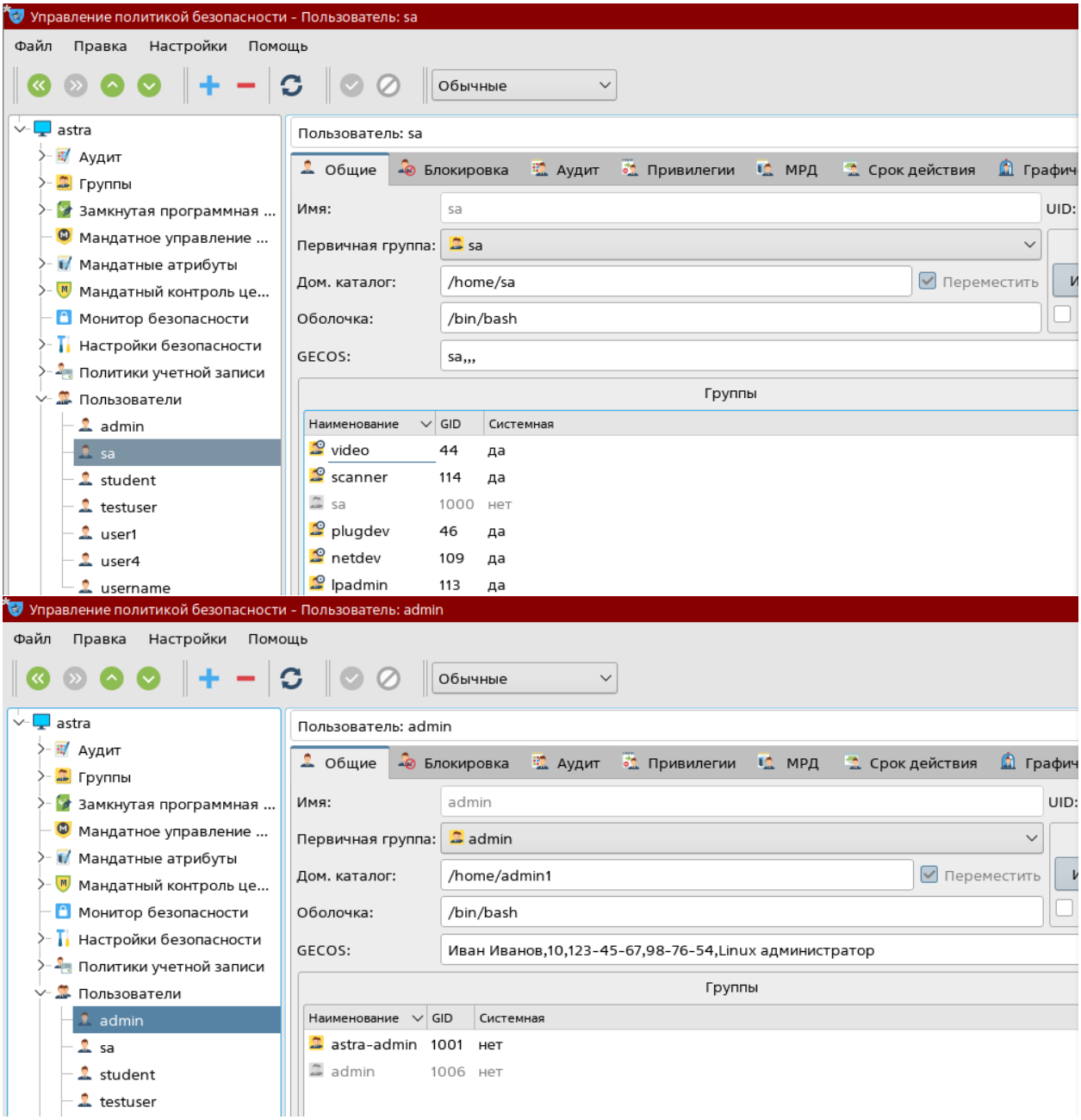
Удалим созданную нами группу.

```
sa@astra:~$ sudo groupdel programmers_grp1
sa@astra:~$ cat /etc/group | grep programmers
```

Управление пользователями и группами в графическом интерфейсе

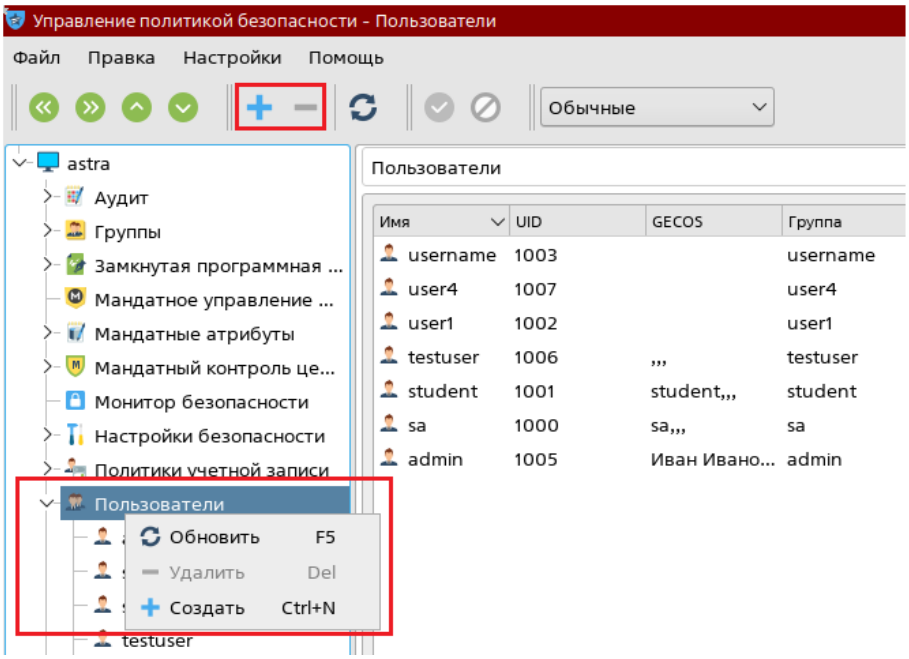
В графическом интерфейсе доступен удобный и интуитивно понятный интерфейс для управления пользователями и группами «Политика безопасности». Вызвать его можно

через меню **Пуск ▸ Панель управления ▸ Безопасность ▸ Политика безопасности** .Пароль для входа: 12345678.



С помощью контекстного меню на пунктах **Группы** и **Пользователи** или с помощью элементов управления + и - можно добавлять и удалять пользователей и группы.

Атрибуты и другие параметры учетных записей пользователей и групп распределим по вкладкам.



Для пользователей предназначение вкладок следующее:

- **Общие** – основные атрибуты учетной записи и пароль.
- **Блокировка** – блокировка пароля и учетной записи.
- **Аудит** – настройка аудита событий, вызванных действиями пользователя.
- **Привилегии** – установка Linux и Parsec привилегий.
- **МРД** – установка мандатных атрибутов пользователя.
- **Срок действия** – сроки действия пароля и учетной записи.
- **Графический киоск** – настройка работы компьютера, когда основное приложение открывается в полный экран (режим графического киоска).
- **Квоты** – настройка дисковых квот для пользователя.

После внесения изменений их можно принять или отклонить.

Практические задания

Задание 1.

1. Создайте пользователя user1 и user2. У них должны быть созданы домашние каталоги, и они должны иметь оболочку входа /bin/bash.
2. Назначьте пароли для пользователей user1, user2.
3. Назначьте для каждого пользователя минимальный срок действия пароля 1 день, максимальный срок действия пароля 30 дней, время предупреждения об истечении пароля 3 дня, период неактивности 3 дня.

Задание 2.

1. Создайте группы group1, group2, group3. Назначьте пароль группе group3 и ее администратором сделайте пользователя user1.
2. Включите пользователей user1, user2 в группы group1, group2.
3. Войдите в систему под пользователем user2 и получите права группы group3. Проверьте, что после ввода пароля user2 состоит в группе group3. Выйдите из системы.
4. Войдите в систему под пользователем user1 и включите user2 в группу group3. Выйдите из системы.

Задание 3.

1. Заблокируйте пользователя user2.
2. Принудительно заставьте пользователя user1 сменить свой пароль. Войдите под user1 в систему и смените пароль. Выйдите из системы.
3. Смените имя пользователя user2 на user3. Разблокируйте пользователя user3 и войдите в систему под его именем.
4. Перенесите домашние каталоги пользователей user1, user3 в /mnt/home. Проверьте, что домашние каталоги пользователей были успешно перенесены.

Задание 4.

1. Удалите группы group1, group2, group3.
2. Удалите пользователей user1, user3 вместе с их домашними каталогами.

Вопросы

1. Назовите четыре файла, в которых содержится информация о пользователях и группах?

2. Как называется файл бекапа для /etc/shadow?

3. Что означает «x» в поле пароля в файле /etc/passwd?

4. В каком файле хранятся настройки диапазонов UID, GID?

5. Что делает команда useradd -D?

6. Какой UID присвоится первому созданному пользователю в системе?

7. Какие две команды могут быть использованы для блокировки и разблокировки пользователя?

8. Как заставить пользователя iivanov принудительно сменить свой пароль при следующем входе?

9. Что делает команда faillog -u iivanov -r?