“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»

Виконала студентка

групи БІКС-13

Лось Злата Володимирівна

Перевірив викладач

Сушанова В.С.

Київ 2024

**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 та віртуальна машина Virtual Box (Oracle).

3. ОС GNU/Linux (будь-який дистрибутив).

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

**Завдання для попередньої підготовки:**

1. \*Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.

Administrative Accounts - Облікові записи, які мають спеціальні привілеї для керування та адміністрування операційної системи або певних ресурсів. Ці облікові записи можуть мати доступ до виконання привілегійних команд, налаштування системних параметрів та інше, що звичайним користувачам заборонено.

Root User - Спеціальний обліковий запис на UNIX-подібних операційних системах, який має найвищі привілеї. Користувач з ім'ям "root" має повний доступ до всіх ресурсів системи і може виконувати будь-які команди та операції, включаючи керування іншими обліковими записами та системними налаштуваннями.

Root Privileges - Спеціальні привілеї, які має користувач "root" або інші адміністративні облікові записи. Ці привілеї надають доступ до виконання привілегійних операцій та команд, які впливають на роботу системи та її ресурсів.

sudo - Команда для виконання команд з адміністративними привілеями.

su - Команда для перемикання між користувачами.

User Accounts - Облікові записи користувачів, які використовуються для ідентифікації та автентифікації користувачів у системі. Кожен користувач має свій унікальний обліковий запис, який дозволяє йому використовувати ресурси та виконувати операції в межах своїх прав доступу.

System Accounts - Спеціальні облікові записи, призначені для використання системними службами та процесами. Вони зазвичай не призначені для використання користувачами напряму, а використовуються для виконання певних фонових операцій або надання послуг.

Group Accounts - Групові облікові записи, які використовуються для організації та управління групами користувачів у системі. Користувачі можуть бути членами однієї або декількох груп, що дозволяє керувати доступом до ресурсів та файлів.

Primary Group Membership - Основна група, до якої належить користувач. Кожен користувач має одну основну групу, до якої він автоматично приєднується при створенні свого облікового запису.

Supplemental Group Membership - Додаткові групи, до яких може належати користувач під час роботи у системі. Крім основної групи, користувач може бути членом інших груп, що надає додаткові права доступу до ресурсів.

Group ID (GID): Ідентифікатор групи (Group ID) - це унікальний числовий ідентифікатор, що призначається кожній групі в операційній системі. GID використовується для ідентифікації групи в системі і контролю доступу до ресурсів, таких як файли та каталоги.

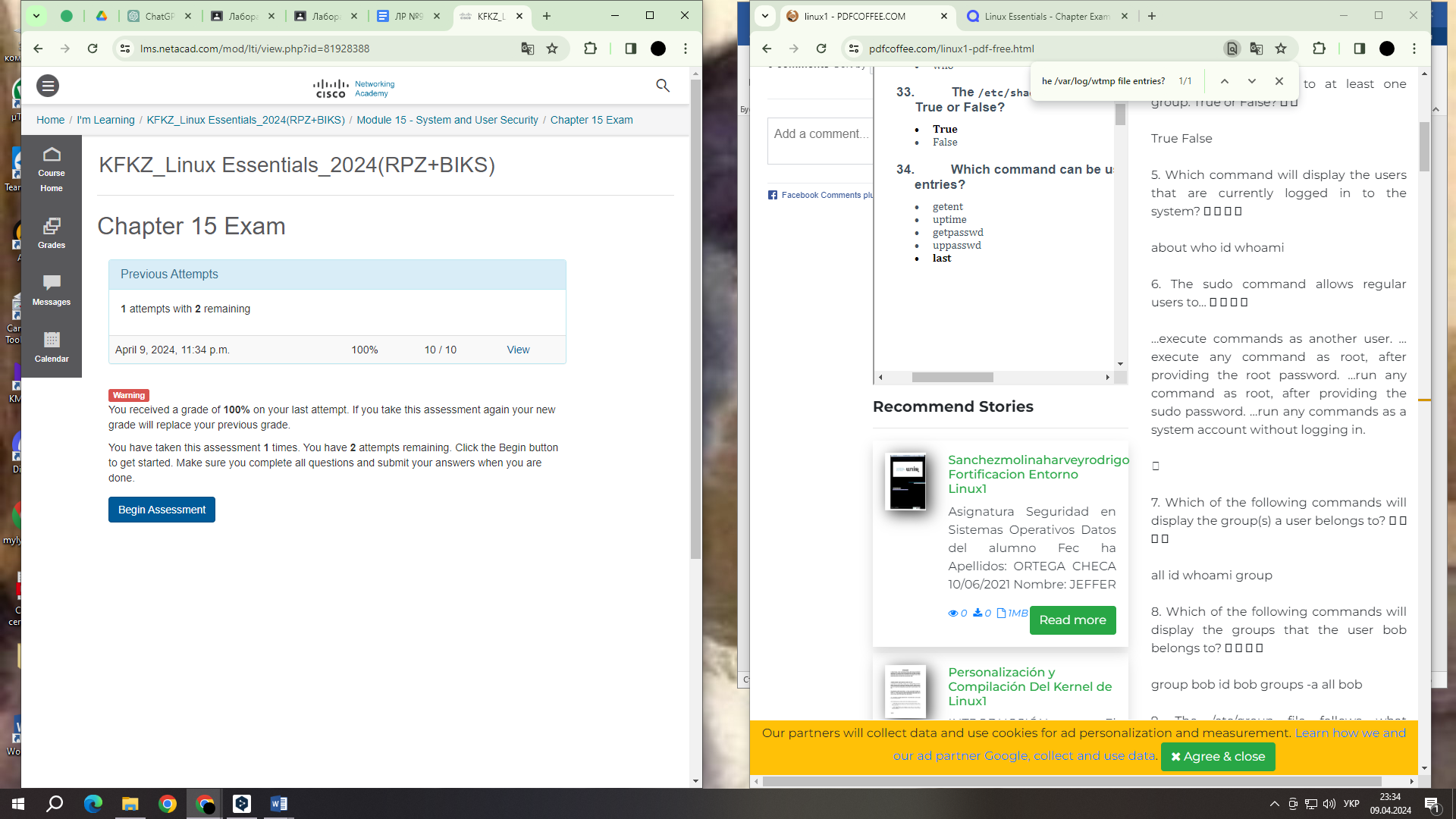
2. Вивчіть матеріали онлайн-курсу академії Cisco “NDG Linux Essentials”:

- Chapter 15 - System and User Security

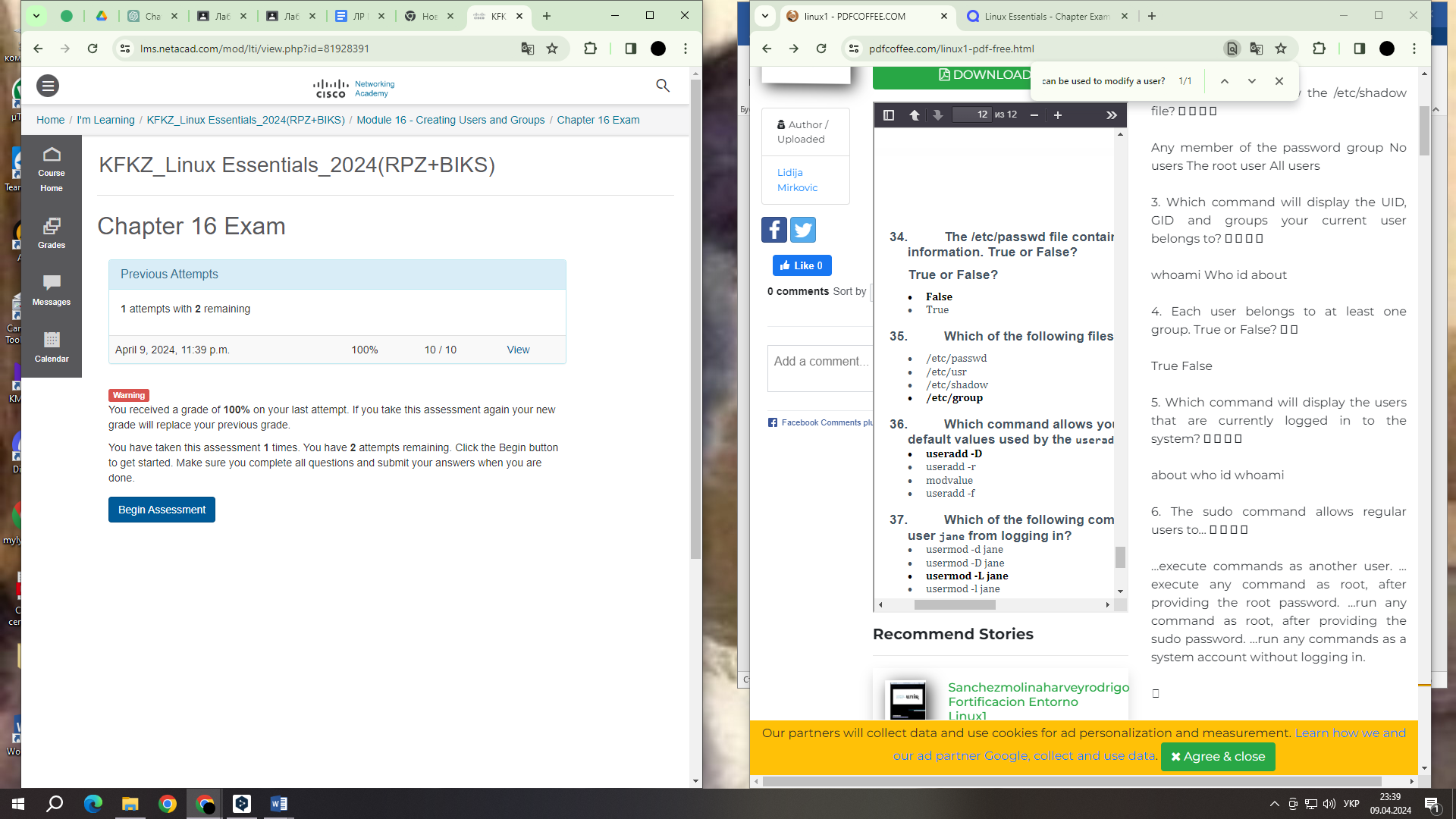
- Chapter 16 - Creating Users and Groups

3. Пройдіть тестування у курсі NDG Linux Essentials за такими темами:

- Chapter 15 Exam



- Chapter 16 Exam



4. На базі розглянутого матеріалу дайте відповіді на наступні питання:

4.1. Розкрийте поняття UPG, коли їх доцільно використовувати?

UPG або User Private Group - це концепція, яка використовується в деяких дистрибутивах Linux, таких як Ubuntu, Fedora тощо. Головна ідея полягає в тому, що для кожного нового користувача автоматично створюється окрема група з тим самим ім'ям, що і користувач.

Коли доцільно використовувати UPG:

* Безпека: UPG сприяє підвищенню безпеки, оскільки вона гарантує, що користувачі мають власні ізольовані групи, до яких іншим користувачам складніше отримати доступ.
* Керування доступом: UPG дозволяє керувати доступом до файлів і ресурсів, що належать конкретним користувачам, через їх власні приватні групи.
* Зручність: UPG робить керування користувачами та групами більш простим і зручним для адміністраторів системи, оскільки вони можуть більш чітко контролювати доступ до ресурсів.
* Ізоляція процесів: Кожен користувач має власну приватну групу, що дозволяє ізолювати процеси ізоляції файлових ресурсів та взаємодіяти з іншими користувачами та процесами.

4.2. \*Якими командами можна створити групи користувачів? Наведіть приклади.

Для створення груп користувачів можна використовувати команду groupadd. Наприклад:

sudo groupadd mygroup

Ця команда створить нову групу користувачів з ім'ям mygroup.

4.3. \*\*Якими командами можна змінити налаштування груп користувачів? Наведіть приклади.

Для зміни налаштувань груп користувачів можна використовувати команду groupmod. Наприклад:

* Зміна імені групи: sudo groupmod -n newname oldname

Ця команда змінить назву групи з oldname на newname

* Зміна ідентифікатора групи (GID): sudo groupmod -g 1001 mygroup

Ця команда змінить ідентифікатор групи mygroup на 1001.

5. Підготувати в електронному вигляді початковий варіант звіту:

- Титульний аркуш, тема та мета роботи.

- Словник термінів.

- Відповіді на п.4.1 та п.4.5 з завдань для попередньої підготовки.

**Хід роботи:**

**1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:**

1.1. Запустіть віртуальну машину VirtualBox, оберіть CentOS та запустіть її. Виконайте вхід в систему під користувачем: CentOS, пароль для входу: reverse (якщо виконуєте ЛР у 401 ауд.) та запустіть термінал.

1.2.Запустіть віртуальну машину Ubuntu\_PC (якщо виконуєте завдання ЛР через академію netacad)

1.3.Запустіть свою операційну систему сімейства Linux (якщо працюєте на власному ПК та її встановили) та запустіть термінал.

**2. 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** |
| sudo | Дозволяє користувачам виконувати команди з підвищеними привілеями (зазвичай виконувати команди в режимі root або іншого суперкористувача). |
| su | Команда для переключення користувача. При використанні з дефісом (-) вона переключає контекст середовища на того користувача, в якого виконується вхід. |
| id | Відображає інформацію про ідентифікатори користувача та групи. |
| exit | Вихід з поточної оболонки або сеансу. |
| head | Виводить перші кілька рядків файлу. |
| getent passwd username | Виводить інформацію про користувача з вказаним ім'ям користувача з бази даних користувачів. |
| man 5 passwd | Відображає сторінку посібника для файлу passwd (в звичайному випадку, конфігураційного файлу для користувачів і груп). |
| who | Виводить інформацію про відкриті сеанси користувачів. |
| w | Виводить додаткову інформацію про поточних користувачів і їх активність. |
| last | Виводить історію входів користувачів. |
| groupadd | Додає нову групу користувачів. |
| groupmod | Модифікує атрибути групи користувачів. |
| groupdel | Видаляє групу користувачів. |
| getent | Виводить записи з одного або більше файлів бази даних. |
| grep | Шукає вказаний текст у вказаному файлі або потоці даних. |
| useradd | Створює нового користувача. |
| usermod | Модифікує атрибути користувача. |
| passwd | Змінює пароль користувача або групи. |
| lastb | Виводить історію неуспішних спроб входу користувачів. |
| usermod -L | Блокує обліковий запис користувача. |
| usermod -U | Розблоковує обліковий запис користувача. |
| userdel | Видаляє обліковий запис користувача. |

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

**3. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):**

- виведіть інформацію про поточного користувача різними способами (підказка використовуйте команди id та grep);

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

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

- \*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;

- \*\*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;

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

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

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

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

- \*\*перегляньте інформацію про існуючі групи користувачів;

- \*\*видаліть створені Вами групи користувачів;

- \*\*перегляньте інформацію про існуючі групи користувачів.

**Контрольні запитання:**

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

Паролі не зберігаються в явному вигляді в конфігураційних файлах з метою безпеки. Якщо паролі зберігалися в явному вигляді, будь-яка особа, яка має доступ до файлу, зможе отримати доступ до облікових записів і використовувати їх для неправомірного доступу до системи.

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

Використання облікового запису root для повсякденних операцій не рекомендується з міркувань безпеки. Обліковий запис root має повний доступ до всіх ресурсів системи, тому якщо зловмисник отримає доступ до такого облікового запису, він зможе вчинити шкоду або змінити налаштування системи.

**3. \*У чому відмінність механізмів отримання особливих привілеїв su і sudo?**

Основна відмінність між механізмами отримання особливих привілеїв su і sudo полягає в тому, що su (substitute user) дозволяє користувачеві змінити свій ідентифікатор користувача на той, який вказаний (зазвичай root), а sudo (SuperUser Do) дозволяє користувачам виконувати окремі команди з підвищеними привілеями, не виходячи з-під свого облікового запису.

**4. \*Чому домашній каталог користувача root не розміщено в каталозі /home?**

Домашній каталог користувача root зазвичай розміщено в /root, а не в /home, для того щоб виділити його як окремий обліковий запис адміністратора системи і відокремити його від інших користувачів.

**5. \*Для чого використовується команда getent?**

Команда getent використовується для отримання інформації з різних баз даних системи, таких як база даних користувачів, груп, хостів і т.д.

**6. \*Як можна змінити пароль користувача?**

Пароль користувача можна змінити за допомогою команди passwd, наприклад: passwd username, де username - ім'я користувача.

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

Для видалення існуючих груп користувачів можна використати команду groupdel, наприклад: groupdel groupname. Інформація про групи зазвичай зберігається в файлі /etc/group.

**8. \*\*Яке призначення команди chage?**

Команда chage використовується для зміни налаштувань дати зміни пароля користувача, таких як термін дії пароля та т.д.

**9. \*\*Які параметри команди usermod ви вважаєте найбільш використовуваними?**

Найбільш використовуваними параметрами команди usermod є -c (змінення коментаря), -d (зміна домашнього каталогу), -e (зміна дати закінчення терміну дії облікового запису), -g (зміна основної групи користувача), -G (додавання користувача до додаткових груп), -l (зміна імені користувача) і -u (зміна UID користувача).

**Висновок:** отримала практичні навички роботи з командною оболонкою Bash, ознайомилась з базовими діями при створенні нових користувачів та нових груп користувачів.