Лабораторная работа №5
«Управление учетными записями пользователей и групп»

1. Теоретическая часть

1.1. Введение в учетные записи пользователей и групп в Linux

Учетная запись пользователя представляет собой набор данных, который включает уникальный идентификатор пользователя (UID), домашний каталог, информацию о пароле, группе пользователей, и другую информацию. При работе с учетными записями важно понимать, что учетная запись позволяет пользователю иметь индивидуальные настройки окружения и доступ к ресурсам, на которые у него есть права.

Группы в Linux используются для объединения пользователей, что упрощает управление доступом к файлам и ресурсам системы. Каждая группа также имеет уникальный идентификатор (GID). Использование групп позволяет администратору назначать права доступа не каждому пользователю индивидуально, а сразу целой группе, что существенно упрощает управление доступом.

1.2. Структура учетной записи пользователя

Учетная запись пользователя в Linux включает несколько ключевых элементов, каждый из которых играет важную роль в обеспечении безопасности и организации работы пользователей.

- **Имя пользователя (username)** – уникальное имя, по которому пользователь идентифицируется в системе. Оно используется для входа в систему и для выполнения различных команд.
- **Идентификатор пользователя (UID)** – это уникальный числовой идентификатор, который используется ядром операционной системы для различения пользователей. Хотя имя пользователя является удобным для чтения человеком, операционная система оперирует именно UID при выполнении операций над файлами и процессами.

- **Домашний каталог** – это каталог, где хранятся персональные файлы пользователя, его настройки и временные данные. Обычно домашний каталог располагается по пути */home/имя_пользователя*. Важным является то, что пользователи не могут изменять файлы в чужих домашних каталогах, если они не имеют специальных прав доступа.
- **Командная оболочка (Shell)** – это программа, которая запускается при входе пользователя в систему. Она предоставляет интерфейс командной строки для взаимодействия с системой. Наиболее распространённой оболочкой является *bash*, но могут использоваться и другие, такие как *zsh*, *fish* и другие.

1.2.1. Основные сведения о UID

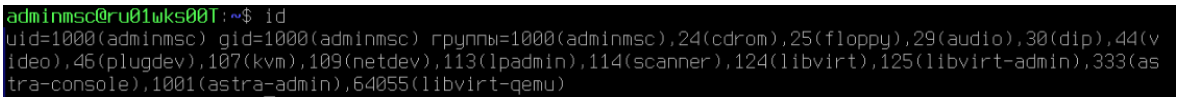
- UID — это числовой эквивалент имени пользователя
- Система оперирует UID при проверке прав доступа к файлам и выполнению команд, хотя для удобства отображается имя пользователя.

Таблица 1 — Описание диапазона значений UID

Диапазон	Описание
0	Зарезервирован для суперпользователя
1–99	Зарезервированы для системных пользователей, таких как демоны и службы
100–999	Используются для динамических системных пользователей и программ
1000 и выше	Назначаются обычным пользователям. По умолчанию для первого созданного пользователя в системе будет назначен UID 1000

65534	Это специальный UID, обычно связанный с пользователем nobody. Пользователь nobody имеет минимальные привилегии и часто используется для выполнения процессов от имени пользователя, который не должен иметь доступ к чувствительным частям системы

Чтобы узнать информацию о пользователе и его UID, можно воспользоваться утилитой **id**



1.3. Пароли и безопасность

Файл */etc/passwd* содержит список всех пользователей системы и информацию о них. Он используется для аутентификации и идентификации пользователей. Этот файл доступен для чтения всем пользователям.

Каждая строка файла */etc/passwd* описывает одного пользователя и состоит из семи полей, разделённых двоеточиями:

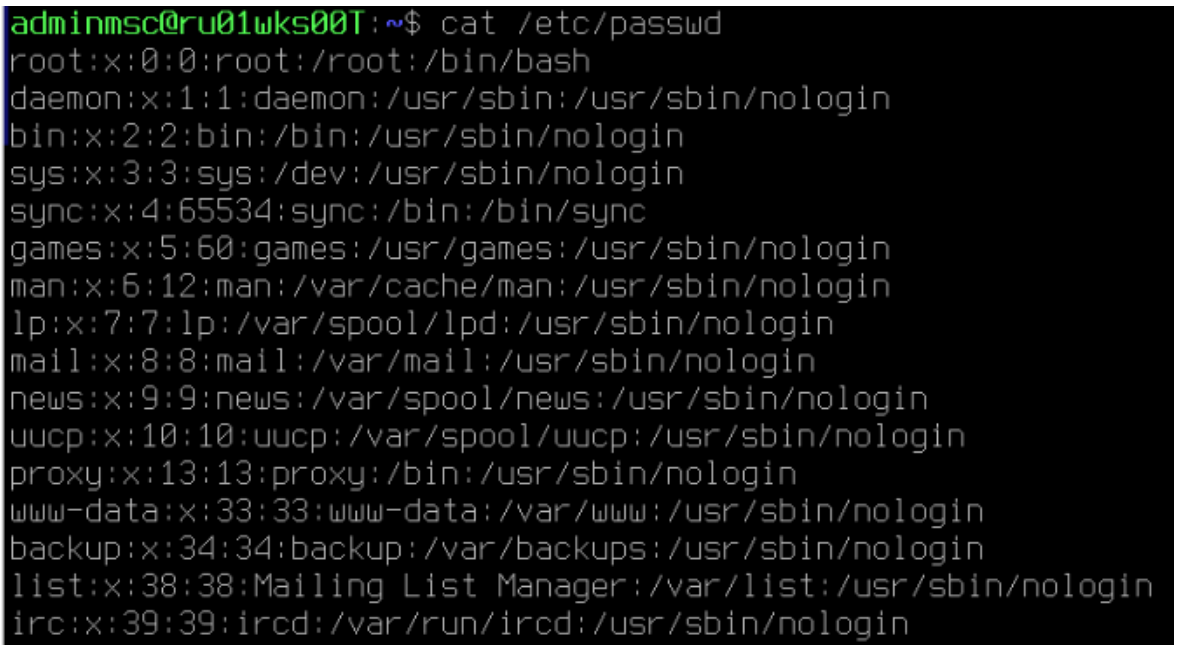
имя_пользователя:x:UID:GID:комментарий:домашний_каталог:оболочка

Описание этих полей:

- имя_пользователя — уникальное имя пользователя в системе (например, *john*).
- пароль — исторически в этом поле хранился зашифрованный пароль, но сейчас вместо него используется символ *x*, указывающий на то, что пароли хранятся в более защищённом файле */etc/shadow*.
- UID (user ID) — уникальный числовой идентификатор пользователя
- GID (group ID) — идентификатор основной группы пользователя

- комментарий — дополнительная информация о пользователе. Это поле часто используется для хранения полного имени пользователя или другой информации, полезной для администратор
- домашний_каталог — путь к домашнему каталогу пользователя, который обычно содержит его персональные файлы и настройки.
- оболочка — программа, которая запускается при входе пользователя в систему. Это может быть командная оболочка (например, */bin/bash*), либо другая программа, определяющая, что пользователь сможет делать в системе

Пример строки из файла **/etc/passwd:**



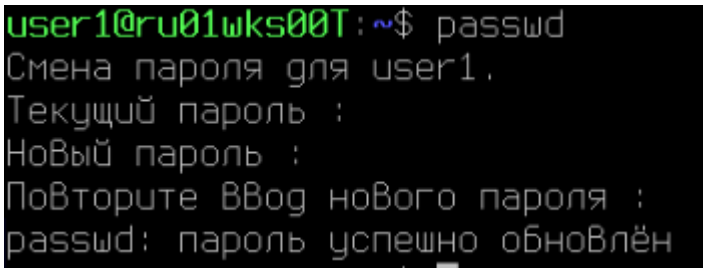
Ранее пароли хранились непосредственно в */etc/passwd* в зашифрованном виде, что делало их уязвимыми для атак. Чтобы повысить безопасность, пароли теперь хранятся в файле */etc/shadow*, который доступен только для чтения пользователю *root*.

Пароли могут задаваться вручную при помощи команды *passwd*. Каждый пользователь, включая администратора (root), может использовать команду

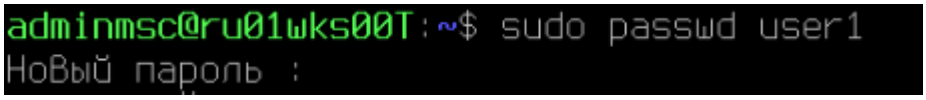
passwd, чтобы обновить свой пароль. У администратора также есть возможность изменять пароли других пользователей.

Основные функции утилиты *passwd*:

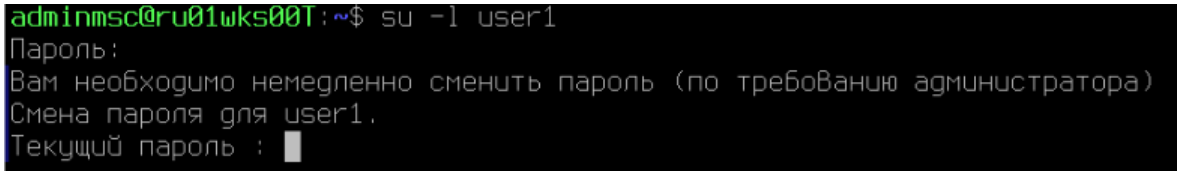
- Смена пароля пользователя. Если обычный пользователь вводит команду *passwd* без аргументов, утилита запросит старый пароль и предложит ввести новый пароль дважды для подтверждения



- Администратор может менять пароли других пользователей. Для этого ему нужно выполнить команду *passwd <имя_пользователя>*, при этом старый пароль не запрашивается



- Сброс срока действия пароля. При следующем входе пользователь будет вынужден сменить пароль



Утилита обеспечивает безопасность учетных записей, поскольку позволяет регулярно менять пароли и задавать параметры истечения паролей для повышения защиты.

Для управления политиками истечения срока действия пароля и учетной записи пользователя используется утилита *chage.* С её помощью администратор может изменять такие параметры, как минимальный и

максимальный срок действия пароля, количество дней предупреждения до истечения пароля и дату деактивации учётной записи

Утилита позволяет:

- Установить максимальный срок действия пароля (в днях)

```
sudo chage -M 90 user1
```

- Установить минимальный срок действия пароля (в днях)

```
sudo chage -m 7 user1
```

- Настроить количество дней предупреждения пользователя до истечения пароля

```
sudo chage -W 7 user1
```

- Установить срок действия учётной записи (дата, когда учётная запись будет отключена). Дата указывается в формате YYYY-MM-DD. В примере ниже будет установлен срок деактивации на 31 декабря 2024 года

```
sudo chage -E 2024-12-31 user1
```

Вышеперечисленные опции можно использовать одновременно:

```
sudo chage -M 90 -m 7 -W 7 -E 2024-12-31 user1
```

Опция *-l* позволяет получить список всех параметров, связанных с истечением пароля для конкретного пользователя

```
adminmsc@ru01wks00T:~$ sudo chage -l user1
Последний раз пароль был изменён                        : окт 12, 2024
Срок действия пароля истекает                           : янв 10, 2025
Пароль будет деактивирован через                        : никогда
Срок действия учётной записи истекает                   : дек 31, 2024
Минимальное количество дней между сменой пароля         : 7
Максимальное количество дней между сменой пароля        : 90
Количество дней с предупреждением перед деактивацией пароля     : 7
```

1.4. Управление группами

Группы – это удобный способ управлять доступом к ресурсам системы для нескольких пользователей одновременно. Группы могут быть первичными и

вторичными. Первичная группа пользователя назначается по умолчанию при создании учетной записи и является основной группой, к которой он принадлежит. Вторичные группы позволяют пользователю иметь дополнительные права доступа к другим ресурсам, которым разрешен доступ только участникам определённых групп.

Основной файл, содержащий информацию о группах, называется */etc/group*. В нем хранится список всех групп системы, их идентификаторы (GID) и члены этих групп. Формат строки в */etc/group:*

имя_группы:пароль:GID:список_пользователей

- имя_группы — название группы
- пароль — поле для пароля группы (обычно пустое)
- GID — уникальный идентификатор группы (Group ID).
- список_пользователей — список пользователей, принадлежащих к группе

В файле */etc/gshadow* содержатся зашифрованные пароли групп и информацию о членах групп. Доступ к этому файлу ограничен

1.4.1. Основные команды для управления группами

- Для создания группы используется команда *groupadd*

```
sudo groupadd group1
```

- Чтобы удалить группу используется команда *groupdel*

```
sudo groupdel group1
```

- Для изменения информации о группе (например, её имени) используется команда *groupmod*

```
sudo groupmod -n new_group group1
```

- Чтобы добавить пользователя в группу используется команда *usermod*

```
sudo usermod user1 -aG group1
```

- Чтобы удалить пользователя из группы используется команда *gpasswd*

```
sudo gpasswd -d user1 group1
```

- Чтобы посмотреть, в каких группах состоит пользователь, можно использовать команду *groups*

1.5. Управление учетными записями пользователей

Создание, изменение и удаление учетных записей пользователей – это важная часть управления системой. В Linux существует множество команд для работы с учетными записями. Рассмотрим некоторые из них

- Для создания нового пользователя используется команда *useradd*
  - *-m* создает домашний каталог
  - **-***s* задает оболочку по умолчанию (например, **/bin/bash**)
  - -u – задать UID явным образом
  - -G – задать список дополнительных (вторичных) групп
  - -c – комментарий (GECOS)

```
sudo useradd -m -s /bin/bash user1
```

В качестве альтернативы возможно использовать команду adduser, обладающую удобным интерфейсом для заполнения всех необходимых данных из поля GECOS и автоматическим включением пользователя в основную и некоторые дополнительные группы. Однако, она предустановлена не на всех дистрибутивах ОС Linux.

Комментарий при создании пользователя можно задать в виде произвольной строки или в формате записи GECOS – поле хранит в себе значения настоящего имени пользователя, его рабочий и домашний телефон, адрес и другую информацию. Для изменения поля используется команда:

```
chfn имя_пользователя
```

С помощью команды chfn обычный пользователь может изменить только те поля в комментарии (GECOS), которые указаны в параметре CHFN_RESTRICT в файле /etc/login.defs (по умолчанию, номер комнаты и номера телефонов).

- Для удаления пользователя используется команда *userdel*
  - *-r* удаляет домашний каталог пользователя

```
sudo userdel -r user1
```

- Для изменения параметров учетной записи (например, имени, оболочки) используется команда *usermod*

```
sudo usermod -s /bin/dash user1
```

- Для установки пароля пользователя используется команда *passwd*

1.6. Pluggable Authentication Modules

Рассуждая о пользователях, нельзя не затронуть тему аутентификации. В UNIX-подобных ОС используется Pluggable Authentication Modules (PAM) — это гибкий механизм для аутентификации, который позволяет приложениям и сервисам использовать разнообразные методы аутентификации без необходимости менять их код.

1.6.1. Основные компоненты PAM

Модули PAM — это плагины, которые реализуют конкретные механизмы аутентификации. Они могут быть встроенными в систему или добавляться сторонними разработчиками

Конфигурационные файлы. Они находятся обычно в */etc/pam.d/* и задают, как именно должны работать модули PAM для различных приложений. В каждом таком файле прописываются модули и их параметры, определяющие политику аутентификации

Общий формат файла представлен в виде:

тип_модуля управляющий_флаг путь_к_модулю [аргументы]

Тип модуля	Описание работы
auth	*Модуль для аутентификации пользователя*

account	*Модуль не занимается аутентификацией, а позволяет контролировать распределение ресурсов системы*
session	*Выполнение действий до или поле получения пользователем доступа к службе*
password	*Модуль для проверки паролей*

Все проверки происходят последовательно. С помощью управляющего флага возможно определить значимость того или иного модуля.

Управляющий флаг	Описание работы
required	*В случае неудачного прохождения данного модуля сообщение об ошибке появится только после корректного прохождения остальных проверок.*
requisite	*В случае неудачного прохождения данного модуля сообщение об ошибке появится сразу*
sufficient	*В случае удачного прохождения данного модуля вся аутентификация будет считаться успешной, если до него никаких ошибок не было выявлено. Неудачное прохождение модуля не считается фатальной.*
optional	*Не критичен для аутентификации – может ограничиться выводом предупреждения на экран*

Существует множество модулей PAM в Linux – рассмотрим в качестве примера модуль для проверки пароля на сложность - pam_cracklib**.** Модуль может проверить различные параметры при создании нового пароля:

- retry= n: определяет количество попыток создания пароля
- minlen=n: определяет минимальную длину пароля

- difok= n: определяет количество символов, на которые должен отличаться новый пароль от старого при изменении
- dcredit=n: вводить не более n цифр при положительном значении и не менее n цифр при отрицательном значении
- ucredit=n: вводить не более n заглавных букв при положительном значении и не менее n заглавных букв при отрицательном значении
- lcredit=n: вводить не более n строчных букв при положительном значении и не менее n строчных букв при отрицательном значении
- ocredit=n: вводить не более n специальных символов при положительном значении и не менее n специальных символов при отрицательном значении

Для изменения политики паролей в Astra Linux необходимо сконфигурировать файл /etc/pam.d/common-password.

Возможная конфигурация:

```
password    requisite       pam_cracklib.so retry=3 minlen=8 difok=3
```

1.6.2. Принцип работы PAM

Когда пользователь пытается получить доступ к системе или выполнить действие, требующее аутентификации, то приложение, использующее PAM, отправляет запрос к соответствующим модулям. Эти модули могут проверять пароли, токены, отпечатки пальцев или использовать другие методы аутентификации. Например, когда вы вводите пароль при входе в систему, PAM может сначала проверить, верен ли пароль, а затем вызвать другие модули для дополнительных проверок, таких как наличие двухфакторной аутентификации.

1.6.3. Основные задачи PAM

- Проверка подлинности пользователя, например, с помощью пароля

- Контроль прав доступа для пользователя, например, срок действия пароля или доступные временные окна для входа
- Настройка или завершение сеансов, например, монтирование дисков при входе
- Управление процессом смены пароля пользователем

1.7. Смена текущего пользователя

Для входа в систему из-под нового пользователя возможно воспользоваться командной su с указанием имени пользователя в качестве параметра. При указании дополнительного параметра «-» переменные окружения предыдущего пользователя не будут доступны новому пользователю. По умолчанию без параметров происходит переключение на пользователя root, которое требует прав суперпользователя, предоставляемых с помощью sudo.

При смене пользователя по умолчанию не изменяется текущая директория, поэтому для перехода в домашнюю директорию пользователя возможно использовать ключ -l

С помощью команды su возможно выполнять команды из-под других пользователей. Для этого необходимо указать её после ключа -c.

```
su - user1          # переключиться на пользователя user1 без сохранения переменных окружения
su -l user1         # переключиться на пользователя user1 и перейти в его домашнюю директорию
su user1 -l -c whoami       # вызвать команду whoami из под пользователя user1
sudo su                     #переключиться на суперпользователя
```

2. Практическая часть

2.1. Создание пользователей и групп

2.1.1. Создайте трех пользователей с именами ваших любимых персонажей мультсериалов. Для каждого из них создайте домашний каталог и укажите оболочку *bash.* Используйте команды adduser и useradd.

2.1.2. Создайте группу с названием мультсериала, из которого взяты созданные персонажи и добавьте пользователей в неё.

2.1.3. Убедитесь, что пользователи были успешно добавлены в систему и в группу

2.2. Управление паролями

2.2.1. Установите пароли для созданных пользователей

2.2.2. Установите следующие параметры для паролей:

	User 1	User 2	User 3
Максимальный срок действия пароля	День вашего рождения + 10	День вашего рождения + 20	День вашего рождения + 30
Минимальный срок действия пароля	День вашего рождения	День вашего рождения	День вашего рождения
Срок действия учетной записи	Месяц вашего рождения + 90	Месяц вашего рождения + 90	Месяц вашего рождения + 90

2.2.2. Проверьте, что изменения вступили в силу, попытавшись войти в систему под новыми учетными записями.

2.3. Создание групп

2.3.1. Создайте новую группу *group2*

2.3.2. Добавьте пользователя *user3* в эту группу *group2*

2.3.3. Убедитесь, что пользователь *user3* теперь принадлежит к новой группе

2.4. Удаление пользователей и групп

2.4.1. Удалите пользователя *user3* вместе с его домашним каталогом

2.4.2. Удалите группу *group2*

2.5. Настройка PAM

2.5.1. Настройте проверку паролей Linux на сложность следующим образом:

- Число попыток для ввода пароля: Номер в списке
- Минимальный размер пароля: 5
- Минимальное количество цифр в пароле: 2
- Минимальное количество прописных букв в пароле: 2
- Минимальное количество строчных букв в пароле: 2

После настройки PAM перезагрузите ПК.

2.5.2. Смените пароль у любого из созданных пользователей. Убедитесь, что пароль не соответствующий требованиям не работает.

Контрольные вопросы

1. В каких файлах хранятся основные данные о пользователях и группах?
2. Какая команда позволяет изменить пароль пользователя?
3. Какой командой можно установить права доступа к файлам и папкам?