ЛР №2. Дискреционное разграничение прав в Linux. Основные атрибуты

Информационная безопасность

Доборщук Владимир Владимирович

НФИбд-01-18

2 октября 2021

Содержание

# 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.

**Задачи:**

* анализ атрибутов директорий/файлов;
* укрепление навыков манипуляции учетными записями;
* укрепление навков взаимодействия с файловой системой.

# Теоретическое введение

Для выполнения данной лабораторной работы мы использовали данные источники, в виде описания лабораторной работы, а также свободные источники в интернете.

# Выполнение лабораторной работы

## 1. Взаимодействие с пользователем

Зайдя в терминал, мы сделали следующие вещи:

* создали учетную запись для guest;
* задали пароль для guest;
* вошли в систему от лица guest;
* определили домашнюю директорию для текущего пользователя;
* уточнили имя текущего пользователя.

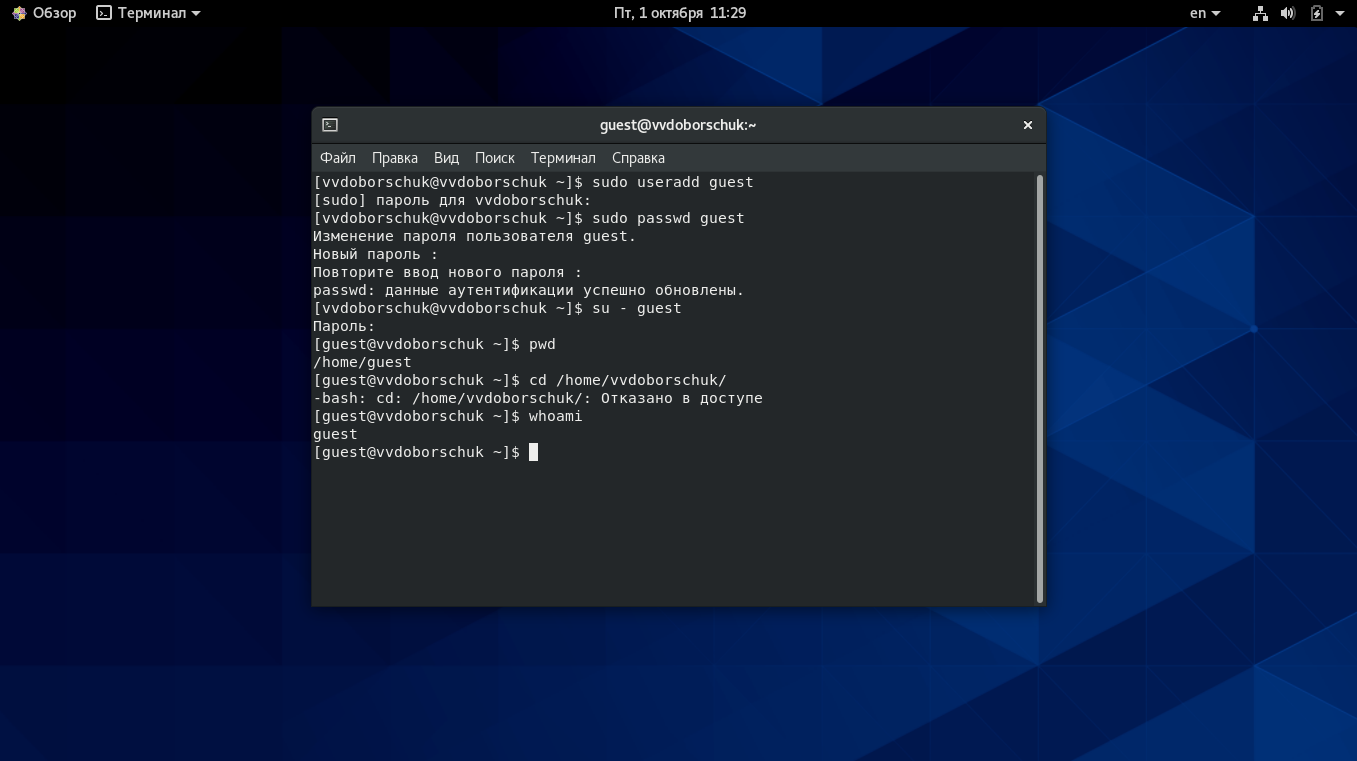


Figure : Взаимодействие с учетной записью нового пользователя

Далее, с помощью команды id мы уточнили имя пользователя, его группу и группы, куда он входит. Также использовали команду groups, благодаря которой мы получаем также группы, в которые входит наш текущий пользователь (что также описано командой id).

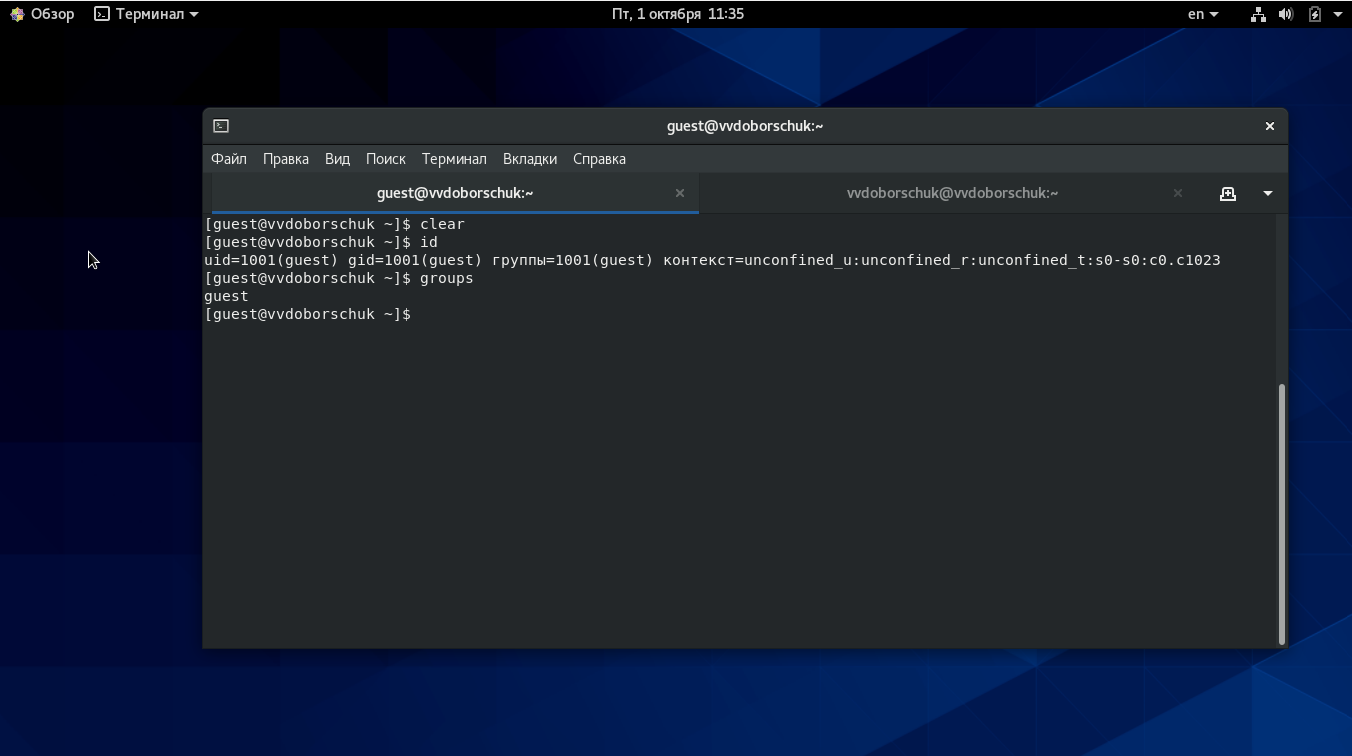


Figure : Информация о пользователе guest

Сравнивая это с данными изначального пользователя, видим основные различия в имени и основной группе пользователей, а также “дефолтный” пользователь входит в группу wheel, в отличие от пользователя guest.

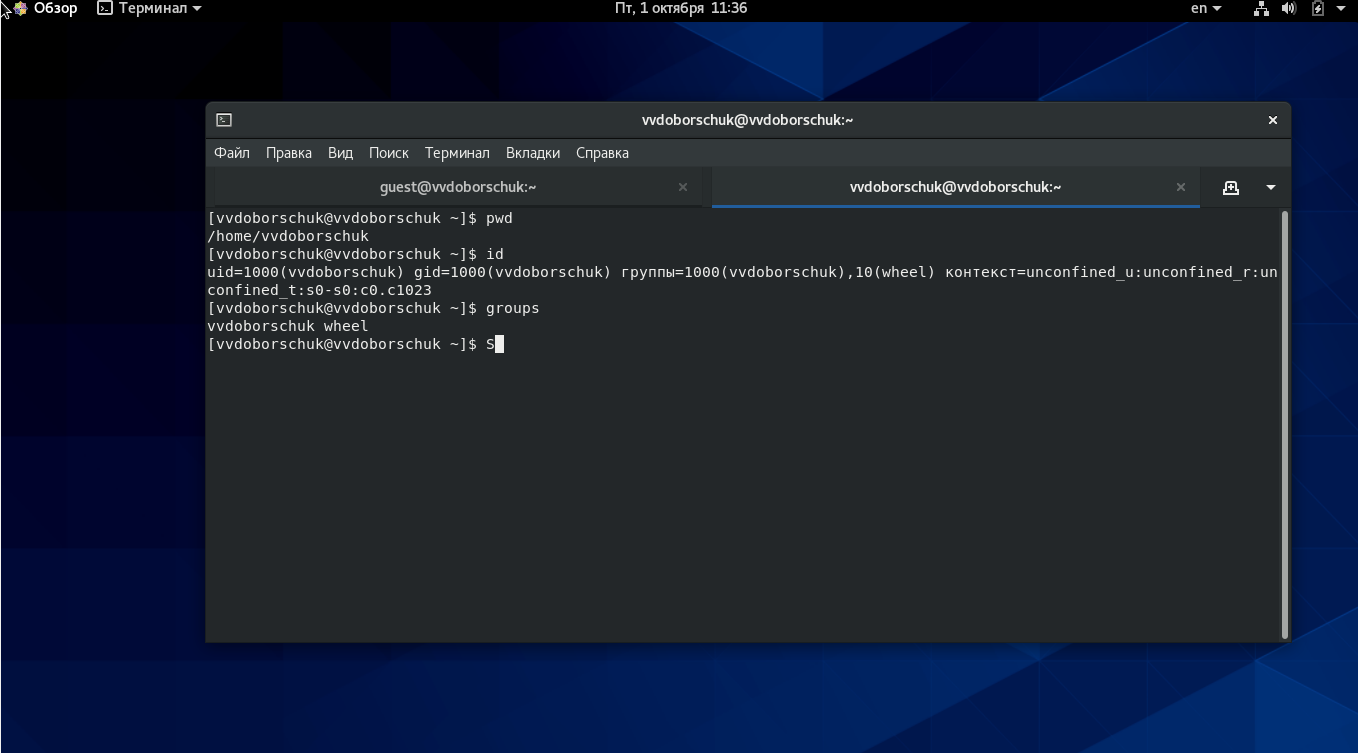


Figure : Информация о пользователе vvdoborschuk

С помощью команды cat /etc/passwd и фильтра grep получили также часть данных о наших пользователях в системе.

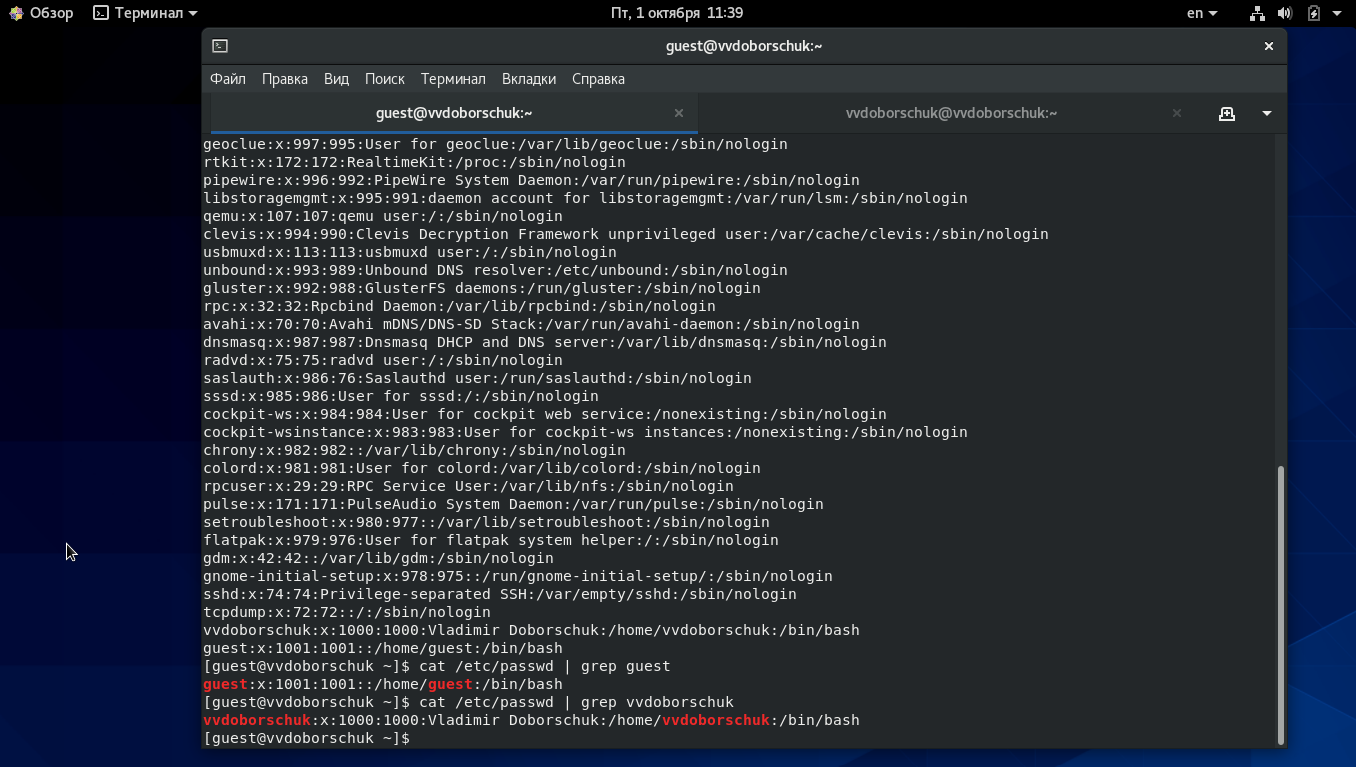


Figure : Файл /etc/passwd

## 2. Работа с атрибутами

Мы попытались определить, какие директории существуют в каталоге /home.

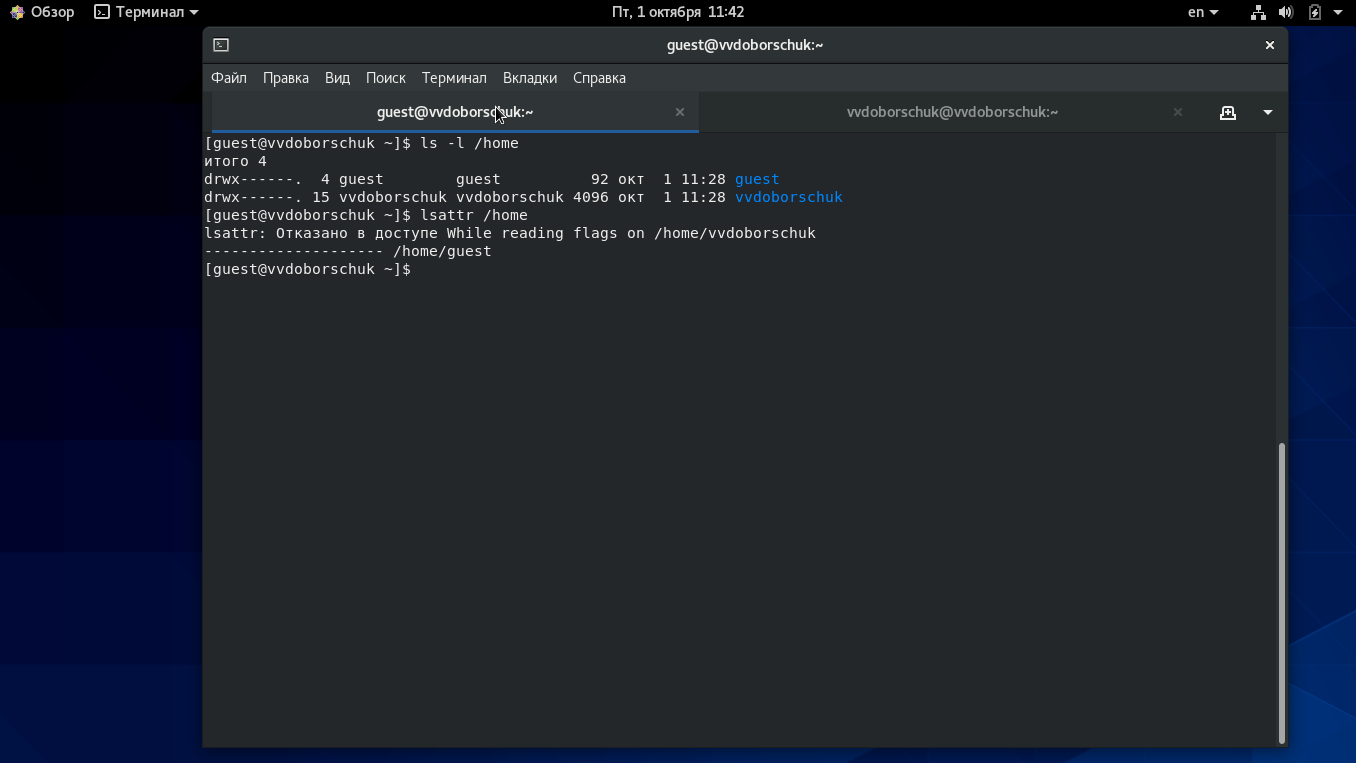


Figure : Вывод информации от guest

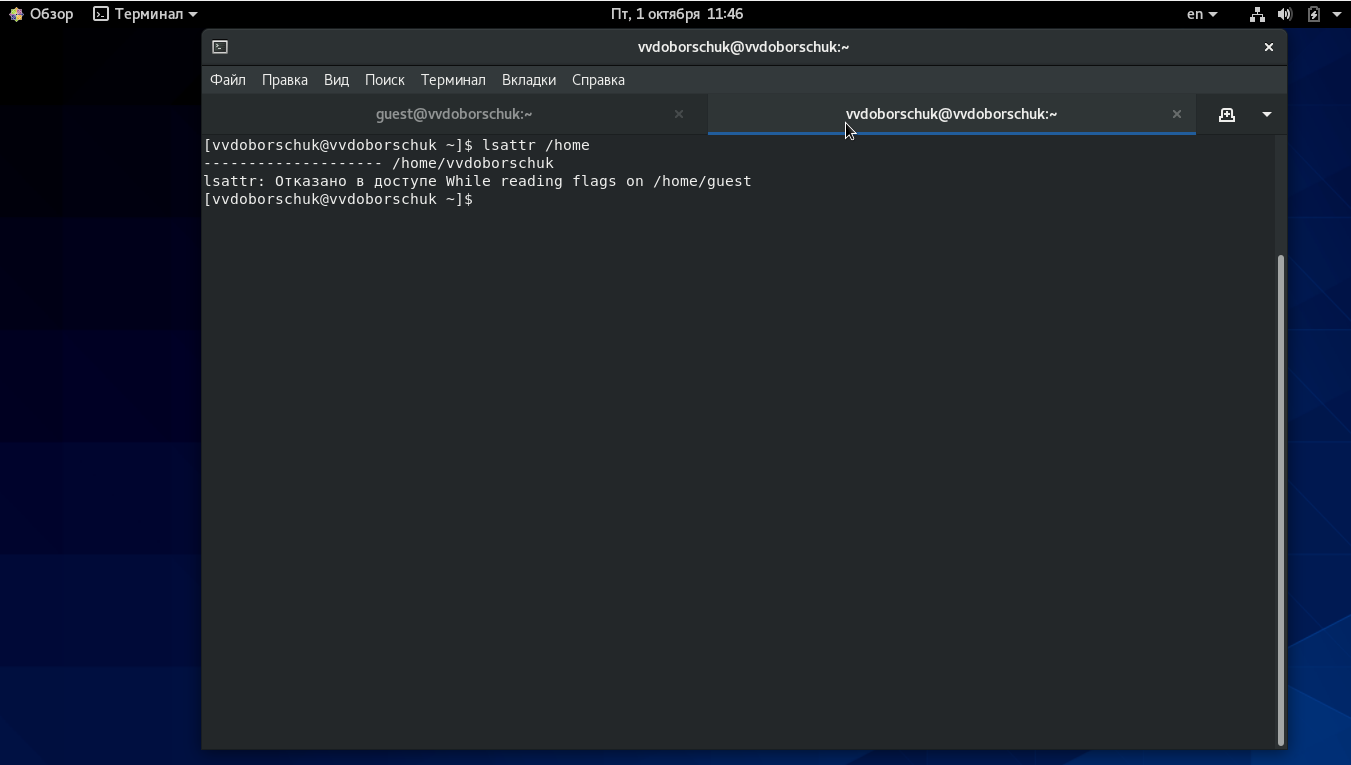


Figure : Вывод информации от vvdoborschuk

Видно, что мы смогли получить список каталогов от любого из данных нам пользователей, но нам недоступны расширенные атрибуты других пользователей.

Выполнили пункты 11-13, параллельно приступив к заполнению нашей таблицы.

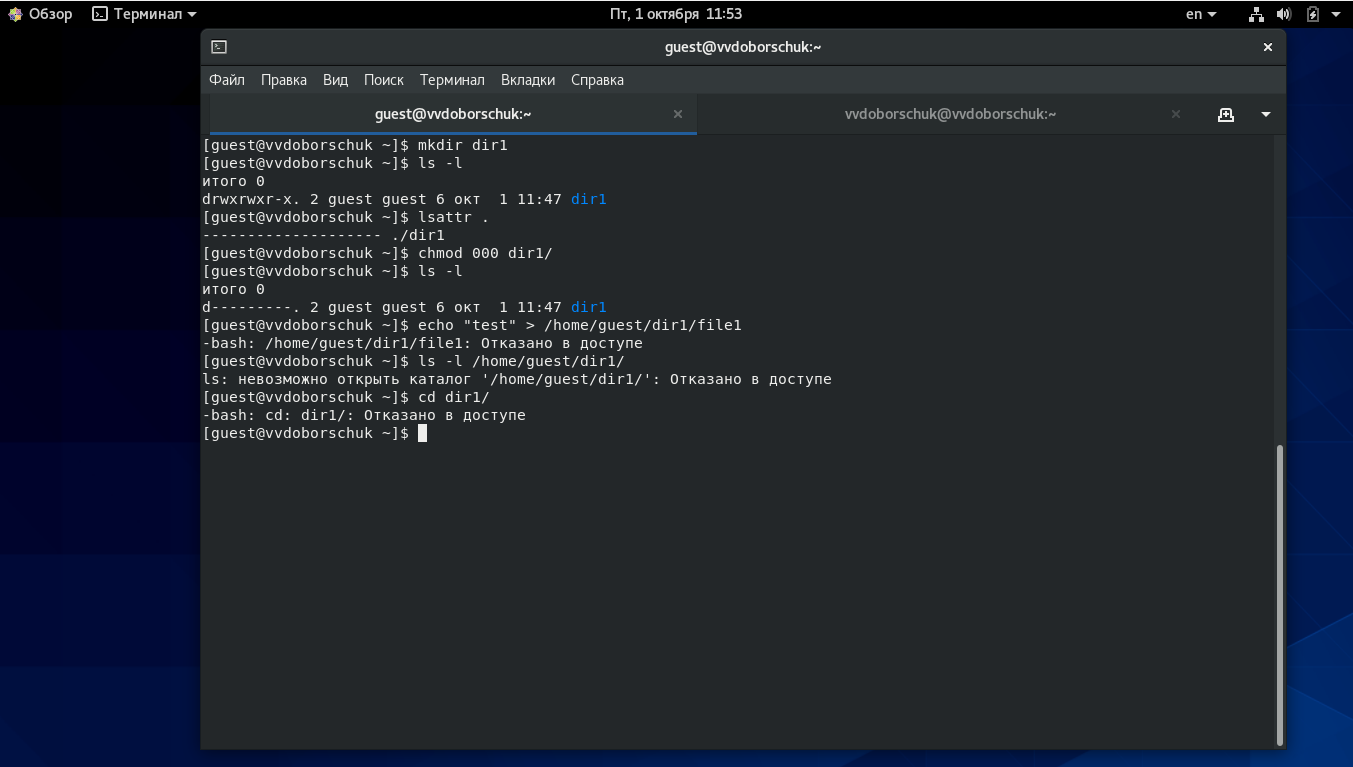


Figure : Работа с директориями и файлами

Мы не смогли записать файл /home/guest/dir1/file1, т.к. права на директорию dir1 эквивалентны (000), что означает запрет на чтение, запись и исполняемость внутри директории. Также, файл не создался внутри директории, как показал проверка.

Перед заполнением таблицы, мы экспериментально проверили все возможные варианты атрибутов для индивидуального пользователя.

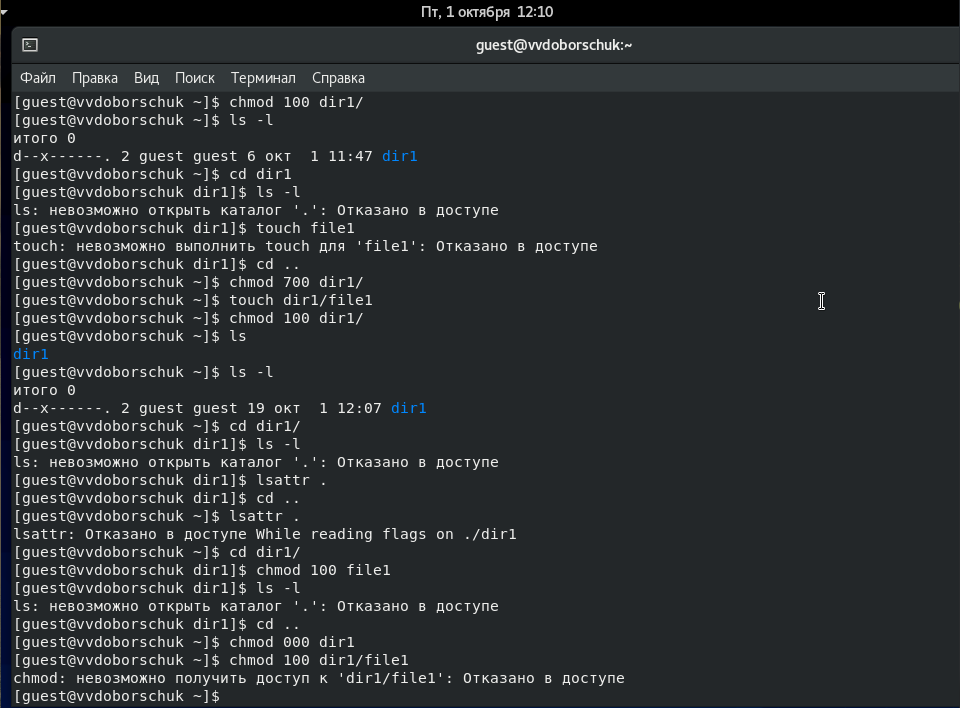


Figure : Атрибуты 100

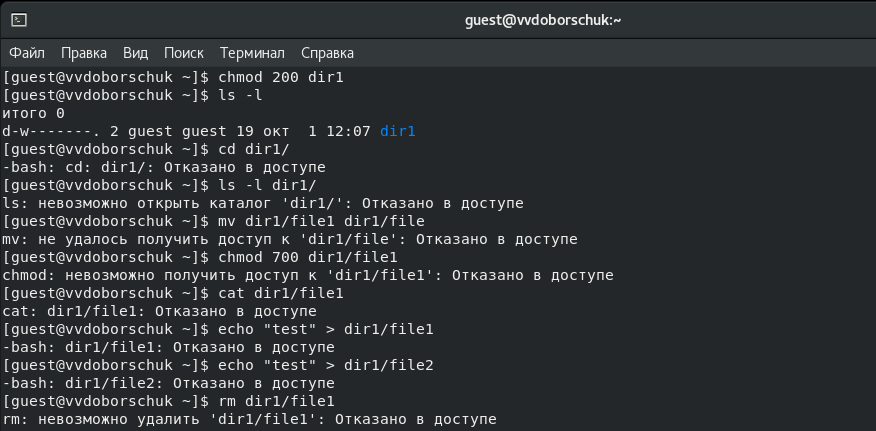


Figure : Атрибуты 200

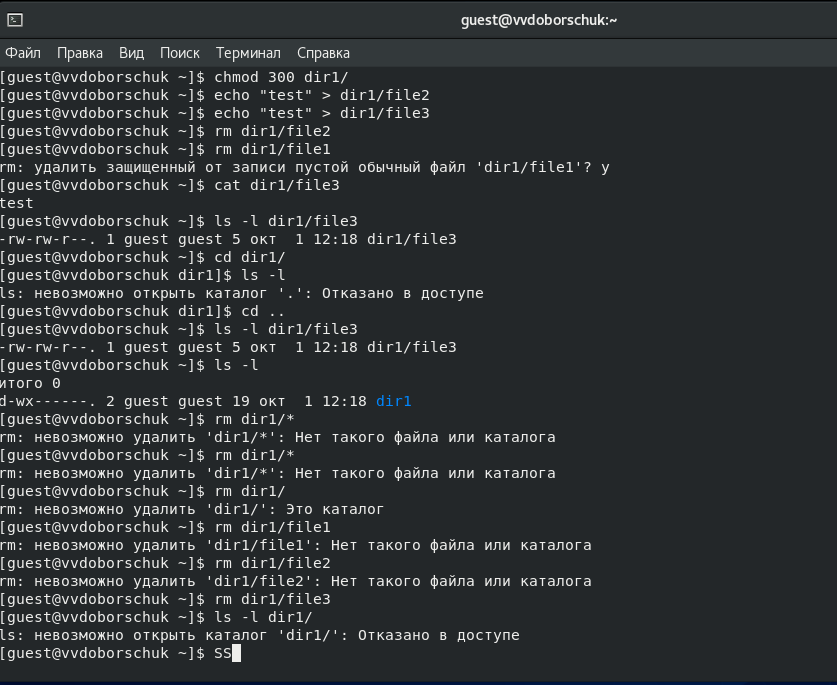


Figure : Атрибуты 300. Часть 1

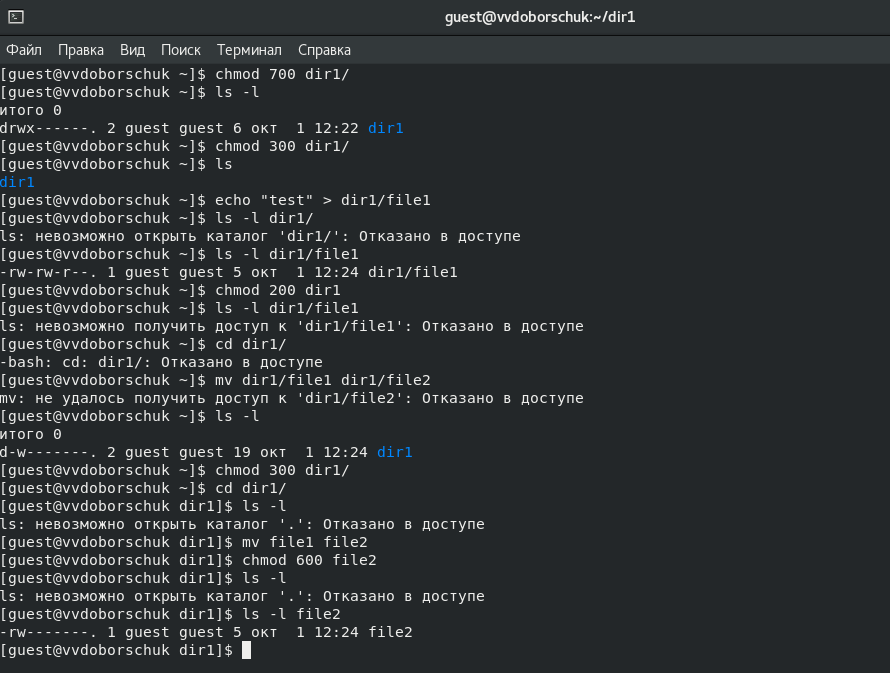


Figure : Атрибуты 300. Часть 2

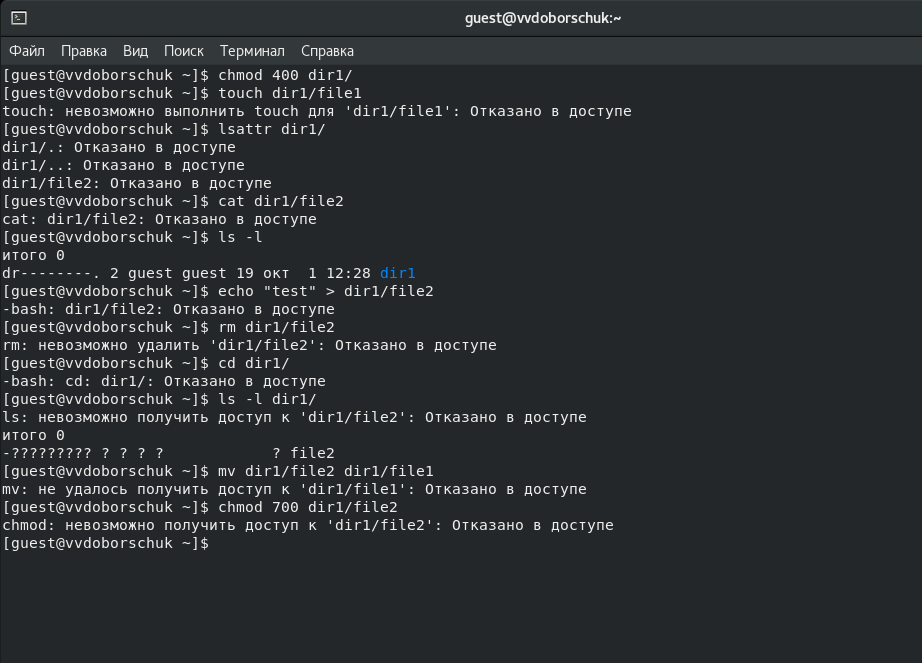


Figure : Атрибуты 400

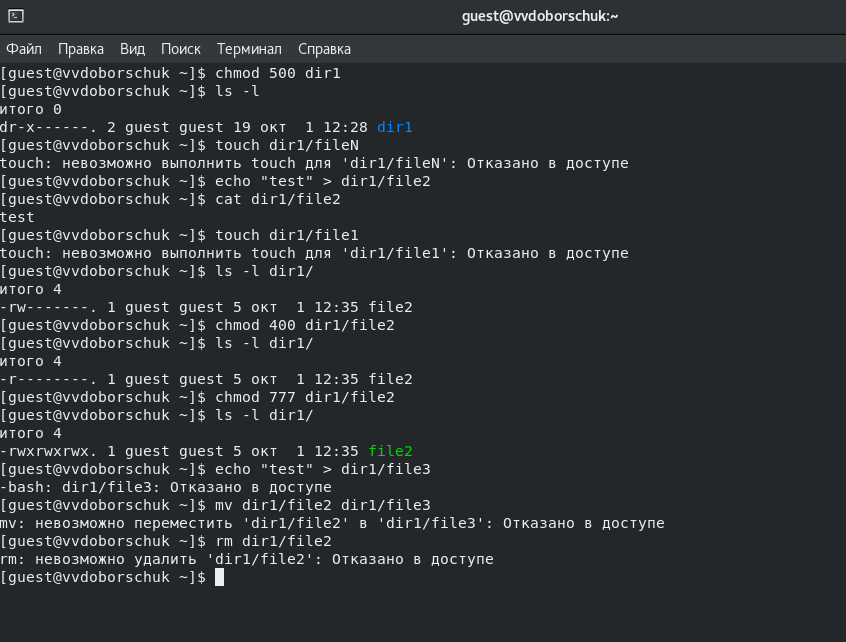


Figure : Атрибуты 500

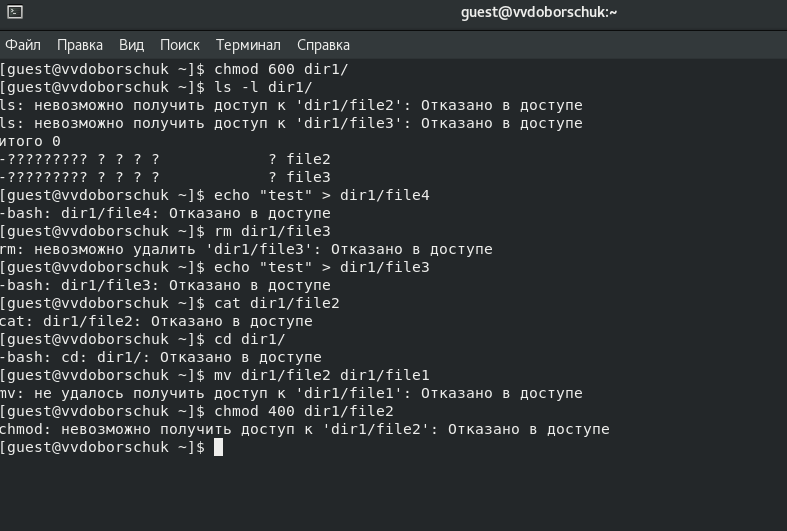


Figure : Атрибуты 600

Для случая с правами (700) все достаточно очевидно, поэтому его мы не стали индивидуально рассматривать.

**Таблица 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--x------ (100) | ---------- (000) | - | - | - | - | + | - | - | + |
| d-w------- (200) | ---------- (000) | - | - | - | - | - | - | - | - |
| d-wx------ (300) | -rwx------ (700) | + | + | + | + | + | - | + | + |
| dr-------- (400) | ---------- (000) | - | - | - | - | - | + | - | - |
| dr-x------ (500) | -rwx------ (700) | - | - | + | + | + | + | - | + |
| drw------- (600) | ---------- (000) | - | - | - | - | - | + | - | - |
| drwx------ (700) | -rwx------ (000) | + | + | + | + | + | + | + | + |

**Таблица 2. Минимальные права для совершения операция**

| Операции | Минимальные права на директорию | Минимальные права на файл |
| --- | --- | --- |
| Создание файла | d-wx------ (300) | --wx------ (300) |
| Удаление файла | d-wx------ (300) | ---x------ (100) |
| Чтение файла | d-wx------ (300) | -r-------- (400) |
| Запись в файл | d-wx------ (300) | -rw------- (500) |
| Переименование файла | d-wx------ (300) | -rw------- (500) |
| Создание поддиректории | drwx------ (700) | ---x------ (100) |
| Удаление поддиректории | drwx------ (700) | ---x------ (100) |

# Заключение

Мы получили практические навыки работы в консоли с атрибутами файлов, закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.