**Настройка аутентификации и авторизации в Linux Ubuntu**

1. Основные понятия

Аутентификация - процесс проверки подлинности пользователя (например, с помощью пароля).

Авторизация - процесс проверки прав пользователя на выполнение определенных действий.

2. Файлы системы аутентификации

Основные конфигурационные файлы:

- `/etc/passwd` - информация о пользователях

- `/etc/shadow` - хэши паролей пользователей

- `/etc/group` - информация о группах

- `/etc/gshadow` - защищенные данные групп

- `/etc/login.defs` - настройки политик паролей

- `/etc/pam.d/` - конфигурация PAM (Pluggable Authentication Modules)

3. Управление пользователями и группами

Создание пользователя:

sudo adduser username

Изменение пароля:

sudo passwd username

Удаление пользователя:

sudo deluser username

Создание группы:

sudo addgroup groupname

Добавление пользователя в группу:

sudo usermod -aG groupname username

4. Настройка SSH аутентификации

Отключение входа по паролю:

sudo nano /etc/ssh/sshd\_config

Изменить:

PasswordAuthentication no

Включение аутентификации по ключам:

PubkeyAuthentication yes

5. Аудит и мониторинг

Просмотр последних входов:

last

lastb # неудачные попытки входа

Установка и настройка auditd:

sudo apt install auditd

sudo auditctl -l

6. Полезные команды для проверки

whoami # текущий пользователь

id # информация о пользователе и группах

groups # группы текущего пользователя

w # кто сейчас в системе

sudo -l # какие команды можно выполнять с sudo