Отчёт по лабораторной работе №2. Дискреционное разграничение прав в Linux. Основные атрибуты.

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

[1 Цель работы 1](#_Toc114269128)

[2 Теоретическое введение 1](#_Toc114269129)

[3 Выполнение лабораторной работы 1](#_Toc114269130)

[4 Вывод 8](#_Toc114269131)

[5 Библиография 8](#_Toc114269132)

# 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. [1]

# 2 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.

chmod (от англ. change mode) — команда для изменения прав доступа к файлам и каталогам, используемая в Unix-подобных операционных системах. Входит в стандарт POSIX, в Coreutils. [3]

# 3 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (использую учётную запись администратора): (рис. [1](#fig:001))

Figure 1: useradd guest

Figure 1: useradd guest

1. Зададим пароль для пользователя guest (используя учётную запись администратора (рис. [2](#fig:002))

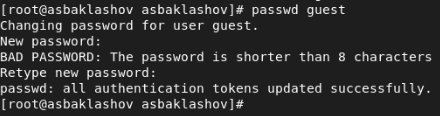


Figure 2: passwd guest

1. Войдём в систему от имени пользователя guest (рис. [3](#fig:003))

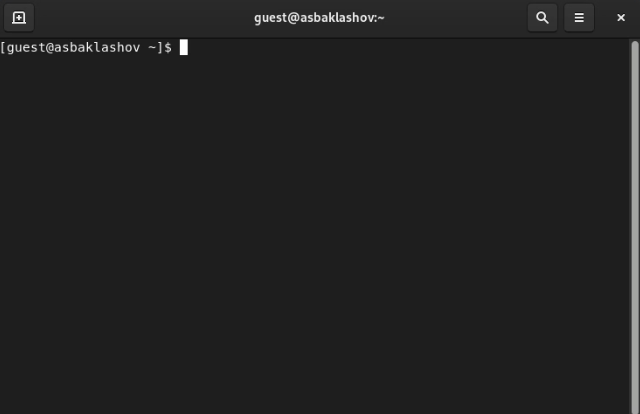


Figure 3: Вход guest

1. Определим директорию, в которой вы находитесь, командой pwd. Сравним её с приглашением командной строки. Определим, является ли она вашей домашней директорией? Если нет, зайдём в домашнюю директорию. (рис. [4](#fig:004))

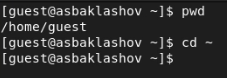


Figure 4: Домашняя директория

1. Уточним имя вашего пользователя командой whoami (рис. [5](#fig:005))

Figure 5: whoami

Figure 5: whoami

1. Уточним имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. запомним. Сравним вывод id с выводом команды groups. (рис. [6](#fig:006))

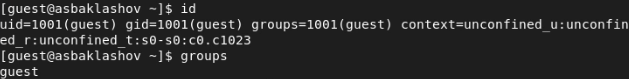


Figure 6: id

Вывод команды id совпадает с выводом команды groups (guest)

1. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. (рис. [7](#fig:007))

Figure 7: Имя пользователя

Figure 7: Имя пользователя

Данные совпадают.

1. Просмотрим файл /etc/passwd командой cat /etc/passwd

Найдём в нём свою учётную запись. Определим uid пользователя. Определим gid пользователя. (рис. [8](#fig:008))

Figure 8: /etc/passwd

Figure 8: /etc/passwd

gid и uid совпадают со значениями из прошлых пунктов.

1. Определим существующие в системе директории командой (рис. [9](#fig:009))

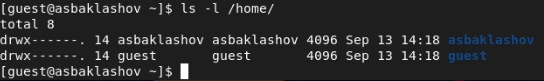


Figure 9: ls -l /home/

Поддиректории /home - /guest и /asbaklashov.

На директориях установлены права на чтение, запись и выполнение для владельца

1. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой (рис. [10](#fig:010))

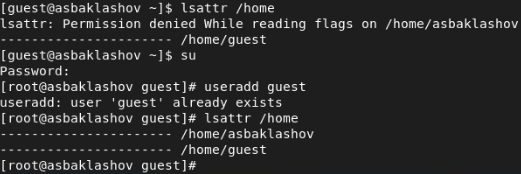


Figure 10: lsattr /home

Расширенные атрибуты удалось увидеть.

Расширенные атрибуты директиорий других пользователей удалось увидеть только от root.

1. 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. [11](#fig:011))

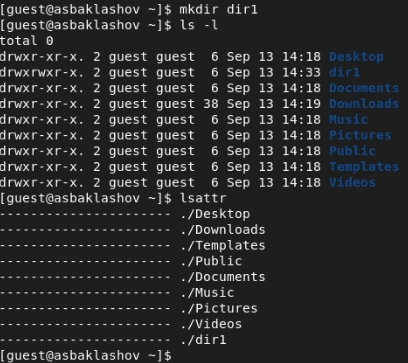


Figure 11: dir1

Директории даны все права доступа, кроме права на запись всем остальным пользователям. Расширенных атрибутов нет.

1. Снимием с директории dir1 все атрибуты командой chmod 000 dir1 (рис. [12](#fig:012))

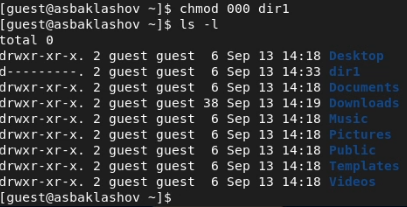


Figure 12: chmod 000 dir1

1. Попытаемся создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1 (рис. [13](#fig:013))

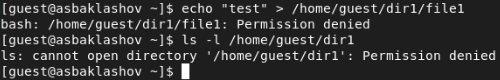


Figure 13: Файл

Создать файл не получилось, т.к. у папки /dir нет права на запись в неё. Файл file1 в папке /dir не создался.

1. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесём в таблицу знак «+», если не разрешена, знак «-». (рис. [14](#fig:014))

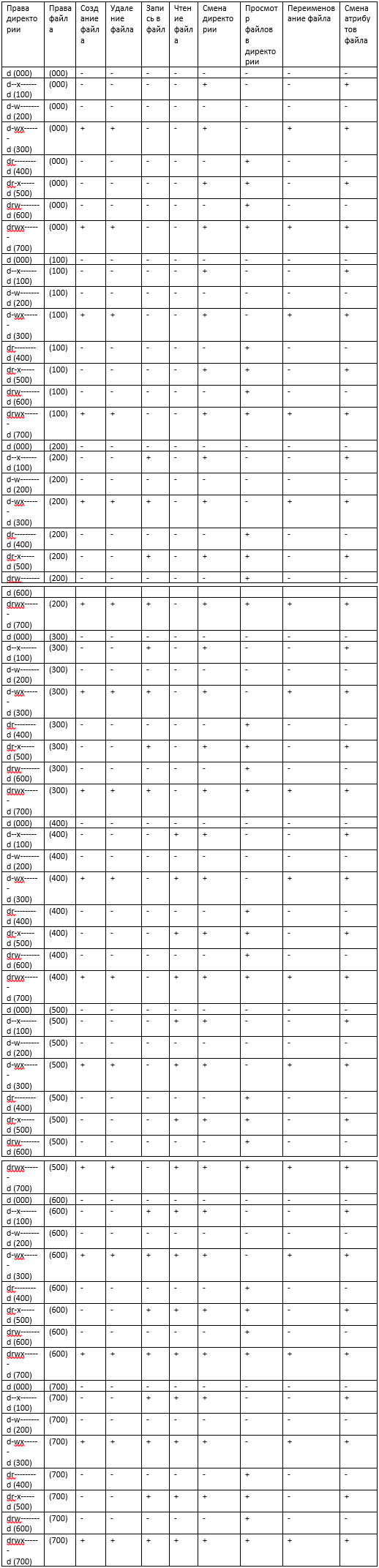


Figure 14: Установленные права и разрешённые действия

1. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1. (рис. [15](#fig:015))

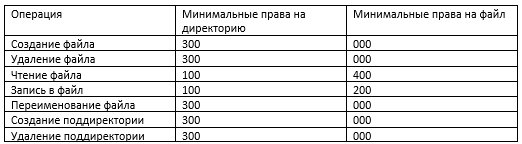


Figure 15: Минимальные права для совершения операций

# 4 Вывод

В ходе данной лабораторной работы я приобрёл практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 5 Библиография

1. Лабораторная работа №2. Дискреционное разграничение прав в Linux. Основные атрибуты. - 5 с. [Электронный ресурс]. М. URL: [Лабораторная работа №1](https://esystem.rudn.ru/pluginfile.php/1651883/mod_resource/content/6/002-lab_discret_attr.pdf) (Дата обращения: 17.09.2022).
2. Rocky Linux Documentation. [Электронный ресурс]. М. URL: [Rocky Linux Documentation](https://docs.rockylinux.org) (Дата обращения: 17.09.2022).
3. Chmod. [Электронный ресурс]. М. URL: [Файловая система](https://ru.wikipedia.org/wiki/Chmod) (Дата обращения: 17.09.2022).