“Київський фаховий коледж зв’язку”

Циклова комісія Комп’ютерної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №9**

з дисципліни: «Операційні системи»

**Тема: «Захист системи та користувачів у Linux. Створення користувачів та груп»**

Виконавли студенти

групи РПЗ-03

Команда: Губенко Є.О.,

Заїка С.В. та Кресан Р.А.

Перевірив викладач

Сушанова В.С.

Київ 2022

**Мета роботи:**

1. Отримання практичних навиків роботи з командною оболонкою Bash.

2. Знайомство з базовими діями при створенні нових користувачів та нових груп користувачів.

**Матеріальне забезпечення занять**

1. ЕОМ типу IBM PC.

2. ОС сімейства Windows (Windows 7).

3. Віртуальна машина – Virtual Box (Oracle).

4. Операційна система GNU/Linux – CentOS.

5. Сайт мережевої академії Cisco netacad.com та його онлайн курси по Linux

**Завдання для попередньої підготовки**

***Готував матеріал студент Губенко Є.О***

1. На базі розглянутого матеріалу дайте відповіді на наступні питання:
   1. Розкрийте поняття UPG, коли їх доцільно використовувати?

*UPG - це абревіатура від словосполучення "Unified Process for Geospatial Information Management" (єдиної процедури управління геопросторовою інформацією). Це методологія управління геопросторовими даними, що включає в себе набір процесів, які можуть використовуватися для розробки, впровадження та управління геопросторовими інформаційними системами.*

*UPG можна використовувати в будь-якому проекті, пов'язаному з геопросторовою інформацією, включаючи геодезію, картографію, телекомунікації, нерухомість, екологію, міське планування, транспорт і т.д. За допомогою UPG можна розробити та впровадити геопросторові інформаційні системи, які допоможуть організаціям з кращим управлінням земельними ресурсами, геодезичними роботами, розробкою карт, маршрутизацією транспорту та багато іншого.*

*UPG надає системний підхід до управління геопросторовими даними, який дозволяє організаціям більш ефективно використовувати свої геопросторові ресурси. UPG допомагає забезпечити стандартизацію та узгодженість даних, сприяє покращенню якості та точності геопросторових інформаційних систем, що дозволяє більш ефективно їх використовувати.*

* 1. Якими командами можна створити групи користувачів? Наведіть приклади.

*Створення груп користувачів може бути здійснене за допомогою різноманітних команд у різних операційних системах та програмах.   
Приклади команд для створення груп користувачів:*

* ***У Windows*** *можна створити групу користувачів за допомогою команди "net localgroup". Наприклад, щоб створити групу з назвою "admins", відкрийте командний рядок і введіть наступну команду: net localgroup admins /add*
* ***У Linux*** *можна створити групу користувачів за допомогою команди "groupadd". Наприклад, щоб створити групу з назвою "developers", відкрийте термінал і введіть наступну команду: groupadd developers*
* ***У MacOS*** *можна створити групу користувачів за допомогою програми "Адміністратор системи". Натисніть на іконку "Адміністратор системи" на панелі Dock, відкрийте вкладку "Групи" та натисніть "+" для додавання нової групи.*
* ***У Microsoft Active Directory*** *можна створити групу користувачів за допомогою консолі "Active Directory Users and Computers". Натисніть правою кнопкою миші на контейнері, до якого ви хочете додати нову групу, виберіть "New" та натисніть "Group". Введіть назву групи та натисніть "OK".*
  1. Якими командами можна змінити налаштування груп користувачів? Наведіть приклади.

*Приклади команд для зміни налаштувань груп користувачів:*

* ***У Windows*** *можна змінити налаштування групи користувачів за допомогою команди "net localgroup". Наприклад, щоб додати користувача до групи "admins", відкрийте командний рядок і введіть наступну команду: net localgroup admins /add username*
* ***У Linux*** *можна змінити налаштування групи користувачів за допомогою команди "usermod". Наприклад, щоб додати користувача з ім'ям "username" до групи "developers", відкрийте термінал і введіть наступну команду: usermod -a -G developers username*
* ***У MacOS*** *можна змінити налаштування групи користувачів за допомогою програми "Адміністратор системи". Виберіть потрібну групу та натисніть на кнопку "Опції". За допомогою цієї програми можна змінювати членство в групі та права доступу.*
* ***У Microsoft Active Directory*** *можна змінити налаштування групи користувачів за допомогою консолі "Active Directory Users and Computers". Виберіть потрібну групу та натисніть правою кнопкою миші на неї, виберіть "Properties" та змініть налаштування, що вам необхідні.*

**Хід роботи**

***Готував матеріал студент Заїка С. В.***

1. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу NDG Linux Essentials - Lab 15: System and User Security та Lab 16: Creating Users and Groups. Створіть таблицю для опису цих команд\*\*\*.

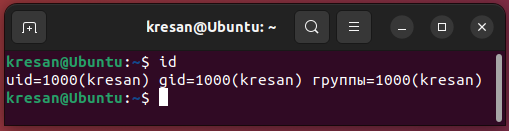
|  |  |
| --- | --- |
| Назва команди | Її призначення та функціональність |
| su - | Використовується в операційних системах на основі Unix, таких як Linux, для зміни користувача на інший та запуску нової оболонки з експортованими змінними середовища нового користувача. |
| id | використовується в операційних системах на основі Unix, таких як Linux, для відображення інформації про ідентифікатори користувача (UID) та груп (GID). |
| head /etc/shadow | використовується для відображення перших декількох рядків з файлу або стандартного введення. |
| sudo head /etc/shadow | використовується для запуску команд з підвищеними привілеями адміністратора (root) в операційних системах на основі Unix, таких як Linux. |
| head /etc/passwd | використовується для відображення перших декількох рядків з файлу або стандартного введення. |
| grep | використовується для пошуку вхідного рядка або файлів на відповідність заданому шаблону або регулярному виразу. Вона дозволяє швидко знаходити відповідні рядки в текстових файлах або стандартному ввідному потоці та виводити їх на екран або записувати у вихідний файл. |
| getent passwd sysadmin | дозволяє отримати інформацію про користувачів, групи, хост-машини та інші ресурси, що зберігаються у системних базах даних, включаючи /etc/passwd, /etc/group, /etc/hosts та інші. |
| w | призначена для відображення інформації про користувачів, які в даний момент залогінились на систему. Ця команда виводить інформацію про ім'я користувача, термінал, на якому він залогінений, час, протягом якого він перебуває в системі, стан та команду, яку він виконує. |
| groupadd -r research | створює нову системну групу з назвою research. Група буде додана до файлу /etc/group та буде містити назву групи та її ідентифікатор. |
| getent group research | повертає інформацію про групу з назвою research, яка знаходиться в файлі /etc/group. Ця команда виводить рядок тексту, що містить інформацію про групу, таку як назву групи, її ідентифікатор, та список користувачів, які належать до цієї групи. |
| useradd -D | Команда useradd використовується для створення нового користувача в системі. За допомогою опції -D можна отримати поточні значення налаштувань, які будуть використовуватися при створенні нового користувача за замовчуванням. |
| nano /etc/default/useradd | відкриває файл конфігурації /etc/default/useradd для редагування у текстовому редакторі nano |
| userdel -r student | використовується для видалення користувача student з системи, разом з його домашнім каталогом та усіма файлами та підкаталогами, які належать цьому користувачу. |

\*\*\*Скріншоти виконання команд в терміналі можна не представляти, достатньо коротко описати команди в таблиці.

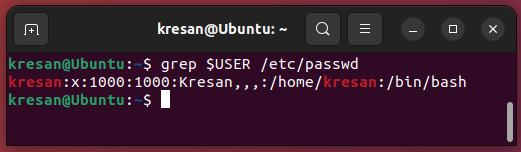
***Готував матеріал студент Кресан Р.А.***

1. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):
   * **виведіть інформацію про поточного користувача різними способами (підказка використовуйте команди id та grep);**

*Виведена інформація містить ідентифікатор користувача (UID), ідентифікатор групи користувачів (GID) та список додаткових груп користувача.*

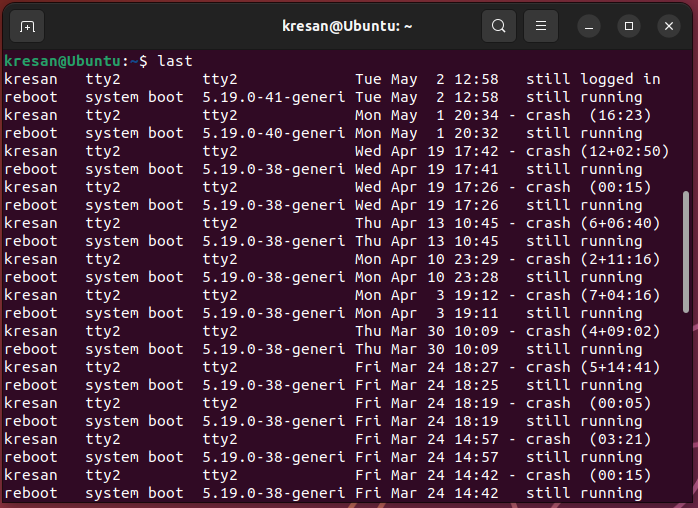


*Виведена інформація містить інформацію про користувача в файлі /etc/passwd, включаючи ідентифікатор користувача та групи.*

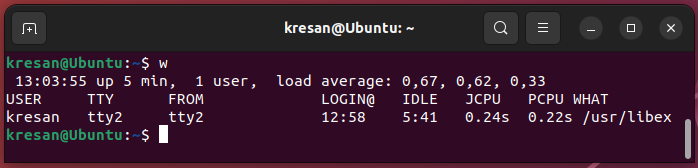


* + **попрактикуйте в терміналі команди last, w та who. Порівняйте результати виводу кожної команди, які деталі відсутні в кожній із команд порівняно з іншими?**

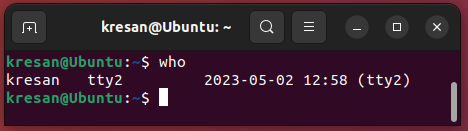
*Команда last виводить інформацію про попередні входження користувачів у систему. Вона показує список користувачів, які успішно ввійшли до системи, а також час їх входу та вихіду. Також відображається термінал, з якого було здійснено вхід.*



*Команда w показує, хто зараз залогінений у системі та які процеси вони виконують. Крім того, він показує інформацію про час роботи користувачів та з якого терміналу вони працюють.*

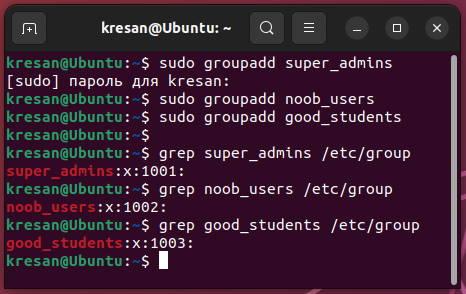


*Команда who відображає лише список користувачів, які залогінені на даний момент до системи, а також інформацію про те, з якого терміналу вони зайшли до системи.*



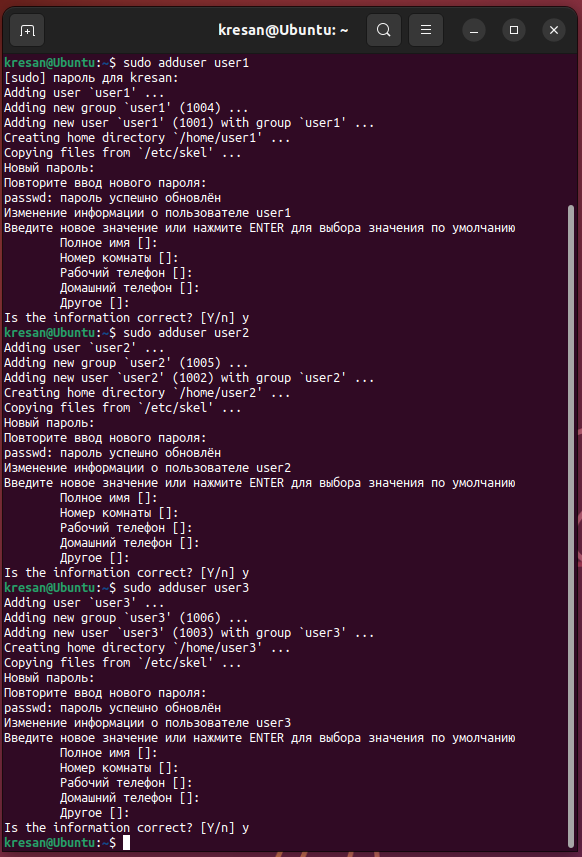
* + **створіть дві нові групи користувачів - super\_admins, noob\_users та good\_students, визначте їх ідентифікатори;**

*Для створення нових груп користувачів можна скористатися командою groupadd. Ідентифікатори новостворених груп можна перевірити за допомогою команди grep та файлу /etc/group, де зберігаються дані про групи користувачів.*

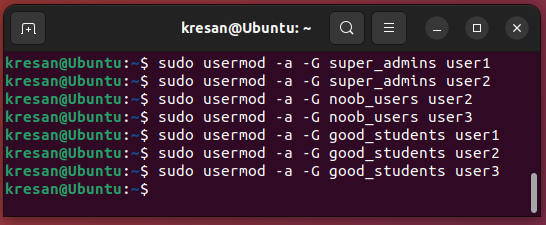


* + **для кожного члену Вашої команди за допомогою терміналу створіть нового користувача (якщо працюєте самі, то просто трьох довільних користувачів), не забудьте після створення нового користувача одразу задати йому пароль;**

*Для створення нового користувача в Linux можна скористатися командою adduser. Після виконання команди система попросить ввести пароль для нового користувача, а також запитає додаткові дані про користувача, такі як ім'я та номер телефону. Ці дані є необов'язковими і можна пропустити їх, натиснувши Enter.*



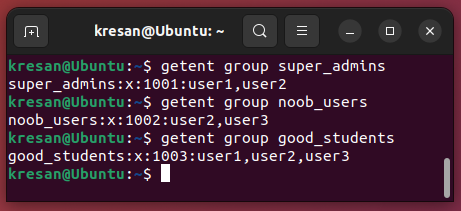
* + **додайте нових користувачів у створені Вами нові групи таким чином, щоб у групах super\_admins та noob\_users було по 2 користувачі, один з яких є в обох групах, у групу good\_students додайте всіх трьох користувачів;**

*Для додавання користувача до групи можна скористатися командою usermod.*

* + **перегляньте інформацію про групи, та які користувачі до них входять, поясніть що ви бачите;**

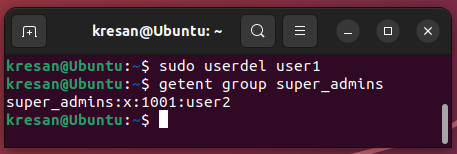
*Інформацію про групи та їх членів можна переглянути за допомогою команди getent.*

*Переглянемо інформацію на групі super\_admins. Тут 1001 - це ідентифікатор групи, а user1, user2 - користувачі, які належать до цієї групи.*



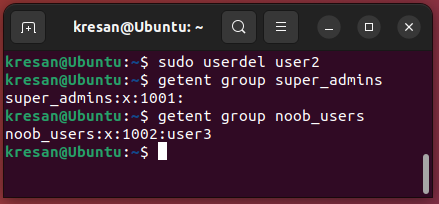
* + **видаліть першого створеного вами користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;**

*Щоб видалити користувача, можна використати команду userdel, передавши їй ім'я користувача, якого потрібно видалити. Після виконання цієї команди інформація про користувача user1 буде видалена з системи. Щоб перевірити, чи залишилась інформація про користувача в групах, можна знову використати команду getent. Якщо у виводі цієї команди є згадка про користувача user1, то це означає, що інформація про нього ще залишилась у групі. В іншому випадку - інформації про користувача немає у групі. У моєму випадку інформація про користувача, у групі, видалилася.*



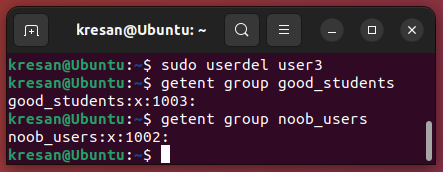
* + **видаліть другого користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;**

*При видаленні користувача user2, інформація про нього в групах зникла.*



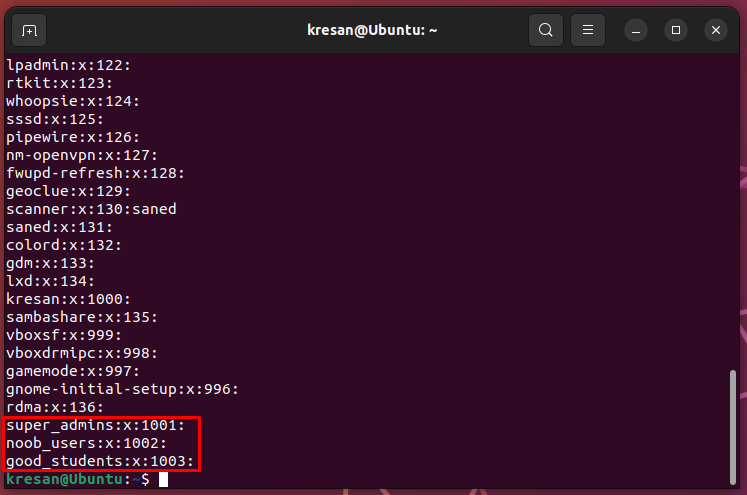
* + **видаліть третього користувача, перегляньте чи залишиться інформація про нього в групах, де він перебував;**

*При видаленні користувача user3, інформація про нього в групах, в яких він перебував, зникла.*



* + **перегляньте інформацію про існуючі групи користувачів;**

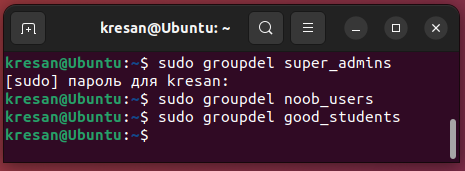
*Щоб переглянути список усіх груп, можна виконати команду getent group. Ця команда виведе список всіх груп на системі, разом з інформацією про їх ідентифікатори та членів.*



*Оскільки ми видалили створених нами користувачів, інформація про них в групі зникла, тому групи порожні.*

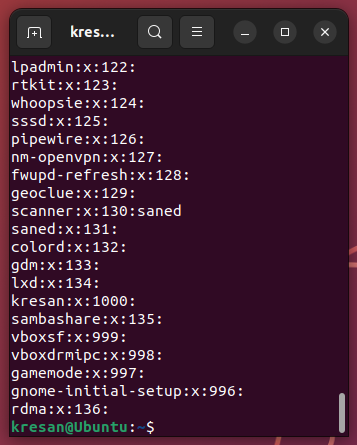
* + **видаліть створені Вами групи користувачів;**

*Щоб видалити групу користувачів в Linux, можна використати команду groupdel, за якою слідує назва групи, яку потрібно видалити. Після виконання цієї команди інформація про видалену групу буде видалена з файлу /etc/group. При цьому користувачі, які були в цій групі, залишаться без групи, і їхня група буде змінена на значення users.*



* + **перегляньте інформацію про існуючі групи користувачів.**

*Виконавши команду getent group, ми помічаємо що створені нами групи зникли.*



***Готував матеріал студент Губенко Є.О***

**Відповіді на контрольні запитання**

1. Чому в конфігураційних файлах паролі не зберігається в явному вигляді?

*У конфігураційних файлах паролі зазвичай не зберігаються в явному вигляді з метою забезпечення безпеки даних. Якщо пароль буде збережений в явному вигляді, то будь-хто, хто має доступ до файлу, зможе побачити пароль та використати його для несанкціонованого доступу до системи.*

*Один з методів захисту паролів у конфігураційних файлах полягає у зашифруванні пароля за допомогою алгоритму шифрування. Зашифрований пароль можна зберегти в конфігураційному файлі, і тільки ті, хто знає ключ для розшифрування, зможуть побачити пароль. Це дозволяє зберегти пароль у безпечному вигляді та зменшити ризик несанкціонованого доступу.*

*Інший метод захисту полягає у збереженні хеш-значення паролю в конфігураційному файлі замість самого пароля. Хеш-значення - це математична функція, яка перетворює вихідні дані (у цьому випадку пароль) на вихідне значення фіксованої довжини. Якщо користувач вводить пароль, система обчислює хеш-значення введеного пароля та порівнює його зі збереженим значенням хеша. Цей метод забезпечує захист паролю в конфігураційному файлі, оскільки навіть якщо файл потрапить у руки зловмисника, він не зможе побачити сам пароль.*

1. Чому не рекомендується виконувати повсякденні операції, використовуючи обліковий запис root?

*Обліковий запис root в Linux має найвищі привілеї, що дозволяють користувачу виконувати будь-яку операцію на системі. Використання облікового запису root для повсякденних операцій може призвести до ризику зниження безпеки системи, збоїв в роботі та навіть до втрати даних.*

*Ось кілька причин, чому не рекомендується виконувати повсякденні операції в Linux з облікового запису root:*

* *Несанкціонований доступ: Якщо обліковий запис root буде скомпрометований зловмисником, він зможе отримати доступ до всіх файлів і каталогів на системі та виконувати будь-які операції. Це може призвести до втрати конфіденційних даних та критичних наслідків для системи.*
* *Випадкова помилка: Виконання повсякденних операцій з обліковим записом root може призвести до випадкових помилок, які можуть спричинити збої в роботі системи або втрату даних. Наприклад, випадкове видалення важливого файлу або каталогу.*
* *Недосконалість програм: Більшість програм не були розроблені з урахуванням безпеки та виконання з правами root. Якщо ви виконуєте ці програми з облікового запису root, то є ризик збоїв в роботі програм або непередбачуваної поведінки.*
* *Непередбачувана поведінка: Використання облікового запису root для повсякденних операцій може мати непередбачувану поведінку системи. Наприклад, деякі програми можуть вести себе інакше з правами root, що може призвести до виникнення проблем з їх роботою.*

1. У чому відмінність механізмів отримання особливих привілеїв su і sudo?

*Механізми отримання особливих привілеїв* ***su*** *і* ***sudo*** *в Linux дозволяють користувачам отримати привілеї адміністратора для виконання завдань, які вимагають підвищених прав доступу. Однак, їхні принципи роботи і механізми відрізняються.*

*Команда* ***su*** *дозволяє користувачу переключитися на обліковий запис користувача з правами* ***root*** *за допомогою введення пароля* ***root****. Після того, як користувач отримав права* ***root****, він може виконувати будь-які завдання з правами адміністратора, але не має обмежень на доступ до системних ресурсів.*

*У випадку з* ***sudo****, користувачеві надається право виконувати певну команду або набір команд з підвищеними правами доступу, зазвичай, після введення власного пароля. Відмінність від* ***su*** *полягає в тому, що* ***sudo*** *дозволяє настроювати деталі доступу, такі як обмеження доступу до певних команд, обмеження часу дії підвищених прав, запис відповідних дій в журналі тощо. Крім того,* ***sudo*** *дозволяє виконувати команди з підвищеними привілеями без необхідності вводити пароль* ***root****.*

1. Чому домашній каталог користувача root не розміщено в каталозі /home?

*Домашній каталог користувача* ***root*** *не розміщено в каталозі* ***/home*** *з технічних та безпекових міркувань.*

*Один з головних принципів дизайну файлової системи в* ***Unix****-подібних системах полягає в тому, що кожен обліковий запис користувача повинен мати свій власний домашній каталог, в якому зберігається користувацька інформація та конфігураційні файли. Зазвичай, домашній каталог користувача знаходиться в підкаталозі* ***/home****.*

*Однак, обліковий запис користувача* ***root*** *є особливим, і його домашній каталог розміщено в іншому місці на файловій системі. Зазвичай, домашній каталог користувача* ***root*** *розташований в каталозі* ***/root****. Це зроблено з технічних причин - в багатьох* ***Unix****-подібних системах користувацький каталог* ***/home*** *може бути монтуваний з іншої файлової системи, і при цьому він може бути недоступним у випадку, коли не вдалося змонтувати цю файлову систему. Крім того, використання окремого каталогу* ***/root*** *дозволяє забезпечити більшу безпеку системи, оскільки домашній каталог користувача* ***root*** *містить конфіденційну інформацію, яка має бути доступна тільки користувачу з правами* ***root****.*

1. Для чого використовується команда getent?

*Команда* ***getent*** *використовується для отримання інформації про користувачів, групи, мережеві сервіси, а також інших системних об'єктів з джерел, які визначені в системному файлі* ***/etc/nsswitch.conf.***

*За замовчуванням в* ***Unix****-подібних системах, інформація про користувачів, групи, хости та інші системні об'єкти зберігаються у спеціальних файлових базах даних, таких як* ***/etc/passwd, /etc/group, /etc/hosts*** *тощо. Однак, інші джерела інформації можуть бути використані, наприклад, централізована база даних, LDAP-сервер або NIS-сервер.*

*Команда* ***getent*** *дозволяє отримати інформацію про системні об'єкти з будь-якого з цих джерел, залежно від налаштувань* ***/etc/nsswitch.conf****. Наприклад, команда* ***getent passwd*** *поверне список всіх користувачів з усіх доступних джерел, включаючи* ***/etc/passwd****, базу даних, LDAP-сервер або NIS-сервер.*

*Крім того, команда getent може бути корисною при відлагодженні деяких проблем з автентифікацією або авторизацією користувачів. Наприклад, якщо виникає проблема з доступом до файлів, використання команди getent group може допомогти визначити, чи належить користувач до відповідної групи, і чи має він доступ до цих файлів.*

1. Яким чином можна видалити існуючі групи користувачів? Чи залишиться інформація про них десь у системі?

*Для видалення групи користувачів в Linux можна використовувати команду groupdel. Синтаксис команди:* ***sudo groupdel <назва\_групи>***

*Наприклад, щоб видалити групу з назвою* ***testgroup****, можна виконати таку команду:* ***sudo groupdel testgroup***

*Після виконання цієї команди група буде видалена з системи, інформація про неї буде видалена з файлу* ***/etc/group.***

*Проте, якщо у групи були користувачі, які до неї належали, то інформація про цих користувачів залишиться у файлі* ***/etc/passwd****, але їхня приналежність до видаленої групи буде видалена. Це може створити проблеми з правами доступу до файлів та каталогів, які були доступні тільки для цієї групи. Тому перед видаленням групи слід переконатися, що немає користувачів, які до неї належать, або перемістити їх до інших груп.*

*Деякі системи можуть мати додаткові механізми збереження інформації про групи, наприклад, може бути використаний LDAP-сервер або NIS-сервер. У цьому випадку інформація про групи може зберігатися на цих серверах, і після видалення групи з локальної системи, інформація про неї може залишитися на сервері. Тому, якщо використовуються ці сервери, слід переконатися, що інформація про видалені групи також видалена на серверах.*

1. Як можна змінити пароль користувача?

*Для зміни пароля користувача в Linux можна використовувати команду passwd. Якщо викликати команду без параметрів, то змінюватиметься пароль для поточного користувача. Якщо вказати ім'я користувача як параметр, то змінюватиметься пароль для вказаного користувача.*

*Синтаксис команди для зміни пароля поточного користувача:* ***passwd***

*Синтаксис команди для зміни пароля іншого користувача:* ***sudo passwd <ім'я\_користувача>***

*Після виклику команди passwd виконувачу буде запропоновано ввести новий пароль. Після цього потрібно підтвердити новий пароль, повторивши його введення. Якщо новий пароль задовольняє вимогам безпеки (достатньо складний), то пароль буде змінено, інакше виконавцеві буде запропоновано ввести новий пароль знову.*

*Наприклад, щоб змінити пароль користувача з ім'ям user1, можна виконати таку команду:* ***sudo passwd user1***

*Після цього виконавцеві буде запропоновано ввести новий пароль для користувача* ***user1****.*

*Також є можливість змінити пароль користувача без використання командного рядка, використовуючи графічний інтерфейс. Для цього потрібно відкрити настройки системи, знайти розділ "Користувачі", вибрати користувача, пароль якого потрібно змінити, і натиснути кнопку "Змінити пароль". Далі слід дотримуватися інструкцій, які з'являтимуться на екрані.*

1. Яке призначення команди chage?4

*Команда chage використовується для зміни параметрів паролю користувача в Linux, таких як термін дії паролю, дата останньої зміни паролю, мінімальний термін дії паролю тощо.*

*Основне призначення команди chage - зміна параметрів паролю користувача, а саме:*

* ***chage -d <дата> <ім'я\_користувача>*** *- встановлює дату останньої зміни паролю.*
* ***chage -E <дата> <ім'я\_користувача>*** *- встановлює дату, коли пароль користувача стане недійсним.*
* ***chage -m <мін\_термін\_дії> <ім'я\_користувача>*** *- встановлює мінімальний термін дії паролю.*
* ***chage -M <макс\_термін\_дії> <ім'я\_користувача>*** *- встановлює максимальний термін дії паролю.*
* ***chage -W <термін\_попередження> <ім'я\_користувача>*** *- встановлює термін, за який до закінчення терміну дії паролю буде надіслане повідомлення про необхідність зміни паролю.*

*Наприклад, щоб встановити максимальний термін дії паролю користувача* ***user1*** *на 90 днів, можна виконати таку команду:* ***sudo chage -M 90 user1***

*Для перегляду поточних налаштувань паролю користувача можна використати команду* ***chage*** *без параметрів:* ***sudo chage <ім'я\_користувача>***

*Ця команда покаже поточні налаштування паролю користувача, такі як дата останньої зміни паролю, мінімальний термін дії паролю, максимальний термін дії паролю тощо.*

1. Які параметри команди usermod ви вважаєте найбільш використовуваними?

*Команда usermod використовується для зміни налаштувань користувача в системі Linux. Найбільш використовуваними параметрами команди є наступні:*

* ***-a або --append****: цей параметр дозволяє додавати користувача до додаткових груп без заміни його поточних груп. Наприклад, usermod -a -G groupname username додасть користувача до групи groupname, не змінюючи його поточних груп.*
* ***-d або --home****: цей параметр дозволяє змінити домашній каталог користувача. Наприклад, usermod -d /new/home/directory username змінить домашній каталог користувача зі стандартного значення /home/username на /new/home/directory.*
* ***-l або --login****: цей параметр дозволяє змінити логін користувача. Наприклад, usermod -l newusername username змінить логін користувача з username на newusername.*
* ***-g або --gid****: цей параметр дозволяє змінити первинну групу користувача. Наприклад, usermod -g groupname username змінить первинну групу користувача на groupname.*

*Ці параметри є найбільш використовуваними, але команда usermod має інші параметри, які також можуть бути корисними в різних ситуаціях. Детальнішу інформацію про команду usermod можна отримати, використовуючи команду man usermod.*

***Готував матеріал студент Заїка С. В.***

**Висновки**

В ході виконання лабораторної роботи ми отримали практичні навички роботи з командною оболонкою Bash. Ознайомились з базовими діями при створенні нових користувачів та нових груп користувачів.