Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Щербак Маргарита Романовна, НПИбд-02-21

2024

Содержание

# Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей [1].

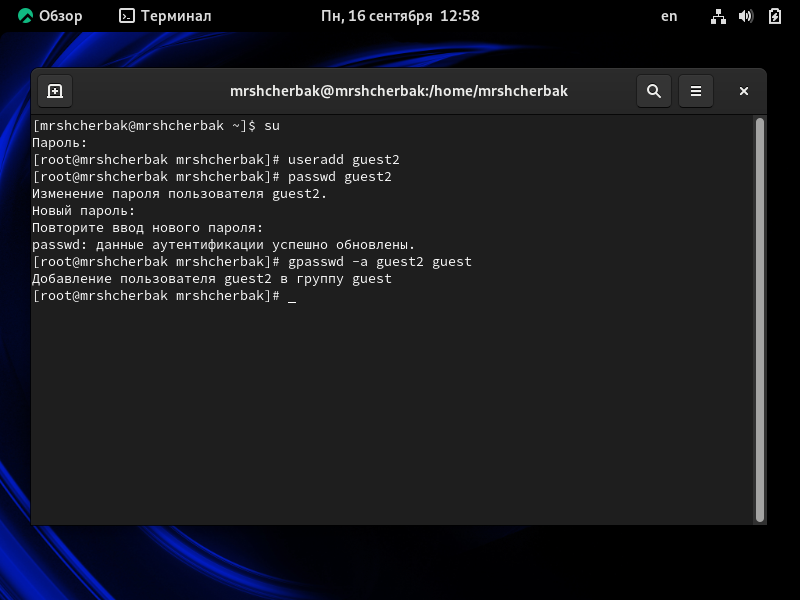
# Теоретическое введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Права доступа в системах управляют тем, какие операции может выполнять пользователь с определенными файлами и папками. Правильная настройка прав доступа помогает создать безопасную среду, где никто не сможет изменять ваши данные или нарушать работу важных системных файлов. Помимо групп root и users, в системе существует множество других, которые созданы для управления доступом программ к общим ресурсам. Участники каждой группы получают права на чтение или изменение конкретных файлов и каталогов, что регулирует их доступ и действия. Эти же права передаются процессам, которые запускает пользователь [2].

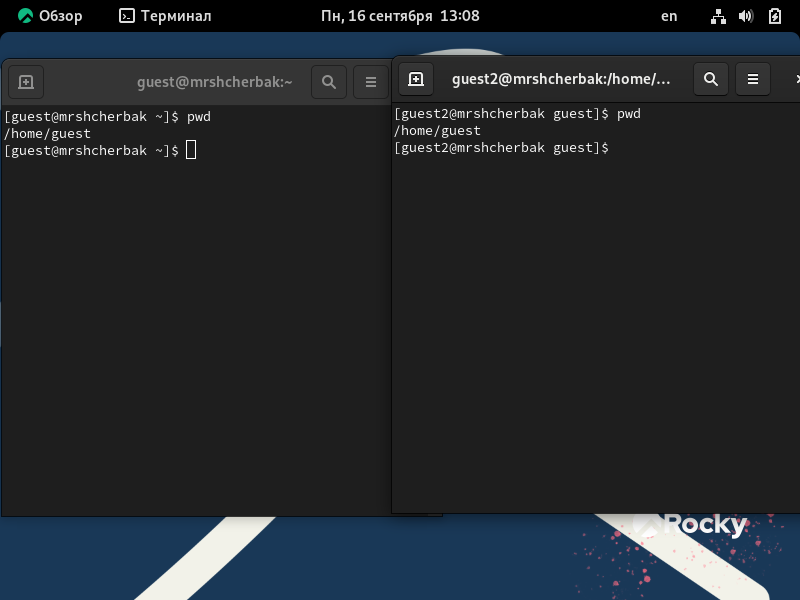
# Выполнение лабораторной работы

1. В установленной операционной системе создадим учётную запись пользователя guest2. Зададим пароль для пользователя guest2 (используя учётную запись администратора). Добавим пользователя guest2 в группу guest (рис.1).



Выполнение команд

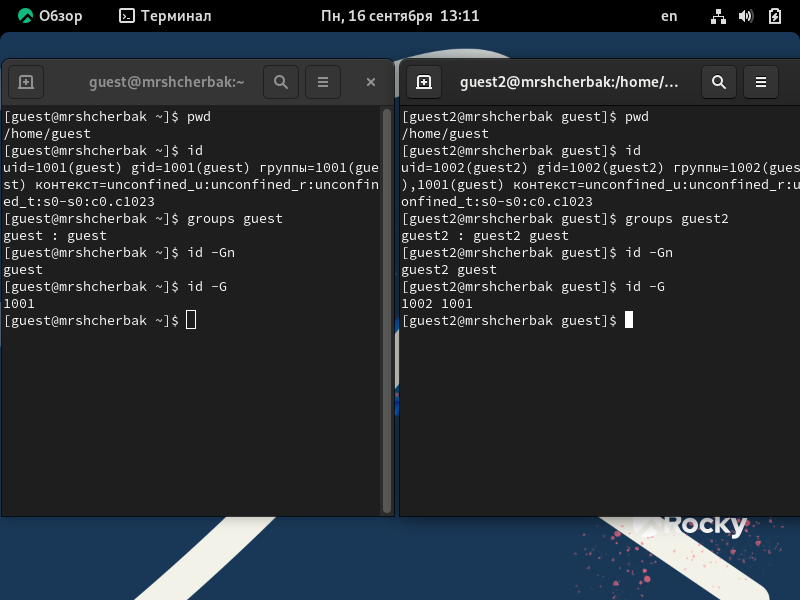
1. Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. Для обоих пользователей командой pwd определим директорию, в которой находимся. Сравним её с приглашениями командной строки (рис.2)



Определение директории

Для guest приглашение совпадает, для guest2 - приглашение guest

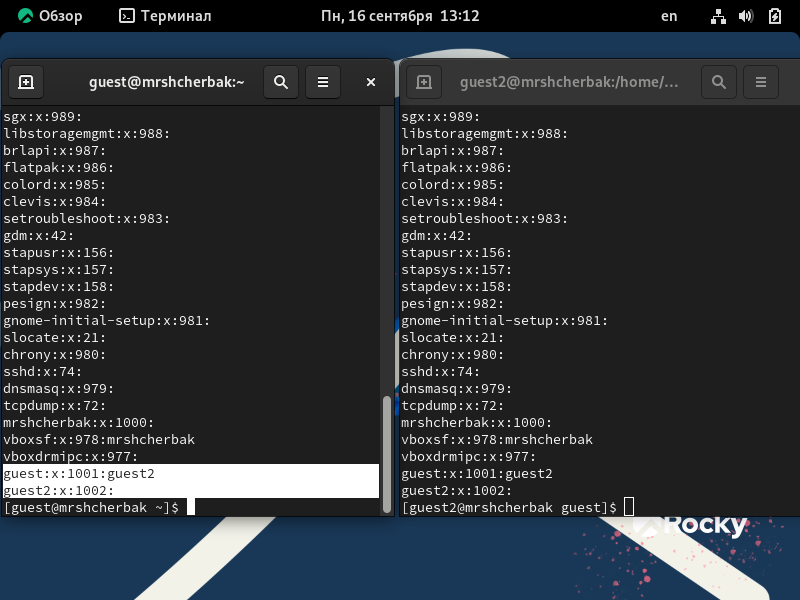
1. Уточним имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определим командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравним вывод команды groups с выводом команд id -Gn и id -G (рис.3).



Выполнение команд

guest выходит в группу guest, guest2 входит в группу guest и guest2. Вывод команды groups совпадает с выводами команд id -Gn и id -G.

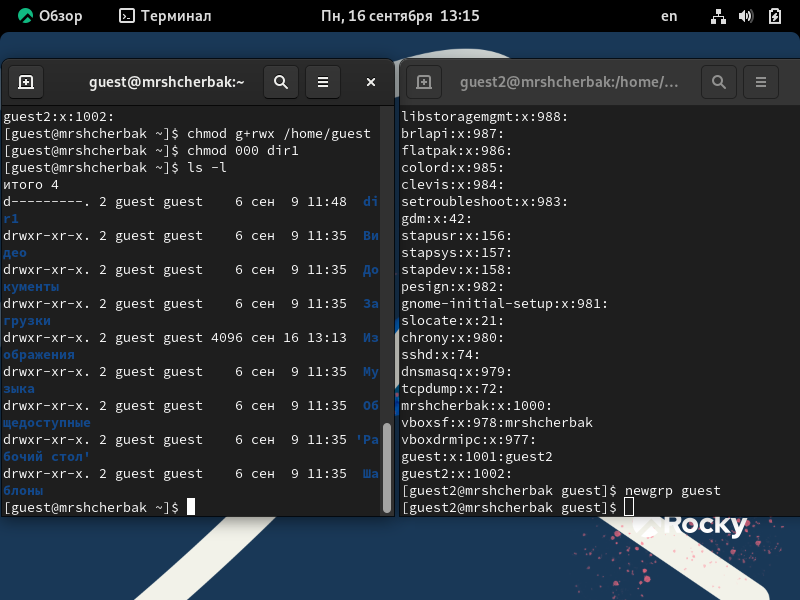
1. Сравним полученную информацию с содержимым файла /etc/group (рис.4).



Содержимое файла /etc/group

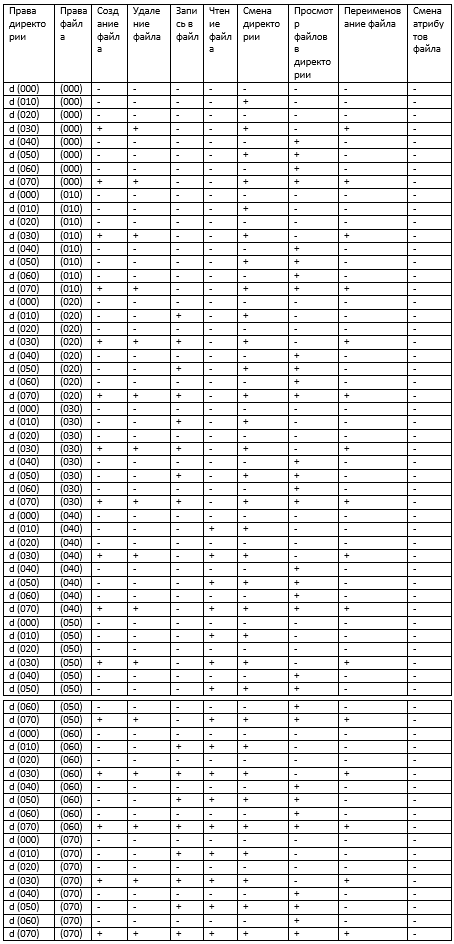
Информация совпадает.

1. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой newgrp guest. От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы. Далее от имени пользователя guest снимем с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl. Проверим правильность снятия атрибутов. Выполненные действия показаны на рис.5.



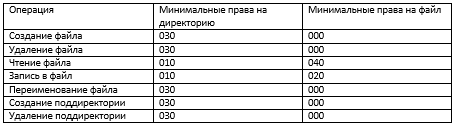
Выполнение команд

1. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполним таблицу, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесём в таблицу знак «+», если не разрешена, знак «-» (рис.6).



Установленные права и разрешённые действия

1. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1 (рис.7).



Минимальные права для совершения операций

# Вывод

Таким образом, в ходе ЛР№3 я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей

# Библиография

1. Методические материалы курса.
2. Chmod. [Электронный ресурс]. М. URL: [Файловая система](https://ru.wikipedia.org/wiki/Chmod) (Дата обращения: 16.09.2022).