УДК 004.056.52

DOI: 10.31673/2412-9070.2020.043845

К. П. СТОРЧАК, канд. техн. наук, доцент;
Д. В. КРАВЕЦЬ, ст. викладач;
А. М. ТУШИЧ, ст. викладач;
Д. В. СОРОКІН, аспірант,
Державний університет телекомунікацій, Київ

АНАЛІЗ МЕТОДІВ ОРГАНІЗАЦІЇ ПРАВ КОРИСТУВАЧІВ У GNU\LINUX СИСТЕМАХ

Розглянуто методи організації прав користувачів у GNU\Linux системах, зокрема надання прав кожному користувачу окремо та об'єднання користувачів з однаковими або подібними правами у групи. Сформовано поняття користувача операційної системи та суперкористувача. Визначено переваги об'єднання користувачів у групи за рівнем доступу. Проаналізовано критерії поділу користувачів на групи залежно від формату використання комп'ютера, структури організації, яка володіє конкретним комп'ютером, та від кількості та посад людей, що будуть працювати з ним. Розглянуто формат збереження прав на файл або каталог та механізм перевірки доступу до файла або каталогу.

Ключові слова: моделювання інформаційних систем; операційна система; GNU\Linux; користувач; група користувачів; права користувача; рівень доступу; адміністрування; тонкий клієнт; сервер; організація роботи; біт; байт; читання; зміна; виконання; файл; каталог; суперкористувач.

ВСТУП

Постановка проблеми. На сучасному рівні розвитку науки і техніки все більше і більше організацій змушені переходити до роботи на комп'ютерах. У випадках, коли комп'ютер використовують кілька осіб, або коли робота на комп'ютері організована за схемою «тонкий клієнт», постає потреба у розмежуванні прав користувачів різних рівнів доступу та адміністраторів системи.

Оскільки більшість дистрибутивів операційних систем сімейства GNU\Linux поширюються безкоштовно, питання організації прав користувачів у таких системах важливе для установ, які не можуть собі дозволити придбати ліцензійну версію інших операційних систем, вважаючи це економічно недоцільним, або мають недостатньо потужне обладнання для роботи інших операційних систем.

Мета статті. Метою статті є аналіз наявних методів організації прав користувачів для операційних систем сімейства GNU\Linux.

Оскільки операційні системи сімейства GNU\Linux розраховано на велику кількість користувачів, питання про організацію розмежування доступу до файлів і каталогів є важливим, і операційна система повинна мати інструменти для його вирішення. Механізми розмежування доступу, встановлені для системи UNIX в 1970-х роках, дуже прості, але вони виявилися настільки ефективними, що й донині успішно виконують поставлені перед ними завдання.

ОСНОВНА ЧАСТИНА

Поняття користувача

Під користувачем розуміємо будь-кого, хто працює з комп'ютером. Як правило, для кожного користувача в системі створюється окремий акаунт, яким присвоюється спеціальне ім'я. За допомогою імені користувач отримує доступ до свого облікового запису і, врешті-решт, до системи. Деякі системні служби запускаються або привілейованими акаунтами, або строго визначеними акаунтами користувачів [1].

Механізм користувачів було розроблено з міркувань безпеки для обмеження доступу до різних частин системи. Кожний користувач може отримати доступ до конкретних каталогів та файлів і водночас бути обмеженим у доступі до інших каталогів чи файлів та до налаштувань операційної системи.

Суперкористувач має повний доступ до операційної системи і її налаштувань. Цей обліковий запис використовується тільки для цілей системного адміністрування.

Групи користувачів

Групи користувачів було розроблено для того, щоб розширити можливості керування правами. У ситуації, коли в організації співробітники для роботи під'єднуються зі своїх робочих місць до одного сервера, необхідним є розмежування користувачів з адміністративними правами і простих користувачів [2]. У кожної людини свій акаунт на сервері. Адміністратори можуть налаштовувати систему, проте користувачам краще не надавати зайвих прав заради стабільної роботоздатності системи. Тому адміністратори об'єднуються в окрему групу, якій надається доступ до всього обладнання, а користувачам, організованим у групу користувачів, дається можливість читати і записувати файли в необхідні каталоги. За потреби груп користувачів може бути більше. Кількість груп користувачів може залежати від такого:

• кількості людей, що працюють на сервері;
• структури організації;
• рівня технічної обізнаності працівників різних підрозділів організації;
• рівня конфіденційності інформації, з якою працюють у тому чи іншому підрозділі.

Кожний користувач може бути введений до однієї або кількох груп. Створює і видаляє групи суперкористувач, який також може змінювати склад учасників тієї чи іншої групи.

Зазвичай існує можливість призначати права для кожного користувача окремо, уможливлюючи йому доступ до того чи іншого файла, але це потребує великого часового ресурсу адміністраторів. Для економії часу адміністраторів було створено механізм об'єднання користувачів у групи. Також механізм груп користувачів корисний для керування службовими користувачами сервісів, запущених в системі.

Права груп і користувачів на каталог або файл

В індексному дескрипторі кожного файла записано ім'я так званого власника файла і групи, яка має права на цей файл. Спочатку, на етапі розроблення файла його власником оголошується той користувач, який цей файл підготував. Точніше — той користувач, від чийого імені запущено процес, який створює файл. Група теж призначається під час створення файла — за ідентифікатором групи процесу, що утворює файл. Власника та групу файла можна замінити в ході подальшої роботи за допомогою команд chown і chgrp.

Права доступу та інформація про тип файла в операційних системах сімейства GNU\Linux зберігаються в індексних дескрипторах в окремій структурі, що складається з двох байтів, тобто 16 біт. Чотири біти з 16-ти відведено для кодованого запису про тип файла. Наступні три біти задають особливі властивості виконуваних файлів. І, нарешті, 9 біт визначають права доступу до файла. Ці 9 біт діляться на три групи по три біти. Перші три біти задають права користувача, наступні три біти — права групи, останні три біти визначають права всіх інших користувачів, тобто всіх користувачів, за винятком власника файла і групи файла.

Водночас, якщо відповідний біт має значення 1, то право надається, а якщо він дорівнює 0, то право не надається. У символьній формі запису прав одиниця замінюється відповідним символом *r*, *w* або *x* (від англ. *read, write, execute*), а нуль подається прочерком.

Право на читання *r* файла означає, що користувач може переглядати вміст файла за допомогою різних команд перегляду через будь-який текстовий редактор. Але, відредагувавши вміст файла в текстовому редакторі, користувач не зможе зберегти зміни у файлі на диску, якщо не має права на запис *w* у цей файл. Право на виконання *x* означає, що користувач може завантажити файл у пам'ять і спробувати запустити його на виконання як виконувану програму. Зазвичай, якщо в дійсності файл не є програмою або скриптом, то запустити цей файл на виконання не вдасться, проте навіть якщо файл дійсно є програмою, але право на виконання для нього не встановлено, то він теж не запуститься.

Згідно з каталогами трактування понять «право на читання», «право на запис» і «право на виконання» дещо змінюється. Право на читання відповідно до каталогів легко зрозуміти, якщо згадати, що каталог — це просто файл, який містить список файлів у даному каталозі. Отже, якщо ви маєте право на читання каталогу, то ви можете переглядати його вміст (цей самий список файлів у каталозі). Маючи право на запис, користувач може створювати і видаляти файли в цьому каталозі, тобто просто додавати в каталог або видаляти з нього файли. Право на виконання в такому разі означає право переходити в цей каталог. Якщо власник каталогу хоче дати доступ іншим користувачам на перегляд якогось файла в своєму каталозі, ви повинні надати їм право доступу в каталог, тобто дати їм «право на виконання каталогу». Більш того, потрібно дати іншим користувачам право на виконання для всіх каталогів, що стоять у дереві вище даного каталогу. Тому для всіх каталогів за замовчуванням встановлюється право на виконання як для власника і групи, так і для всіх інших користувачів. І вже якщо виникає потреба у закритті доступу в каталог, то необхідно позбавити всіх користувачів (зокрема групи) права входити в цей каталог

Може здатися, що право на читання каталогу не дає нічого нового порівняно з правом на виконання. Однак різниця в цих правах усе ж таки є. Якщо задати тільки право на виконання, користувач може увійти в каталог, але не зможе побачити там жодного файла.

Алгоритм перевірки прав користувача під час звернення до файла можна описати у такий спосіб. Система спочатку перевіряє, чи збігається ім'я користувача з ім'ям власника файла. Якщо ці імена збігаються, то перевіряється, чи має власник відповідне право доступу: на читання, на запис або на виконання, оскільки суперкористувач може позбавити деяких прав власника файла. Якщо право таке є, то відповідна операція дозволяється. Якщо ж потрібного права власник не має, то перевірка прав, наданих через групу або через групу атрибутів доступу для інших користувачів, вже не здійснюється, а користувачеві видається повідомлення про неможливість виконання дії.

Змінювати права доступу до файла за допомогою команди chmod може тільки сам власник файла чи суперкористувач. Для того щоб мати можливість змінити права групи, власник повинен додатково бути членом тієї групи, якій він хоче дати права на даний файл.

Висновки

Задача організації прав користувачів може вирішуватись за допомогою безпосереднього надання прав на необхідні файли і каталоги кожному користувачу, а також об'єднанням користувачів зі схожими або однаковими правами в групи.

Список використаної літератури

1. ***Users*** *and groups [Електронний ресурс]. 2020. URL:*

https://wiki.archlinux.org/index.php/Users_and_groups.

2. ***Hertzog R., Mas R.*** *The Debian Administrator's Handbook // Computers & Internet. 2020. 541 с.*

К. П. Сторчак, Д. В. Кравец, А. Н. Тушич, С. В. Сорокин

АНАЛИЗ МЕТОДОВ ОРГАНИЗАЦИИ ПРАВ ПОЛЬЗОВАТЕЛЕЙ В GNU\LINUX СИСТЕМАХ

Рассмотрены методы организации прав пользователей в GNU\Linux системах, такие как предоставление прав каждому пользователю отдельно и объединение пользователей с одинаковыми или подобными правами в группы. Сформировано понятие пользователя операционной системы и суперпользователя. Определены преимущества объединения пользователей в группы по уровню доступа. Проанализированы критерии разделения пользователей на группы в зависимости от формата использование компьютера, структуры организации, которая владеет конкретным компьютером, и от количества и должностей людей, которые будут работать с ним. Рассмотрены формат сохранения прав на файл или каталог и механизм проверки доступа к файлу или каталогу.

Ключевые слова: моделирование информационных систем; операционная система; GNU\Linux; пользователь; группа пользователей; права пользователя; уровень доступа; администрирование; тонкий клиент; сервер; организация работы; бит; байт; чтение; изменение; исполнение; файл; каталог; суперпользователь.

K. Storchak, D. Kravets, A. Tushych, D. Sorokin

ANALYSIS OF METHODS FOR ORGANIZING USER RIGHTS IN GNU\LINUX SYSTEMS

This article is about user's rights to files or directories. The GNU\Linux systems have many great security features, but one of the most important is the file permissions system. Methods for organizing user rights in GNU\Linux systems, such as granting rights to each user individually and grouping users with the same or similar rights into groups, are discussed. The concept of operating system user and superuser is formed. The benefits of grouping users by access level have been identified. The criteria for dividing users into groups are analyzed, depending on the format of computer use, the structure of the organization that owns a particular computer and the number and positions of people who will work with it. Also, the benefit of the mechanism of organizing users into groups to manage service users of services running in the system is considered. It is said that any file and directory in Linux has an owner user and an owner group. That is, any file and directory belongs to some system user and some group. In addition, any file and directory has three access rights groups: one for the owner user, one for members of the owner group, and one for all other users on the system. Each group consists of the rights to read, write and execute the file for execution. The format of saving rights to a file or directory and the mechanism of checking access to a file or directory are considered. An explanation is given of what the right to read, the right to modify and the right to execute means for the file and for the directory. It is with the help of these sets of permissions that the permissions of files in Linux are established. Each user can only have full access to files that he owns or those that he is allowed to access. Only the Root user can work with all files, regardless of their set of permissions.

Keywords: modeling of information systems; operating system; GNU\Linux; user; user group; user rights; access level; administration; thin client; server; work organization; bit; byte; read; change; execution; file; directory; superuser.