Отчет по лабораторной работе 3

Даниил Генералов, 1032212280

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

Мы продолжаем выполнение с того места, где мы остановились в лабораторной работе 2: теперь, чтобы проверить, как работает контроль доступа в Linux с двумя пользователями, надо создать второго пользователя и зайти в систему от его имени. Мы видим, что пользователь guest находится в папке /home/guest, а пользователь guest2 – в папке /home/guest2, но они оба имеют приглашение, которое говорит им, что они находятся в ~ – это сокращение указывает на домашнюю папку текущего пользователя. (рис. 1).

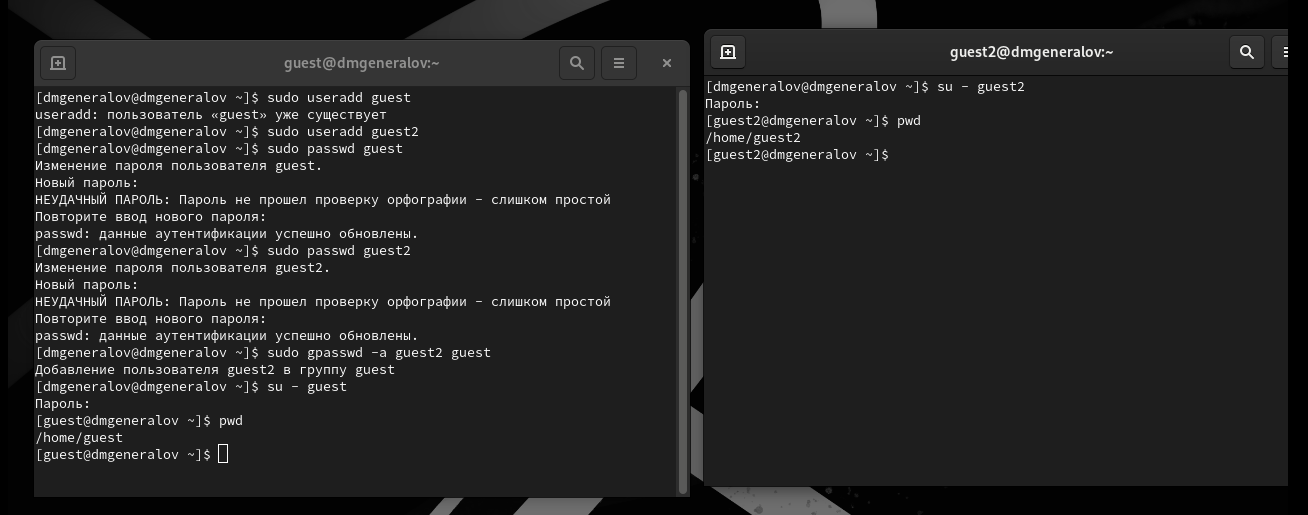


Рис. 1: useradd

Команды groups и id дают нам одинаковую информацию: пользователь guest принадлежит только группе guest (GID=1001), а пользователь guest2 – группе guest2 (GID=1002), а также группе guest. В файле /etc/groups написана только вторая связь, потому что основной GID пользователя хранится в /etc/passwd (рис. 2).

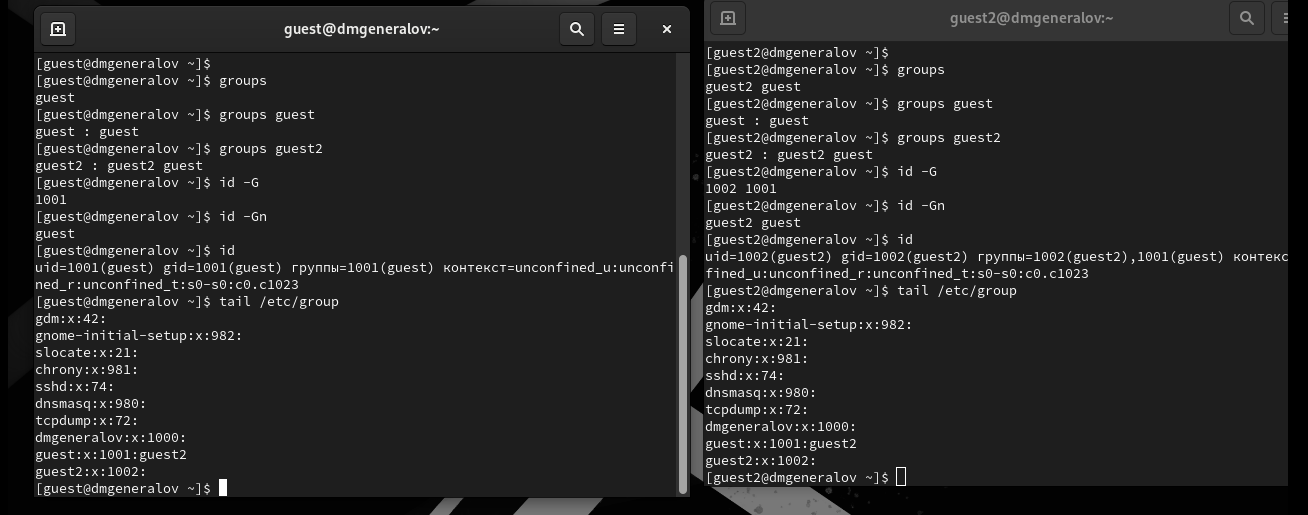


Рис. 2: groups

После этого мы меняем активную группу пользователя guest2 с помощью команды newgrp, а затем запрещаем все операции над папкой /home/guest/dir1. Это можно подтвердить, потому что в выводе ls -l для этой папки стоят все прочерки в битах разрешения (рис. 3).

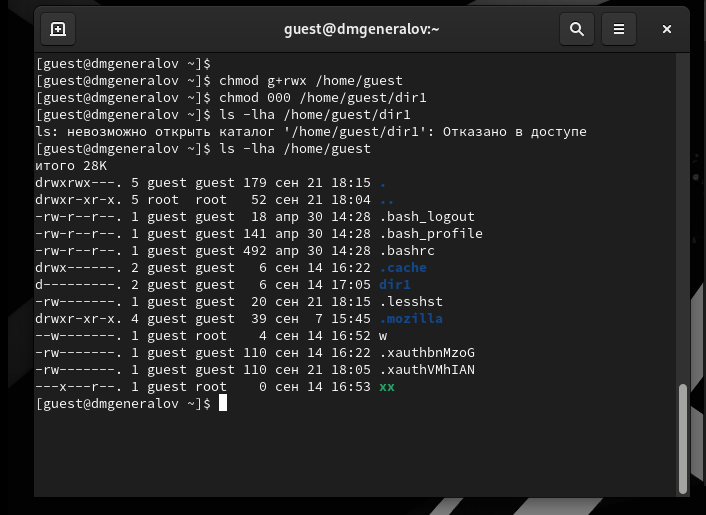


Рис. 3: chmod

На основании этого можно заполнить таблицу разрешений:

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d (000) | (000) | - | - | - | - | - | - | - | - |
| d-x (100) | -x(100) | - | - | - | - | + | - | - | - |
| d-w (200) | -w(200) | + | - | - | - | - | - | - | - |
| d-wx (300) | -wx(300) | + | + | + | - | + | - | + | + |
| dr (400) | r(400) | - | - | - | + | - | - | - | - |
| dr-x (500) | r-x(500) | - | - | - | + | + | + | - | - |
| drw (600) | rw(600) | - | - | + | + | - | - | - | - |
| drwx (700) | rwx(700) | + | + | + | + | + | + | + | + |

На основании этого можно вывести таблицу минимальных прав, которые необходимы для каждой операции:

| Операция | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | -wx | ??? |
| Удаление файла | -wx | — |
| Чтение файла | –x | r– |
| Запись в файл | –x | -w- |
| Переименование файла | -wx | — |
| Создание поддиректории | -wx | ??? |
| Удаление поддиректории | -wx | — |

# 3 Выводы

Мы изучили, как использовать базовый дискреционный контроль доступа в Linux, и определили, какие аттрибуты позволяют выполнять какие действия над папками или файлами. Мы также проверили, что эти свойства сохраняются при ситуации с несколькими пользователями.