# Лабораторная работа № 2

**Дискреционное разграничение прав в Linux. Основные атрибуты**

Беличева Дарья Михайловна

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 2 Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ, discretion — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей [1].

Основная команда для работы с правами в Linux: `chmod`. Есть три основных вида прав:

- r – чтение;
- w – запись;
- x – выполнение;
- s – выполнение от имени суперпользователя (дополнительный);

Также есть три категории пользователей, для которых вы можете установить эти права на файл linux:

- u – владелец файла;
- g – группа файла;

- o – все остальные пользователи.

# 3 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора) с помощью команды `useradd guest`. Зададим пароль для пользователя guest командой `passwd guest` (рис. 3.1).

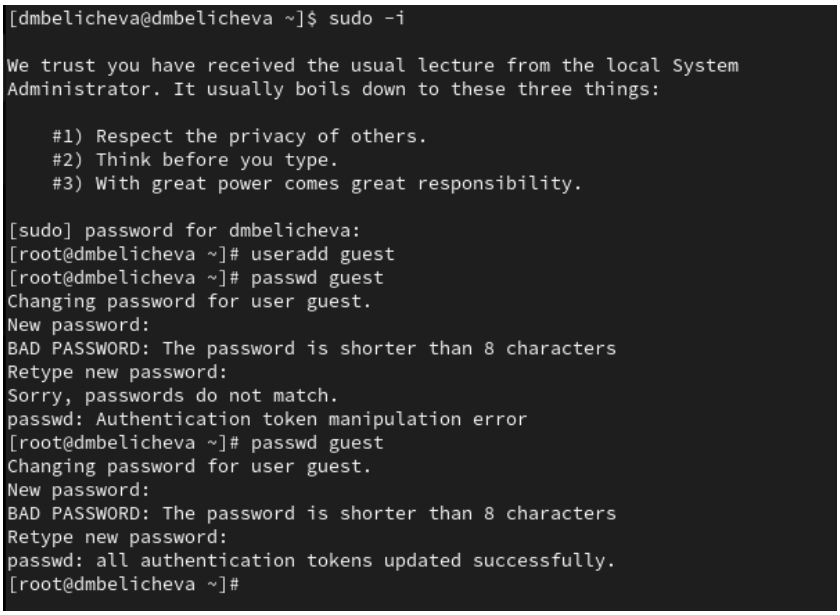


Рис. 3.1: Создание учетной записи пользователя guest и задание пароля

Войдем в систему от имени пользователя guest (рис. 3.2, 3.3).

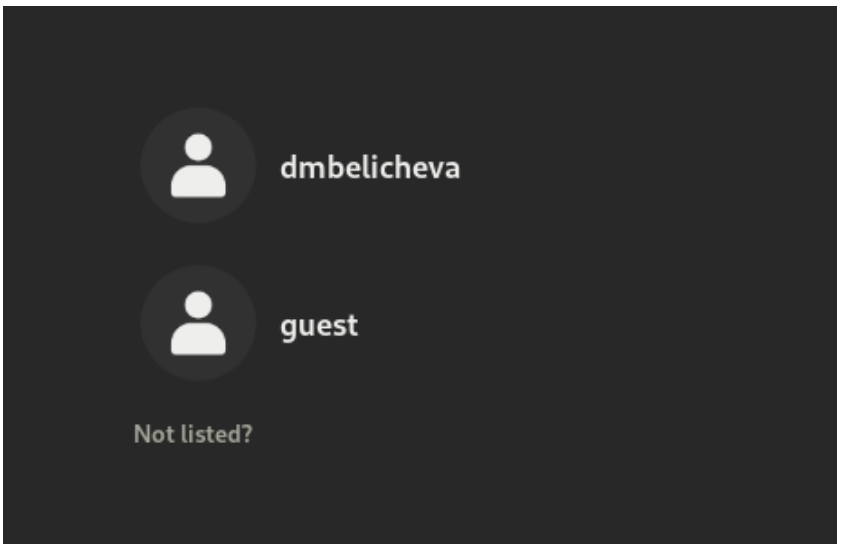


Рис. 3.2: Вход в систему от имени пользователя guest

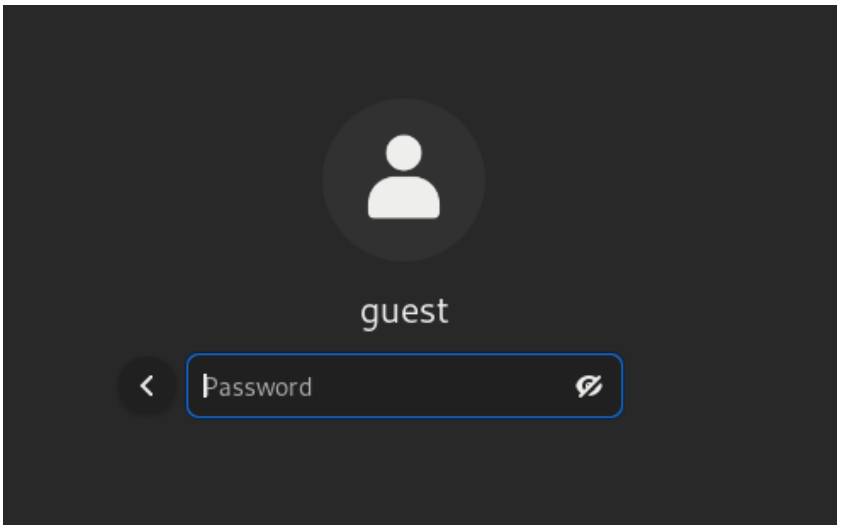


Рис. 3.3: Ввод пароля для пользователя guest

Определим директорию, в которой находимся, командой `pwd`. Мы находимся в директории /home/guest. Сравнив её с приглашением командной строки, увидим что они идентичны (guest). Также с помощью команды `cd ~` определим, что директория, в которой мы находимся, является домашней директорией. Уточним имя пользователя командой whoami, увидим имя guest. Уточним имя пользовате-

ля, его группу, а также группы, куда входит пользователь, командой `id` (рис. 3.4). Увидим, что имя пользователя guest, его uid - 1001, группа также называется guest, ее gid - 1001. Сравним вывод `id` с выводом команды `groups`, вывод идентичен.


Рис. 3.4: Определение директории, имени пользователя, группы и их идентификаторов

Просмотрим файл /etc/passwd командой `cat /etc/passwd` (рис. 3.5). Найдем в нём свою учётную запись, определим uid пользователя и gid пользователя. Используем программу `grep` в качестве фильтра. Сравнив найденные значения с полученными в предыдущих пунктах, увидим, что они одинаковы.


Рис. 3.5: Просмотр файла /etc/passwd

Определим существующие в системе директории командой `ls -l /home/` (рис. 3.6). Нам удалось получить список поддиректорий /home, а именно там находится две директории dmbelicheva и guest. У этих поддиректорий есть все права (rwx) для пользователя, для групп и других прав нет.

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой `lsattr /home`. Нам удалось увидеть расширенные атрибуты директории guest (их нет), но доступа к директории dmbelicheva у нас нет.

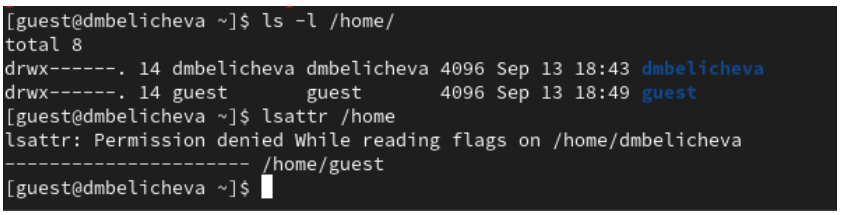


Рис. 3.6: Существующие в системе директории, их права и расширенные атрибуты

Создадим в домашней директории поддиректорию dir1 командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис. 3.7). На директорию dir1 по умолчанию были выставлены права drxwr-xr-x, то есть для пользователя у нас доступны все права, для групп и других только чтение и выполнение.

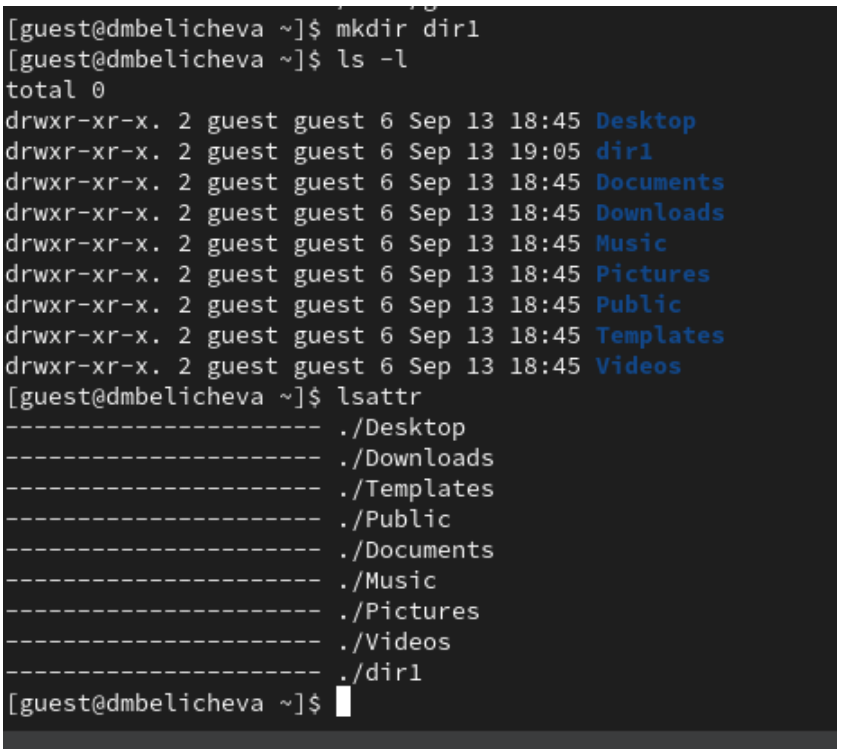


Рис. 3.7: Создание директории dir1 и определение ее прав

Теперь снимем с директории dir1 все атрибуты командой `chmod 000 dir1` и

проверим правильность выполнения с помощью команды `ls -l` (рис. 3.8). Действительно, увидим, что у директории dir1 теперь права d———, то есть нет прав.

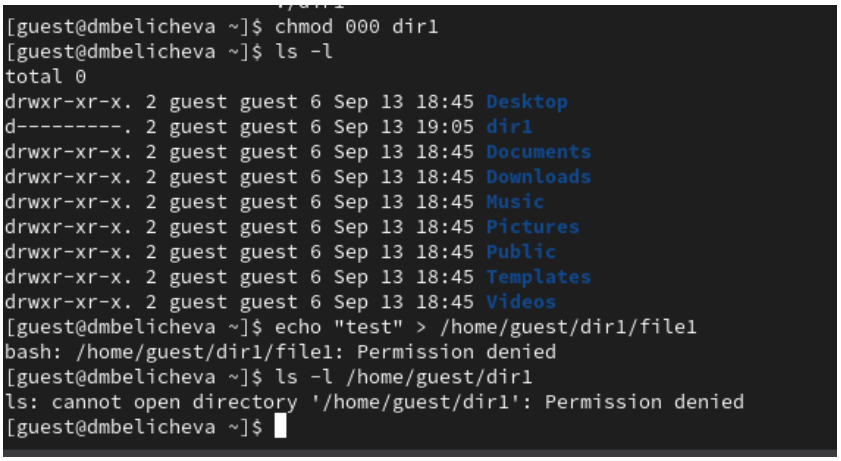


Рис. 3.8: Лишение всех прав директории dir1

При попытке создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1` мы получим отказ, так как у этой директории нет никаких прав, соответственно создавать в ней файлы мы не можем (рис. 3.9). Оценить, как сообщение об ошибке отразилось на создании файла командой `ls -l /home/guest/dir1`, так как мы не можем перейти в эту директории, нам отказано в доступе.


Рис. 3.9: Попытка создание файла в директории dir1

В табл. [3.1] приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Для заполнения таблицы, нам предлагалось опытным путем проверить, какие права позволяют выполнять те или иные действие (рис. 3.10).

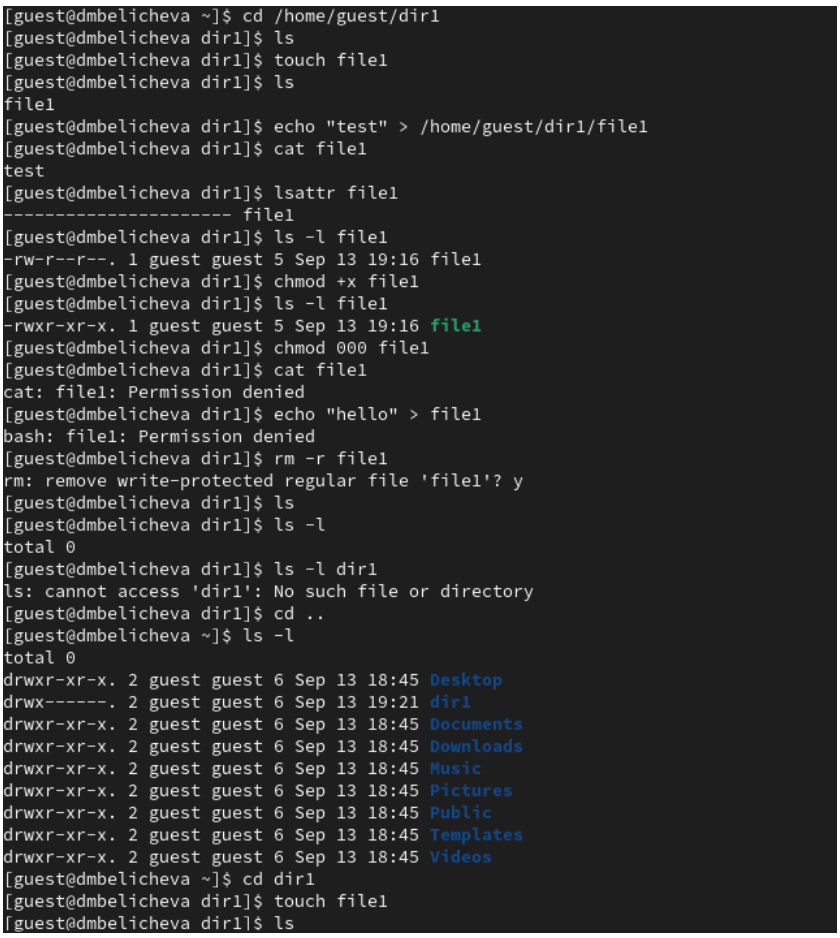


Рис. 3.10: Определения разрешенных действий с различными правами

Таблица 3.1: Установленные права и разрешённые действия

| 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(100) | (000) | - | - | - | + | + | - | - | + |
| d(200) | (000) | - | - | - | - | - | - | - | - |
| d(300) | (000) | + | + | - | - | + | - | + | + |
| d(500) | (000) | - | - | - | - | + | + | - | + |
| d(400) | (000) | - | - | - | - | - | + | - | - |
| d(600) | (000) | - | - | - | - | - | + | - | - |
| d(700) | (000) | + | + | - | + | + | + | + | + |
| d(000) | (100) | - | - | - | - | - | - | - | - |
| d(100) | (100) | - | - | - | - | + | - | - | + |
| d(200) | (100) | - | - | - | - | - | - | - | - |
| d(300) | (100) | + | + | - | - | + | - | + | + |
| d(400) | (100) | - | - | - | - | - | + | - | - |
| d(500) | (100) | - | - | - | - | + | + | - | + |
| d(600) | (100) | - | - | - | - | - | + | - | - |
| d(700) | (100) | + | + | - | - | + | + | + | + |
| d(000) | (200) | - | - | - | - | - | - | - | - |
| d(100) | (200) | - | - | + | - | + | - | - | + |
| d(200) | (200) | - | - | - | - | - | - | - | - |

| 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(300) | (200) | + | + | + | - | + | - | + | + |
| d(400) | (200) | - | - | - | - | - | + | - | - |
| d(500) | (200) | - | - | + | - | + | + | - | + |
| d(600) | (200) | - | - | - | - | - | + | - | - |
| d(700) | (200) | + | + | + | - | + | + | + | + |
| d(000) | (300) | - | - | - | - | - | - | - | - |
| d(100) | (300) | - | - | + | - | + | - | - | + |
| d(200) | (300) | - | - | - | - | - | - | - | - |
| d(300) | (300) | + | + | + | - | + | - | + | + |
| d(400) | (300) | - | - | - | - | - | + | - | - |
| d(500) | (300) | - | - | + | - | + | + | - | + |
| d(600) | (300) | - | - | - | - | - | + | - | - |
| d(700) | (300) | + | + | + | - | + | + | + | + |
| d(000) | (400) | - | - | - | - | - | - | - | - |
| d(100) | (400) | - | - | - | + | + | - | - | + |
| d(200) | (400) | - | - | - | - | - | - | - | - |
| d(300) | (400) | + | + | - | + | + | - | + | + |
| d(400) | (400) | - | - | - | - | - | + | - | - |
| d(500) | (400) | - | - | - | + | + | + | - | + |
| d(600) | (400) | - | - | - | - | - | + | - | - |
| d(700) | (400) | + | + | - | + | + | + | + | + |

| 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) | (500) | - | - | - | - | - | - | - | - |
| d(100) | (500) | - | - | - | + | + | - | - | + |
| d(200) | (500) | - | - | - | - | - | - | - | - |
| d(300) | (500) | + | + | - | + | + | - | + | + |
| d(400) | (500) | - | - | - | - | - | + | - | - |
| d(500) | (500) | - | - | - | + | + | + | - | + |
| d(600) | (500) | - | - | - | - | - | + | - | - |
| d(700) | (500) | + | + | - | + | + | + | + | + |
| d(000) | (600) | - | - | - | - | - | - | - | - |
| d(100) | (600) | - | - | + | + | + | - | - | + |
| d(200) | (600) | - | - | - | - | - | - | - | - |
| d(300) | (600) | + | + | + | + | + | - | + | + |
| d(400) | (600) | - | - | - | - | - | + | - | - |
| d(500) | (600) | - | - | + | + | + | + | - | + |
| d(600) | (600) | - | - | - | - | - | + | - | - |
| d(700) | (600) | + | + | + | + | + | + | + | + |
| d(000) | (700) | - | - | - | - | - | - | - | - |
| d(100) | (700) | - | - | + | + | + | - | - | + |
| d(200) | (700) | - | - | - | - | - | - | - | - |
| d(300) | (700) | + | + | + | + | + | - | + | + |
| d(400) | (700) | - | - | - | - | - | + | - | - |

| 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(500) | (700) | - | - | + | + | + | + | - | + |
| d(600) | (700) | - | - | - | - | - | + | - | - |
| d(700) | (700) | + | + | + | + | + | + | + | + |

В табл. [3.2] приведены данные о том, какие минимальные права должны быть для совершения различных действий.

Таблица 3.2: Минимальные права для совершения операций

| Операция | Минимальные права на директорию | Минимальные права на файл |
|---|---|---|
| Создание файла | d(300) | (000) |
| Удаление файла | d(300) | (000) |
| Чтение файла | d(100) | (400) |
| Запись в файл | d(100) | (200) |
| Переименование файла | d(300) | (000) |
| Создание поддиректории | d(300) | (000) |
| Удаление поддиректории | d(300) | (000) |

# 4 Выводы

В процессе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# Список литературы

1. Дискреционное разграничение доступа Linux [Электронный ресурс]. 2023. URL: https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/.