“Київський фаховий коледж зв’язку”

Циклова комісія комп’ютерної та програмної 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”

Виконали студенти

групи БІКС-13

Команда JRSY: Андрущик П.С   
Бурбан Д.Ю.  
Перевірив викладач

Сушанова В.С.

Київ 2024

**The goal of the work: (робила студентка Андрущик Поліна)**1. Getting hands-on skills with the Bash shell.  
2. Getting to know the basic actions when changing file owners, file access rights  
3. Introduction to special directories and files in Linux.  
  
**1. \*Read the short theoretical information for the laboratory work and make a small dictionary of basic English terms for the assignment of commands and their parameters.**

|  |  |
| --- | --- |
| **Term in English** | **Term in Ukrainian** |
| User Owner | Користувач, якому належить файл. За замовчуванням користувач, який створює файл, стає його власником. Право власності користувача можна змінити, але зазвичай потрібні права адміністратора. Право власності пов’язане з ідентифікатором користувача (UID). |
| Group Owner | Кожен файл також має власника групи. За замовчуванням власником групи стає основна група користувача, який створює файл. Користувачі можуть змінити групу власників файлів, якими вони володіють, на будь-яку групу, до якої вони належать. Право власності на групу пов’язано з ідентифікатором групи (GID). |
| UID | Ідентифікатор користувача. Числовий ідентифікатор, пов’язаний з обліковим записом користувача. |
| GID | ID групи. Числовий ідентифікатор, пов’язаний з обліковим записом групи. |
| Sticky bit | Спеціальний дозвіл для каталогів, щоб гарантувати, що лише власник файлу може видалити його, навіть якщо інші мають дозвіл на запис до каталогу. |

**On the basis of the considered material, answer the following questions:  
1. What is the purpose of the id command?**The id command is used to retrieve information about a user's identity, including a unique user identifier (UID), username, group identifier (GID), and group membership.  
**2. How to see what access rights the owner of a file has?**To view the access rights of a file's owner, you can use the ls -l command, which will display detailed information about the file, including access rights, owner, and owner's group.  
**3. \*How to change the group owner?**To change the owner of a group, use the chown command, specifying the new group owner and the file or directory to which you want to apply the changes.   
sudo chown :new\_owner\_group file\_or\_directory **4. \*How can you view the current file type in the terminal? Give examples for different types of files**To view the current file type in the terminal, you can use the file command.For a text file:  
file example.txt  
  
For an executable file (program):  
file my\_program  
  
For the catalog:  
file my\_directory  
**5. \*\*What are Setuid and Setgid permissions used for?**Setuid (Set User ID) and Setgid (Set Group ID) permissions are used to change the execution context of a program or access files depending on the owner of the file. When a program has Setuid permission, it runs with the rights of the owner of the file, not the user who launched it. This can be useful for applications that require special privileges, such as access to system resources. Setgid allows a program or file to use the rights of the owner's group instead of the group of the user who launched the program. This can be useful for group work on files when users belong to different groups.  
**6. \*\*Why does the system need the so-called “sticky bit” (Sticky Bit)? Give examples of when this permission should be used.**Sticky Bit is used in the system to prohibit the deletion or renaming of files except for the file owner, directory owner, and system administrator. This is especially useful in situations where multiple users have access to shared directories or files, and you want to ensure that each user can create, modify, or delete their own files in those directories, but cannot delete or modify other users' files.

For example, consider a situation where a system administrator creates a shared directory to which different users have access. To prevent accidental or intentional deletion or renaming of files by other users, the administrator can set the sticky bit on this directory. Therefore, while users can create, modify, or delete their files in this directory, they will not be able to delete or rename the files of other users who also have access to this directory.

Using the sticky bit allows you to preserve the confidentiality and security of files in shared directories, to avoid accidental or intentional deletion of files by other users, and to ensure appropriate management of access to system resources.  
  
**The main positions of the course of work:**