“Київський фаховий коледж зв’язку”

Циклова комісія Комп’ютерної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №10**

з дисципліни: «Операційні системи»

**Тема: «Зміна власників і прав доступу до файлів в Linux. Спеціальні каталоги та файли в Linux»**

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 зміні власників файлів.
3. Знайомство з базовими діями при зміні прав доступу до файлів
4. Знайомство з спеціальними каталогами та файлами в Linux.

**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*** ***Заїка С. В.***

1. На базі розглянутого матеріалу дайте відповіді на наступні питання:
   1. Яке призначення команди id?

*Команда id використовується в операційних системах, таких як Linux і Unix, для відображення інформації про ідентифікатори користувачів і груп.*

*Зазвичай, коли ви виконуєте команду id без аргументів в командному рядку, вона повертає інформацію про ваш поточний ідентифікатор користувача (UID), ідентифікатор групи (GID) та список інших груп, до яких ви належите. Ця інформація може бути корисною для визначення прав доступу до файлів та каталогів.*

*Крім того, можна вказати іншого користувача або групу в якості аргумента команди id, щоб отримати інформацію про їхні ідентифікатори. Наприклад, команда id someuser поверне інформацію про ідентифікатор користувача та групу для користувача з іменем someuser.*

* 1. Як переглянути які права доступу має власник файлу?

*Для перегляду прав доступу до файлу, вам необхідно використовувати команду ls з аргументом -l, який вказує на відображення детальної інформації про кожен файл в поточному каталозі. Крім того, потрібно вказати назву файлу, права доступу до якого ви хочете переглянути.*

* 1. Як змінити власника групи?

*Щоб змінити власника групи для файлу в операційній системі Linux або Unix, ви можете використати команду chown з опцією -g, яка дозволяє змінити групу власника файлу.*

* 1. Як можна переглянути у терміналі який тип поточного файлу? Наведіть приклади для різних типів файлів.

*Щоб переглянути тип поточного файлу у терміналі, можна використати команду file. Вона повертає інформацію про тип файлу згідно з його змістом, а не тільки з розширенням його імені.*

* 1. Для чого використовуються дозволи Setuid та Setgid?

*Дозвіл Setuid (SUID) дозволяє запускати виконуваний файл в контексті власника файлу, а не в контексті користувача, який запускає його. Це дозволяє користувачам отримувати додаткові привілеї, необхідні для виконання певних завдань. Наприклад, команда passwd має дозвіл Setuid, тому користувач може змінити свій пароль, навіть якщо він не має дозволу на запис до файлу /etc/shadow, де зберігаються паролі.*

*Дозвіл Setgid (SGID) дозволяє встановлювати групу власника для виконуваних файлів та директорій. Якщо в директорії встановлено дозвіл SGID, всі нові файли та директорії, створені в цій директорії, будуть мати ту саму групу власника, що й директорія. Це дозволяє групі користувачів спільно працювати з файлами та директоріями, не дозволяючи іншим користувачам зовнішнього середовища отримати доступ до цих файлів та директорій.*

* 1. Для чого в системі потрібен так званий “липкий біт” (Sticky Bit). Наведіть приклади коли цей дозвіл доцільно використовувати.

*Sticky Bit - це спеціальний дозвіл в операційній системі Unix/Linux, який можна встановлювати для директорій. Якщо дозвіл Sticky Bit встановлено для директорії, то тільки власник файлу може його видалити або перейменувати.*

*Існує декілька сценаріїв використання дозволу Sticky Bit:*

*Забезпечення безпеки в системі файлової структури: Дозвіл Sticky Bit дозволяє забезпечити безпеку даних та запобігти їх випадковому видаленню. Наприклад, в директорії /tmp встановлюється дозвіл Sticky Bit, щоб забезпечити безпеку даних користувачів, які створюють тимчасові файли. Це дозволяє забезпечити, що інші користувачі не можуть випадково видалити або змінити файли, які не належать їм.*

*Спільний доступ до директорії: Якщо в директорії встановлено дозвіл Sticky Bit, то це дозволяє групі користувачів спільно працювати з файлами та директоріями, не дозволяючи іншим користувачам зовнішнього середовища отримати доступ до цих файлів та директорій. Це може бути корисно в тих випадках, коли користувачі мають обмежені права доступу до даних та потребують спільного доступу до спільних ресурсів.*

*Забезпечення приватності даних: Якщо в директорії з важливими даними встановлено дозвіл Sticky Bit, то це дозволяє забезпечити приватність даних та запобігти їх випадковому видаленню.*

**Хід роботи**

***Готував матеріал студент (Имя)***

1. Створіть таблицю команд вивчених у п.2 ходу роботи у наступному вигляді:

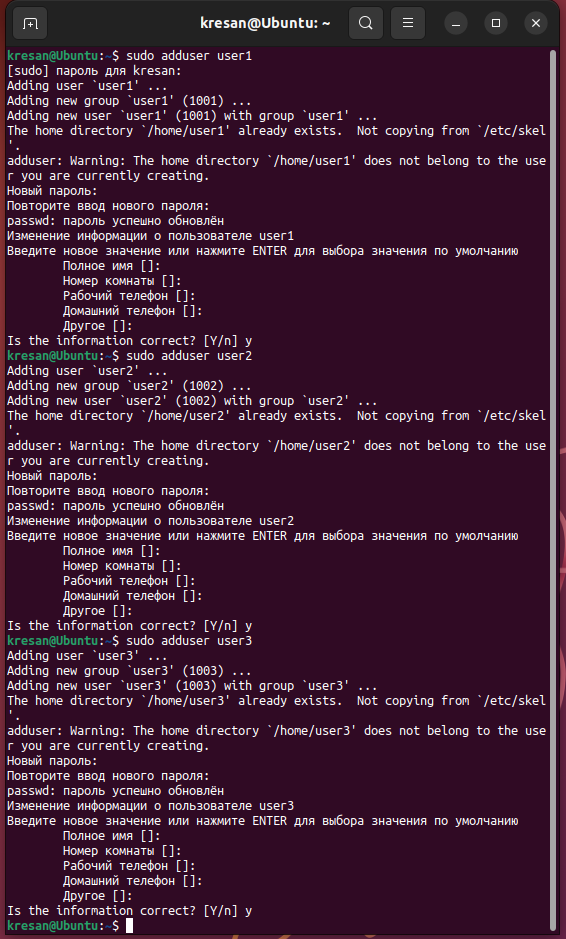
|  |  |
| --- | --- |
| **Назва команди** | **Її призначення та функціональність** |
|  |  |
|  |  |
|  |  |
|  |  |

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

***Готував матеріал студент Кресан Руслан***

1. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):
   * **створіть трьох нових користувачів;**

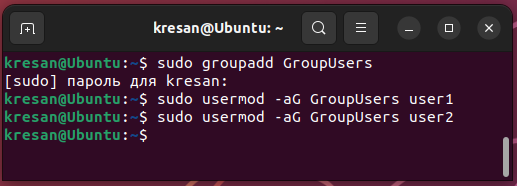
*Щоб створити трьох нових користувачів, слід виконати команду adduser. Після введення цієї команди в терміналі вам буде запропоновано ввести пароль та додаткову інформацію про користувача, якщо ви бажаєте. Після введення цієї інформації Linux створить нового користувача з вказаними параметрами.*



* + **створіть нову групу користувачів, туди додайте двох, з трьох створених користувачів;**

*Щоб створити нову групу користувачів і додати до неї двох з трьох створених користувачів в терміналі Linux, слід виконати наступні кроки:*

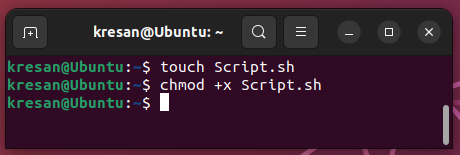
* *Створити нову групу користувачів за допомогою команди groupadd.*
* *Додати користувачів до нової групи за допомогою команди sudo usermod -aG.*



* + **створіть новий файл, який буде доступний на зчитування, редагування та виконання власником файлу, наприклад найпростіший скриптовий сценарій;**

*Щоб створити новий файл, який буде доступний на зчитування, редагування та виконання власником файлу, наприклад, найпростіший скриптовий сценарій в терміналі Linux, слід виконати наступні кроки:*

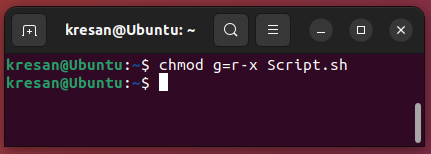
* + 1. *Створити новий файл за допомогою команди touch.*
    2. *Відкрити файл для редагування та додати вміст скрипту.*
    3. *Зберегти файл та встановити йому права на виконання за допомогою команди chmod +x.*



* + **для користувачів групи власника надайте дозволи на перегляд та виконання (без дозволу на редагування) цього файлу;**

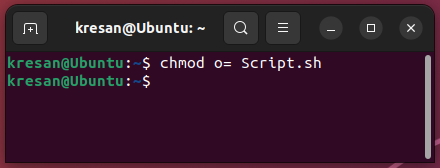
*Щоб надати дозволи на перегляд та виконання файлу для користувачів групи власника, не надаючи їм дозволу на редагування, слід виконати наступні кроки:*

1. *Виконати команду ls -l. Ця команда виведе поточні права доступу до файлу.*
2. *Замінити права доступу до файлу за допомогою команди chmod.*
3. *Встановити права доступу для користувачів групи власника файлу, не надаючи їм дозволу на редагування. Щоб цього досягти, слід встановити права r-x, які дозволять читати та виконувати файл, але не дозволять редагувати його. Для цього слід виконати команду chmod g=r-x.*



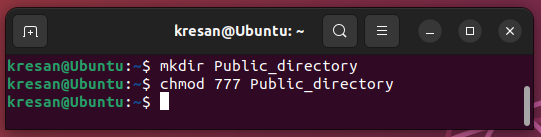
* + **для інших користувачів заборонити доступ до цього файлу;**

*Щоб заборонити доступ до файлу іншим користувачам, не належним до групи власника, слід виконати команду chmod o=, де o= встановлює права доступу для інших користувачів на немає доступу (тобто не можуть читати, записувати або виконувати файл).*

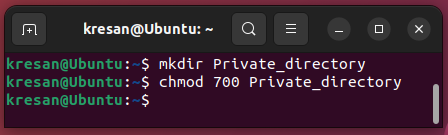


* + **подібні дії виконайте для директорій - створіть директорію, яка буде доступна для всіх трьох користувачів, створіть директорію, яку буде доступна тільки для власника, створіть директорію, яку користувачі групи власника зможуть переглядати, але не редагувати;**

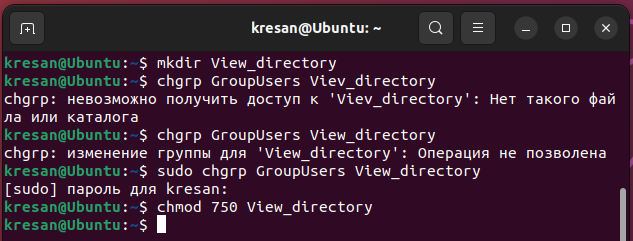
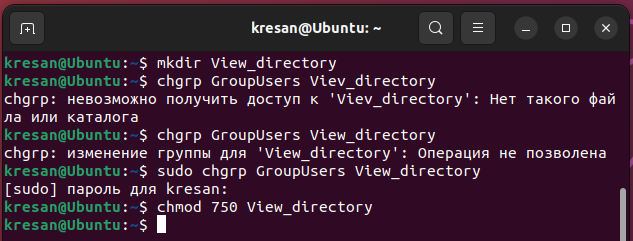
*Створення директорії, доступної для всіх трьох користувачів:*



*Створення директорії, яка доступна тільки для власника:*

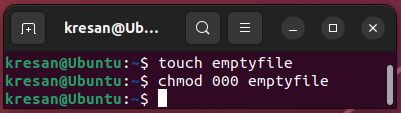


*Створення директорії, яку користувачі групи власника зможуть переглядати, але не редагувати:*

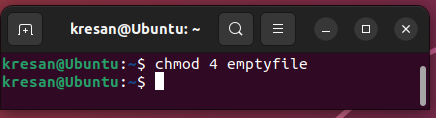


* + **створіть порожній файл під назвою emptyfile за допомогою команди touch emptyfile. Тепер “обнуліть” дозволи для файлу з chmod 000 emptyfile. Що станеться, якщо змінити дозволи для emptyfile, передавши лише одне значення для chmod у числовому режимі, наприклад, chmod 4 emptyfile? Що буде, якщо ми використаємо два числа, наприклад chmod 44 emptyfile? Що ми можемо дізнатися про те, як chmod зчитує числове значення?**

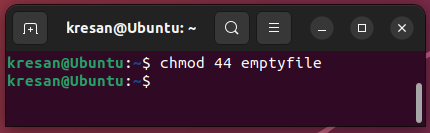
*Після виконання команди chmod 000 emptyfile всі дозволи на файл будуть обнулені, тобто будь-який користувач не зможе читати, редагувати або виконувати файл.*



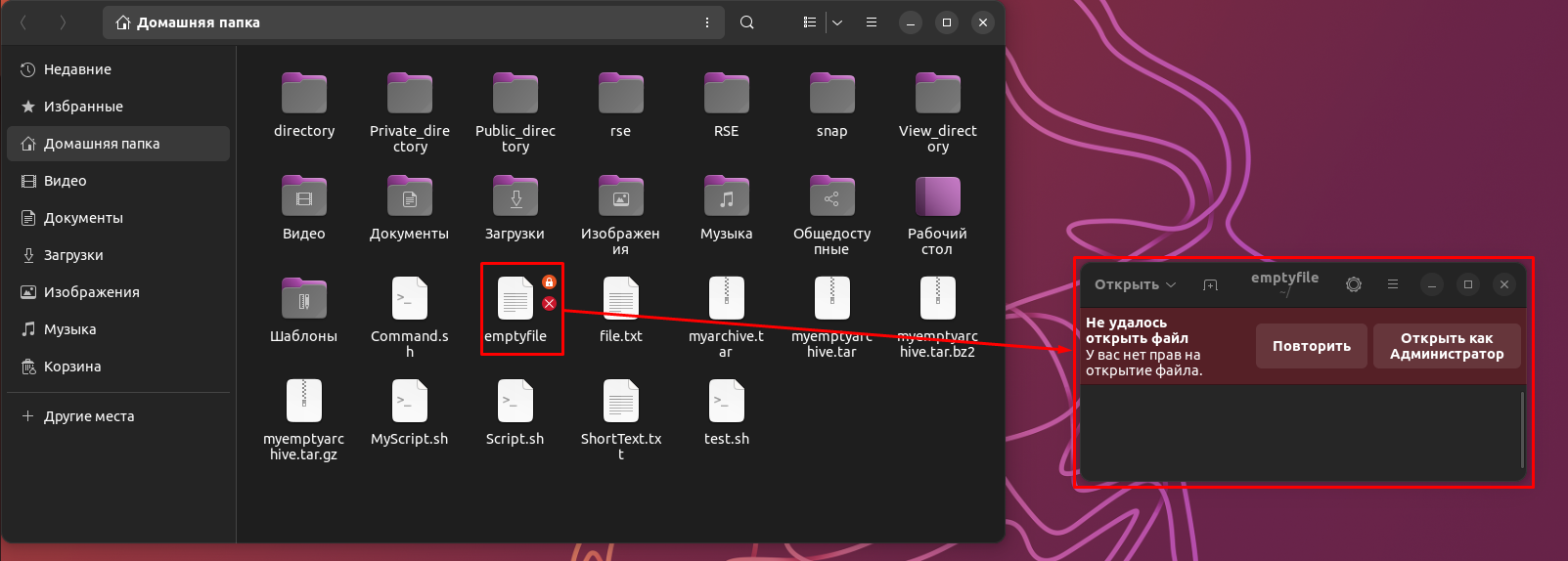
*Якщо ми виконаємо команду chmod 4 emptyfile, то ми встановимо тільки дозвіл на читання для власника файлу, тому що 4 відповідає бінарному значенню 100, що встановлює дозвіл на читання тільки для власника. Для групи та інших користувачів дозволи будуть залишатися незмінними (тобто будуть рівні нулю).*



*Якщо ми виконаємо команду chmod 44 emptyfile, то ми встановимо дозволи на читання для власника та групи файлу, а для інших користувачів дозволи будуть залишатися незмінними.*



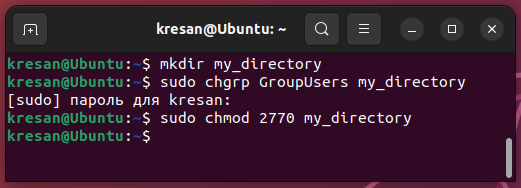
*При використанні числового режиму в chmod, ми можемо встановити різні дозволи для власника, групи та інших користувачів, використовуючи різні комбінації чисел. Кожне число відповідає бітовому значенню дозволів (4 для читання, 2 для запису, 1 для виконання), і можна додавати ці числа для встановлення різних комбінацій дозволів.*



* + **створіть каталог під назвою, де всі файли автоматично будуть належати Вашій групі користувачів і можуть бути видалені лише користувачем, який їх створив?**

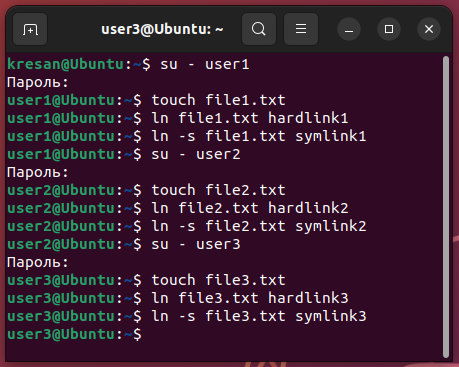
*Опція 2 встановлює SetGID-біт, що означає, що всі файли та папки, що створюються в директорії, належатимуть групі користувачів, до якої належить директорія. Опція 7 встановлює належність тільки власнику та групі користувачів, а також дозволяє їм читати, писати та виконувати файли. Опція 0 встановлює нульові дозволи для всіх інших користувачів.*

*Тепер всі файли та директорії, які створюються в директорії my\_directory, належатимуть до вашої групи користувачів, а інші користувачі не зможуть видалити файли, які були створені в цій директорії.*

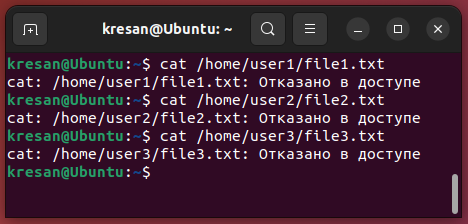


* + **під кожним користувачем створіть по одному новому файлу, та жорстке та символічне посилання на нього;**

*Для створення нових файлів та жорстких посилань на них, використаємо наступні команди:*



* + **спробуйте іншими користувачами переглянути ці файли;**



* + **спробуйте іншими користувачами видалити ці файли, зробіть висновки.**

*Інші користувачі, які не є власниками файлів, не можуть їх видалити без відповідних дозволів. У разі, якщо файли були створені з дозволами, які дозволяють власникам групи виконувати операції з файлом, інші користувачі з цієї групи можуть мати деякі права на файл, наприклад, можуть його переглядати, але не можуть видалити без додаткових дозволів. Таким чином, власник файлу або користувач з відповідними дозволами можуть видалити ці файли, а інші користувачі не можуть цього зробити.*

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

**Відповіді на контрольні запитання**

1. Наведіть приклади зміни прав доступу символічним методом (Symbolic Method)?

*Символічний метод - це спосіб зміни прав доступу до файлів та директорій в Unix / Linux, який використовує символьні мнемоніки для встановлення нових прав.*

*Приклади зміни прав доступу за допомогою символічного методу:*

*Для зміни прав доступу до файла file.txt так, щоб власник міг зчитувати, редагувати і виконувати його, група могла зчитувати, а всі інші користувачі не мали доступу, виконайте наступну команду: chmod u+rwx,g+r,o-rwx file.txt*

*Для зміни прав доступу до директорії mydir так, щоб всі користувачі могли зчитувати та виконувати файли у цій директорії, але тільки власник міг редагувати файли, виконайте наступну команду: chmod u+rwx,g+rx,o+rx mydir*

*Для зміни прав доступу до файла script.sh так, щоб всі користувачі могли виконувати його, але не могли редагувати або зчитувати його, виконайте наступну команду: chmod a+x script.sh*

*У цих прикладах команда chmod використовує символьну нотацію для встановлення прав доступу до файлів та директорій. u вказує на власника файлу, g вказує на групу користувачів, o вказує на інші користувачі, а a вказує на всіх користувачів. r означає право на зчитування файлу, w - право на його редагування, а x - право на виконання файлу.*

1. Наведіть приклади зміни прав доступу числовим методом (numeric method, octal method)?

*Числовий метод (або октальний метод) - це спосіб зміни прав доступу до файлів та директорій в Unix / Linux, який використовує восьмеричні числа для встановлення нових прав. Кожне право (зчитування, запис, виконання) має свій власний числовий код, а отримані коди об'єднуються в восьмеричне число, що відображає потрібний набір прав.*

*Приклади зміни прав доступу за допомогою числового методу:*

*Для зміни прав доступу до файла file.txt так, щоб власник міг зчитувати, редагувати і виконувати його, група могла зчитувати, а всі інші користувачі не мали доступу, виконайте наступну команду: chmod 750 file.txt*

*У цьому випадку число 7 відповідає за права доступу власника (зчитування, запис і виконання), число 5 відповідає за права доступу групи (зчитування та виконання), а число 0 відповідає за права доступу інших користувачів (без доступу).*

*Для зміни прав доступу до директорії mydir так, щоб всі користувачі могли зчитувати та виконувати файли у цій директорії, але тільки власник міг редагувати файли, виконайте наступну команду: chmod 755 mydir*

*У цьому випадку число 7 відповідає за права доступу власника (зчитування, запис і виконання), число 5 відповідає за права доступу групи (зчитування та виконання), а число 5 відповідає за права доступу інших користувачів (тільки зчитування та виконання).*

*Для зміни прав доступу до файла script.sh так, щоб всі користувачі могли виконувати його, але не могли редагувати або зчитувати його, виконайте наступну команду: chmod 111 script.sh*

*У цьому випадку у всіх трьох числових значеннях встановлено тільки дозвіл на виконання, що відповідає значенню 1 в октальній системі. Таким чином, тільки користувачі можуть виконувати файл script.sh, але не можуть читати або редагувати його.*

1. Чи можна виконати файл, для якого є права на виконання, але не встановлені права на читання (--x)? Поясніть.

*Так, можна виконати файл, для якого є права на виконання, але не встановлені права на читання. Це можливо тому, що для виконання файлу не потрібно читати його вміст. При виконанні файлу, операційна система просто виконує інструкції, які зберігаються в файлі, і виводить результат на екран або в інший вихідний потік.*

*Наприклад, якщо у файлу є право на виконання, але немає права на читання, ви все ще зможете запустити цей файл як скрипт на виконання. Однак, якщо ви спробуєте прочитати вміст файлу до того, як виконати його, то отримаєте помилку від операційної системи.*

1. Яке призначення команди umask?

*Команда umask в Unix / Linux встановлює значення маски дозволів за замовчуванням для новостворених файлів та директорій в поточній сесії. Маска дозволів за замовчуванням віднімається від максимально дозволених прав доступу, тобто вона визначає, які дозволи за замовчуванням не будуть встановлюватись при створенні нових файлів та директорій.*

*Значення маски дозволів за замовчуванням можна встановити від 0 до 777 в вісімковому форматі. Кожна цифра представляє маску дозволів для відповідної групи користувачів (власник, група та інші). Наприклад, якщо маска дозволів за замовчуванням встановлена як 022, це означає, що з максимально дозволених прав доступу будуть відняті дозволи на запис для групи та інших користувачів.*

1. Якщо ми змінюємо права доступу та дозволи в поточній сесії чи будуть вони збережені в наступній?

*Зміна прав доступу та дозволів в поточній сесії зазвичай є тимчасовою і не буде збережена після закриття сесії або перезавантаження системи.*

*Якщо ви змінюєте права доступу та дозволи в поточній сесії, то вони застосовуються до всіх файлів та директорій, з якими ви взаємодієте під час цієї сесії. Ці зміни не будуть застосовані до інших сеансів взаємодії з системою або до інших користувачів, крім випадку, якщо ви змінюєте права доступу в системних файлів або використовуєте команди, які використовують ці права як частину своєї функціональності.*

1. Чи є якийсь шаблон, яким система користується щодо прав та доступів при створенні нових файлів. Як можна змінити права дозволу за замовчуванням?

*Так, у більшості операційних систем є шаблон, який використовується для прав доступу при створенні нових файлів та директорій. Зазвичай, коли створюється новий файл або директорія, система використовує значення за замовчуванням, які можна налаштувати за допомогою команди umask. Значення umask встановлює бітову маску, яка віднімає певні дозволи доступу при створенні нових файлів та директорій.*

*Зазвичай значення за замовчуванням для нових файлів мають права -rw-rw-rw- або 666, що означає, що всі користувачі мають дозвіл на читання та запис, але не на виконання. Для нових директорій значення за замовчуванням зазвичай є -rwxrwxrwx або 777, що означає, що всі користувачі мають повний доступ до директорії.*

*Щоб змінити права дозволу за замовчуванням, можна встановити нове значення umask. Наприклад, якщо ви хочете встановити права доступу для нових файлів на -rw-r--r-- або 644, ви можете виконати наступну команду: umask 022*

1. Уявіть, що програмі потрібно створити одноразовий тимчасовий файл, який більше ніколи не знадобиться після закриття програми. Який правильний каталог для створення цього файлу?

*Найкраще місце для створення тимчасових файлів у більшості операційних систем - це /tmp або /var/tmp. Ці каталоги зазвичай призначені саме для тимчасових файлів та мають правильні права доступу, щоб забезпечити безпеку та ефективність системи. Для створення тимчасового файлу можна використовувати команду mktemp, яка автоматично створює унікальний файл з випадковою назвою та правами доступу. Наприклад, команда mktemp /tmp/tempfile.XXXXXX створить тимчасовий файл зі змінною частиною XXXXXX у каталозі /tmp. Після використання тимчасового файлу його потрібно видалити за допомогою команди rm, щоб звільнити місце в системі.*

1. Яким чином можна створити жорстке посилання? В яких ситуаціях їх доцільно використовувати?

*Жорстке посилання (hard link) - це ім'я файлу, яке посилається на той же самий вузол файлової системи, що й початкове ім'я файлу. Файли, на які посилаються жорсткі посилання, виглядають як один файл, оскільки вони мають одинакові inode та вказують на один і той же блок даних на диску.*

*Для створення жорсткого посилання використовується команда ln з опцією -s, аргументами якої є вихідний файл та ім'я жорсткого посилання. Наприклад, щоб створити жорстке посилання file2 на файл file1 в поточному каталозі, необхідно виконати команду: ln file1 file2*

*Жорсткі посилання зазвичай використовуються в ситуаціях, коли потрібно мати доступ до одного файлу з різних імен або коли потрібно створити бекапи файлів. Вони дозволяють зменшити кількість дискового простору, оскільки вони посилаються на один і той же блок даних на диску. Також, якщо вихідний файл буде переміщено або перейменовано, жорстке посилання на нього все ще буде працювати, оскільки воно посилається на inode, а не на ім'я файлу. Однак, жорсткі посилання не можуть бути створені на іншому диску або файловій системі, і вони не можуть посилатися на каталоги.*

1. Яким чином можна створити символічне посилання? В яких ситуаціях їх доцільно використовувати?

*Символічні посилання (symlink або soft link) - це особливий тип файлу, який створюється для посилання на інший файл або каталог. Він містить посилання на ім'я файлу, а не на його інодінійну структуру, і тому може посилатися на файл або каталог незалежно від його місцезнаходження в файловій системі.*

*Для створення символічного посилання використовується команда* ***ln*** *з опцією* ***-s****: ln -s /шлях/до/оригінального\_файлу /шлях/до/символічного\_посилання*

*Наприклад, якщо ми хочемо створити символічне посилання на файл* ***/home/user/Documents/report.txt*** *в каталозі* ***/home/user/Downloads****, ми можемо виконати наступну команду: ln -s /home/user/Documents/report.txt /home/user/Downloads/report-link*

*Тепер у каталозі* ***/home/user/Downloads*** *з'явиться файл з ім'ям* ***report-link****, який буде посилатися на файл* ***report.txt*** *у каталозі* ***/home/user/Documents****.*

*Символічні посилання можуть бути корисними в таких ситуаціях:*

* *При створенні посилання на довгий шлях до файлу з короткою назвою, щоб полегшити доступ до файлу.*
* *При розміщенні файлів, які часто переміщуються, на зовнішніх носіях або в мережевих каталогах, щоб забезпечити стабільний доступ до цих файлів, незалежно від їх місцезнаходження.*
* *При створенні багатьох ідентичних копій одного файлу, щоб зменшити обсяг зайнятого місця на диску.*
* *При створенні посилання на каталог, щоб мати дві різні назви для одного й того ж каталогу.*

1. Порівняйте жорсткі та символічні посилання?

*Жорстке та символічне посилання - це два способи створення посилань на файл або каталог у Linux.*

*Жорстке посилання створюється шляхом створення нового запису в файловій системі, який посилається на той самий вузол файлової системи, що й оригінальний файл. Жорстке посилання може бути використане для доступу до оригінального файлу з різних директорій, включаючи ту саму директорію, де знаходиться оригінальний файл. Він не може бути створений для каталогів і не може пересікати межі файлових систем.*

*Символічне посилання - це запис, який містить шлях до оригінального файлу. Воно створюється за допомогою команди ln з опцією -s. Символічне посилання може пересікати межі файлових систем та бути створене для каталогів. Воно може бути використане для створення зручного шляху до оригінального файлу з різних директорій.*

*Одна з основних відмінностей між жорстким та символічним посиланням полягає у тому, що якщо ви видаляєте оригінальний файл, то жорстке посилання на нього все ще буде існувати і матиме доступ до даних файлу, але якщо ви видаляєте оригінальний файл, на який посилається символічне посилання, то символічне посилання буде недійсним.*

*Жорсткі посилання короткі та ефективні, оскільки не використовують додаткової пам'яті, щоб зберігати додаткову інформацію про посилання. Символічні посилання надають більшу гнучкість та зручність, оскільки вони можуть бути використані для створення посилань на каталоги та файлові системи, які перетинаються.*

1. Є файл оригінал та для нього створено два посилання - символічне та жорстке. Що відбудеться з іншими файлами, якщо видалити:
   * файл оригінал;

*При видаленні оригінального файлу, жорстке посилання продовжить існувати і буде посилатися на той самий вміст*

* + символічне посилання;

*Якщо видалити символічне посилання, то оригінальний файл залишиться на місці, але символічне посилання буде недійсним і вказуватиме на ніщо.*

* + жорстке посилання.

*Однак, якщо ви видалите жорстке посилання, то оригінальний файл і символічне посилання не будуть зберігатись на жорсткому диску, і будуть недійсними.*

***Готував матеріал студент (Имя)***

**Висновки**

В ході виконання лабораторної роботи …