Отчет по лабораторной работе №2

Информационная безопасность

Чекалова Лилия Руслановна

Содержание

# 1 Цель работы

* Приобретение 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 Задание

* Создание новой учетной записи
* Просмотр сведений об учетной записи
* Изменение прав доступа к директориям и файлам
* Проверка возможных в рамках заданных прав доступа действий
* Заполнение таблиц

# 3 Теоретическое введение

Файлы и директории имеют три вида прав доступа:

* Чтение — разрешает получать содержимое файла, но не изменять. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;
* Запись — разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;
* Выполнение — разрешает выполнять файл как программу и переходить в директорию.

Каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

* Владелец — набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права.
* Группа — любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу. Остальные — пользователи, не входящие в предыдущие категории.

Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является или к тем, доступ к которым ему разрешен. Только пользователь Root может работать со всеми файлами независимо от их набора их полномочий.

Более подробно о см. в [1,2].

# 4 Выполнение лабораторной работы

В качестве первого шага лабораторной работы мы перешли в режим sudo, дающий нам больше прав, и создали учетную запись guest с помощью команды useradd (рис. [1](#fig:001)).

Figure 1: Создание новой учетной записи

Figure 1: Создание новой учетной записи

Далее мы задали пароль для этой учетной записи (рис. [2](#fig:002)).

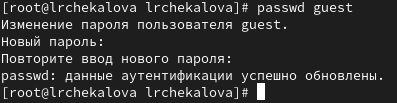


Figure 2: Задание пароля

После этого мы вошли в систему от имени только что созданного пользователя (рис. [3](#fig:003)).

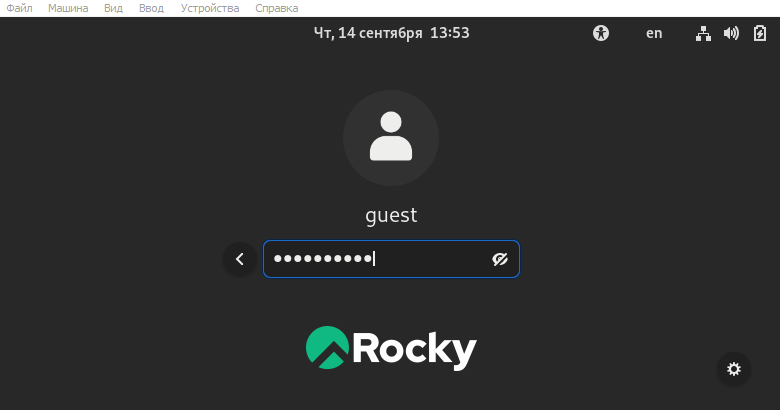


Figure 3: Вход в систему

Мы определили директорию, в которой находимся, с помощью команды pwd, узнали информацию об имени пользователя командой whoami, уточнили с помощью команды id информацию об имени и группах пользователя и сравнили вывод с выводом команды groups (рис. [4](#fig:004)). Результаты команд не противоречат друг другу.

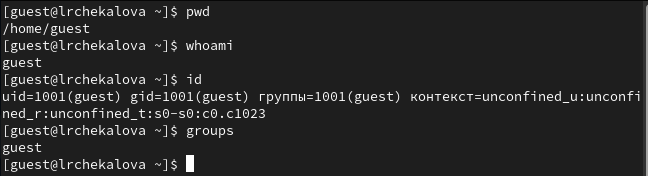


Figure 4: Получение дополнительных сведений о пользователе

Просмотрели содержимое etc/passwd и нашли информацию о нашем пользователе командой grep (рис. [5](#fig:005)). Данные соответствуют полученным ранее.

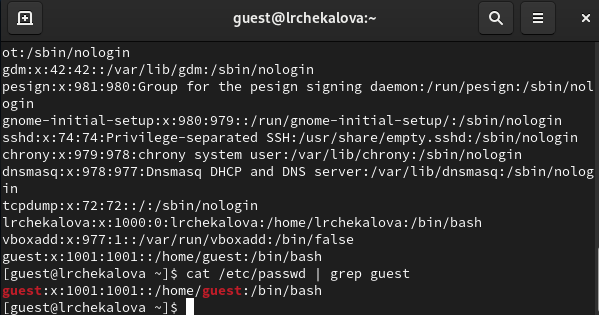


Figure 5: Просмотр файла etc/passwd

Определили список существующих директорий с помощью команды ls -l и попытались получить информацию о расширенных атрибутах поддиректорий /home с помощью команды lsattr (рис. [6](#fig:006)). Доступ к поддиректории, относящейся к другой учетной записи, получить не удалось.

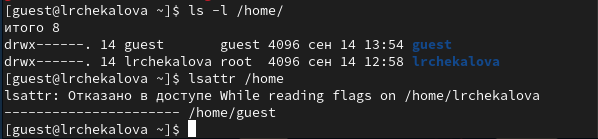


Figure 6: Просмотр прав доступа и расширенных атрибутов

Далее создали папку dir1 и посмотрели права доступа (рис. [7](#fig:007)) и расширенные атрибуты (рис. [8](#fig:008)), установленные на эту папку.

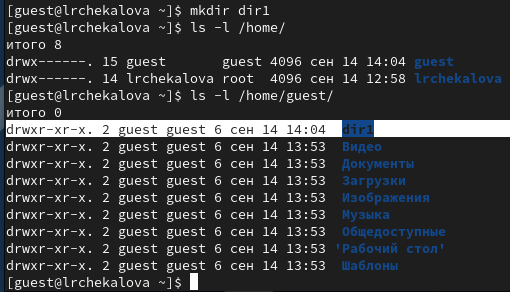


Figure 7: Просмотр прав доступа dir1

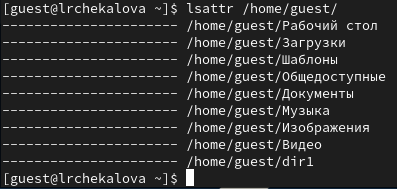


Figure 8: Просмотр расширенных атрибутов dir1

Сняли с директории все атрибуты командой chmod (рис. [9](#fig:009)).

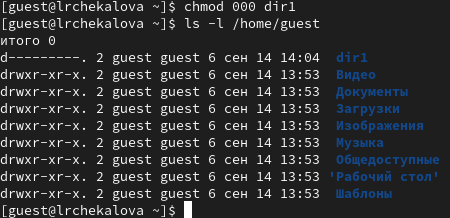


Figure 9: Снятие атрибутов с dir1

Попытались создать в этой директории файл, но нам было отказано в доступе (рис. [10](#fig:010)).

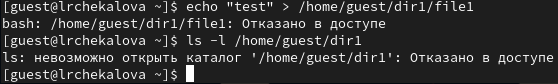


Figure 10: Попытка создания файла

Комбинируя разные права доступа к директории и к файлу, проверили, какие действия доступны для разных прав доступа (рис. [11](#fig:011)-[12](#fig:012)).

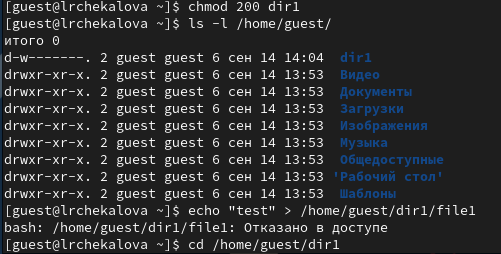


Figure 11: Изменение прав доступа и проверка доступных действий, 1

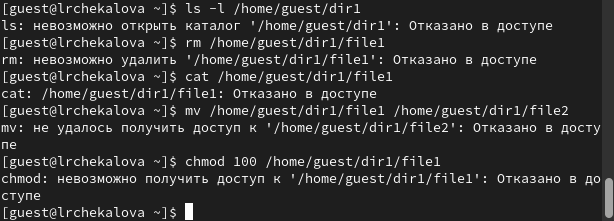


Figure 12: Изменение прав доступа и проверка доступных действий, 2

Заполнили таблицу полученной информацией (рис. [13](#fig:013), [14](#fig:014), [15](#fig:015)).

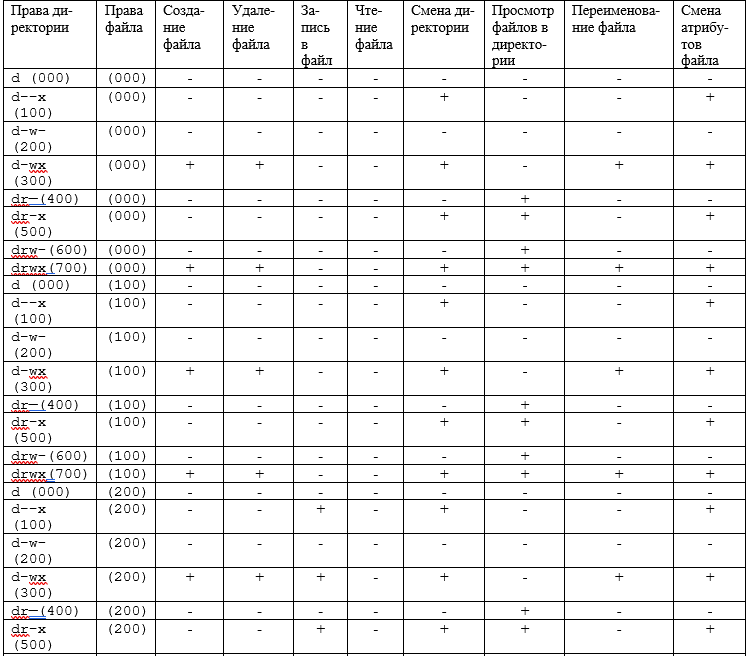


Figure 13: Установленные права и разрешенные действия, 1

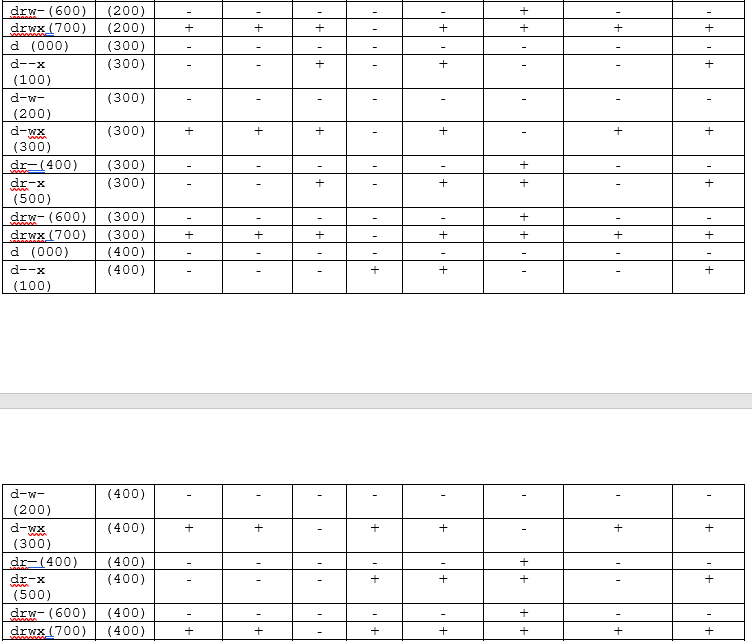


Figure 14: Установленные права и разрешенные действия, 2

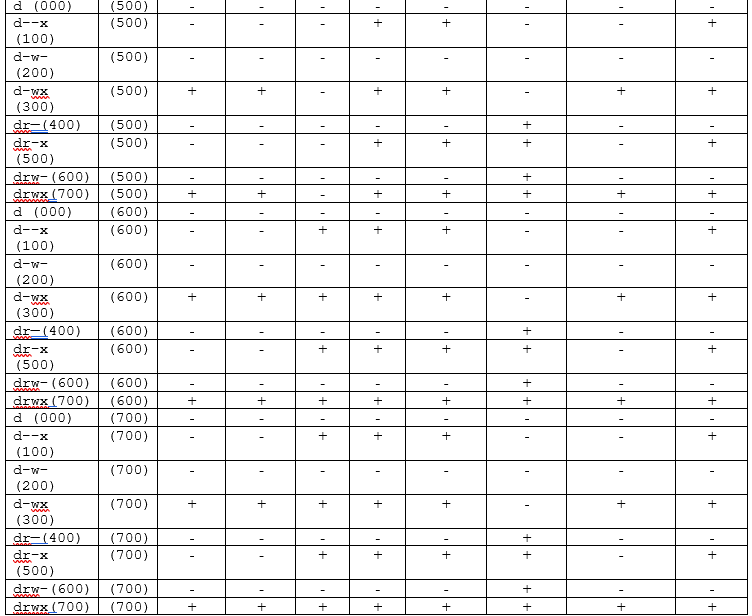


Figure 15: Установленные права и разрешенные действия, 3

Проанализировали полученную таблицу и определили, какие минимальные права доступа на директорию и на файл необходимы для различных операций (рис. [16](#fig:016)). Мы видим, что, например, создание, переименование и удаление файла не требует от файла прав доступа на чтение, запись или исполнение.

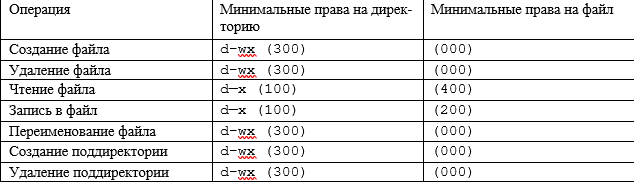


Figure 16: Минимальные права для совершения операций

# 5 Выводы

В результате лабораторной работы мной были получены навыки работы с атрибутами файлов, закреплены знания о правах доступа в системах на базе ОС Linux, а также были выявлены минимальные необходимые права доступа для выполнения операций над файлами и директориями.

# Список литературы

1. Дискреционное разграничение прав в Linux. Основные атрибуты [Электронный ресурс]. URL: <https://esystem.rudn.ru/mod/resource/view.php?id=1031371>.

2. Права доступа к файлам в Linux [Электронный ресурс]. URL: <https://losst.pro/prava-dostupa-k-fajlam-v-linux?ysclid=lmj6rdxo4478919330>.