Лабораторная работа № 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Аксёнова Алина Владимировна

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.

# Задание

Закрепить дискреционное разграничение прав в Linux.

# 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 - 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. Чтобы получить доступ к файлам в Linux, используются разрешения. Эти разрешения назначаются трем объектам: файлу, группе и другому объекту. Для управления правами используется команда chmod. При использовании chmod в относительном режиме вы работаете с тремя индикаторами, чтобы указать, что вы хотите сделать. Сначала вы указываете, для кого вы хотите изменить разрешения. Для этого вы можете выбрать между пользователем (u), группой (g) и другими (o). Затем вы используете оператор для добавления или удаления разрешений из текущего режима или устанавливаете их абсолютно. В конце вы используете r(read), w(write) и x(execute), чтобы указать, какие разрешения вы хотите установить.При использовании chmod вы можете устанавливать разрешения для пользователя (user), группы (group) и других (other).Помимо основных разрешений, о которых вы только что прочитали, в Linux также есть набор расширенных разрешений. Это не те разрешения, которые вы устанавливаете по умолчанию, но иногда они предоставляют полезное дополнение.

# Ход работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаем учётную запись пользователя guest. (Рис. 1).

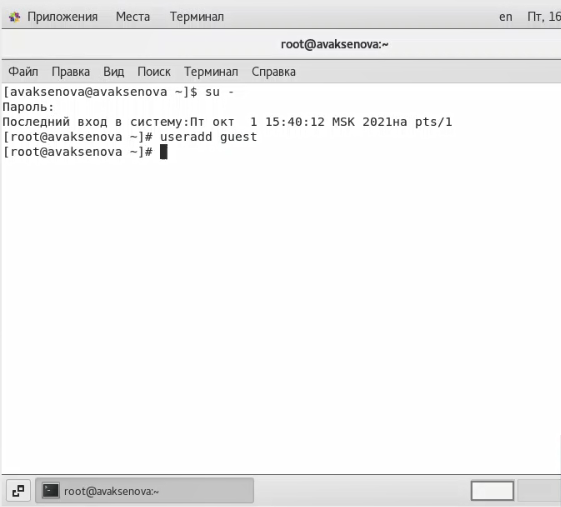


Figure 1: Создание новой учетной записи

1. Задаем пароль для пользователя guest (использую учётную запись администратора). (Рис. 2).

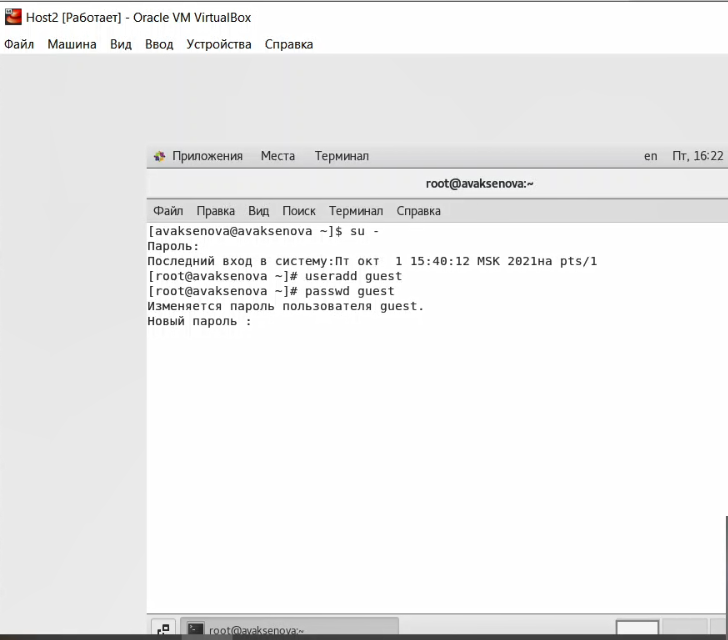


Figure 2: Пароль для новой учетной записи

1. Входим в в систему от имени пользователя guest и определяем директорию, в которой мы находимся. Как можно заметить, мы находимся в домашней директории, о чем свидетельствует значок тильды, а также результат введения команды pwd. (Рис. 3, 4).

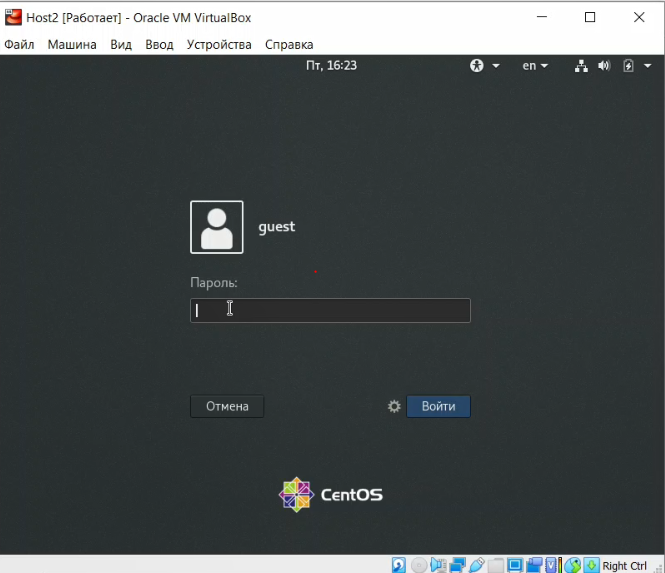


Figure 3: Вход в систему

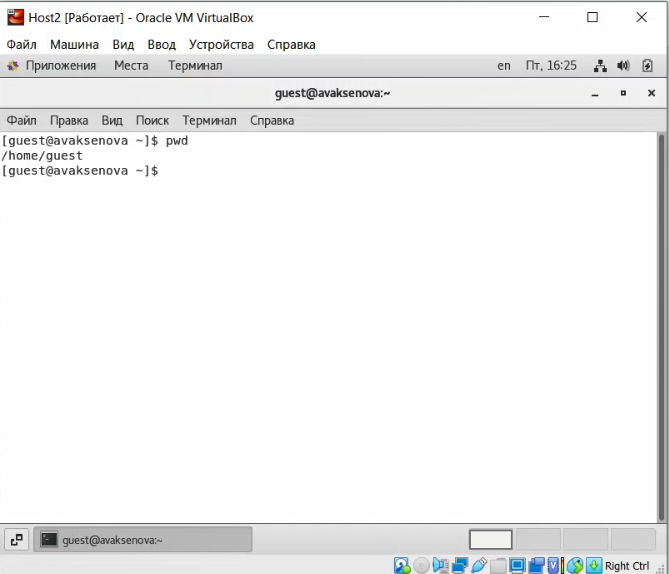


Figure 4: Определение текущей директории

1. Уточняем имя пользователя командой whoami. Уточняем его группу, а также группы, куда входит пользователь, командой id.Выведенные значения uid, gid сравниваем с выводом команды groups. Нетрудно заметить, что они совпадают. Кроме того, полученная информация совпадает с данными, выводимыми в приглашении командной строки. (Рис. 5, 6, 7, 8).

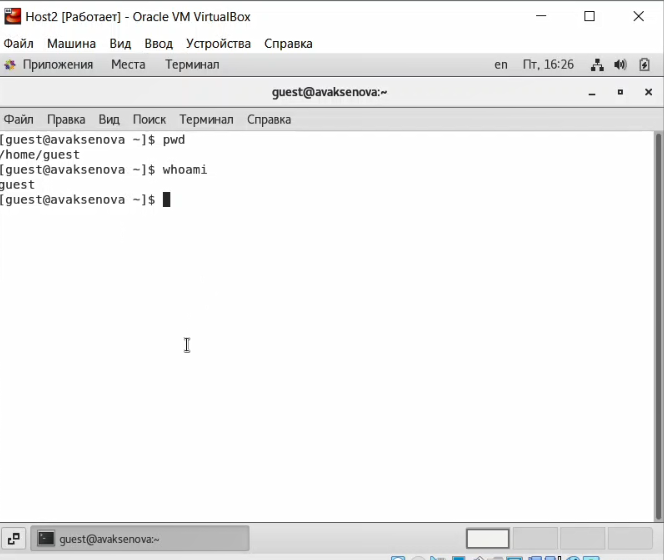


Figure 5: Уточнение имени пользователя

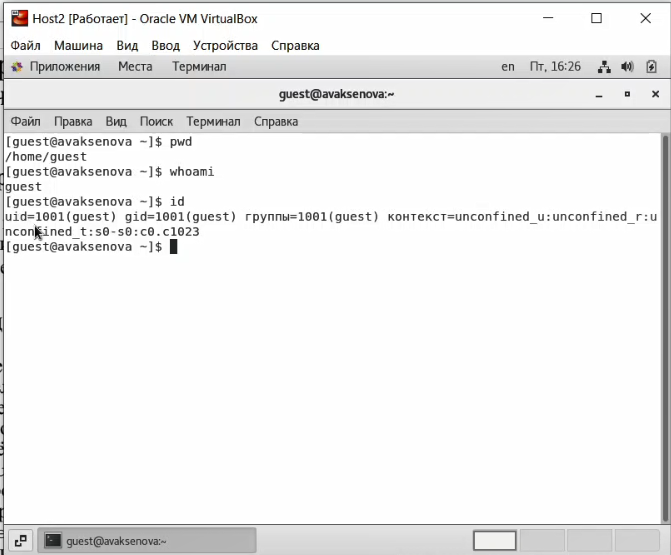


Figure 6: Группы, в которые входит пользователь

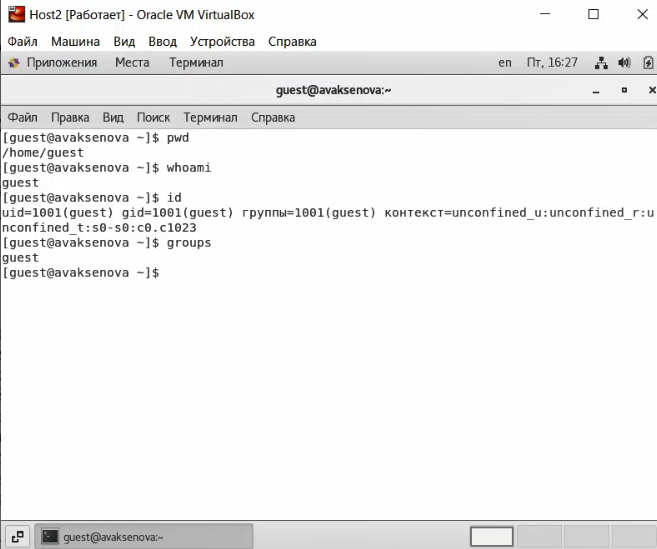


Figure 7: Вывод команды groups

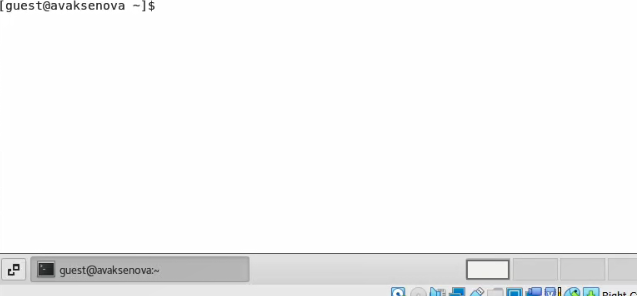


Figure 8: Данные в приглашении командной строки

1. Просматриваем файл /etc/passwd командой cat /etc/passwd. Найдя в нём свою учётную запись, определяем uid и gid пользователя. Значения совпадают с полученными в предыдущих пунктах. (Рис. 9).

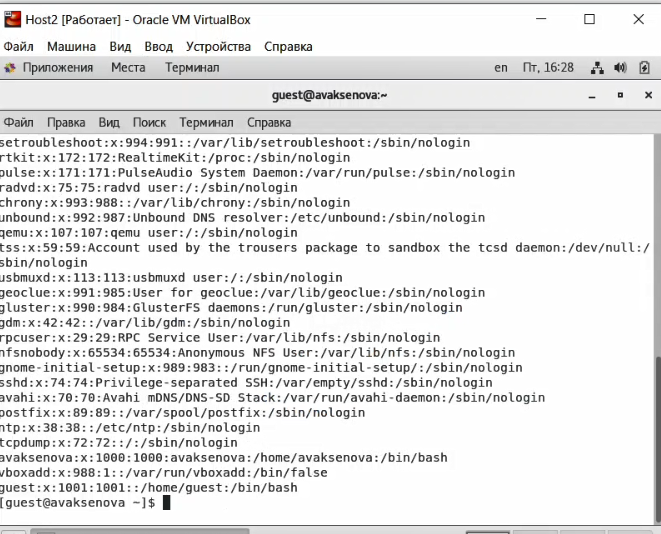


Figure 9: Просмотр файла /etc/passwd и определение uid и gid пользователя

1. Определяем существующие в системе директории командой ls -l /home/. В результате удалось получить список поддиректорий директории /home. На имеющихся директориях (avaksenova и guest) был установлен полный набор прав. (Рис. 10).



Figure 10: Поддиректории директории /home

1. Командой lsattr /home проверяем, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home.Расширенные атрибуты директории avaksenova увидеть не удалось из-за нехватки прав доступа, а расширенные атрибуты директории guest отстутствуют. (Рис. 11).

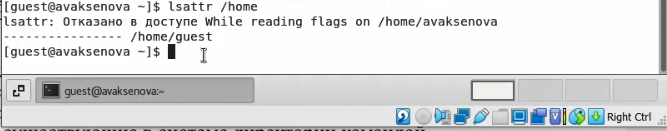


Figure 11: Проверка расширенных атрибутов

1. Создаем в домашней директории поддиректорию dir1 командой mkdir dir1. Определяем командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1, а затем снимаем с директории dir1 все атрибуты командой chmod 000 dir1 и проверяем правильность выполнения с помощью ls -l. (Рис. 12, 13).

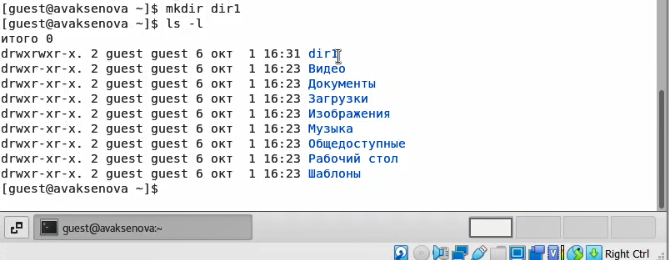


Figure 12: Создание поддиректории

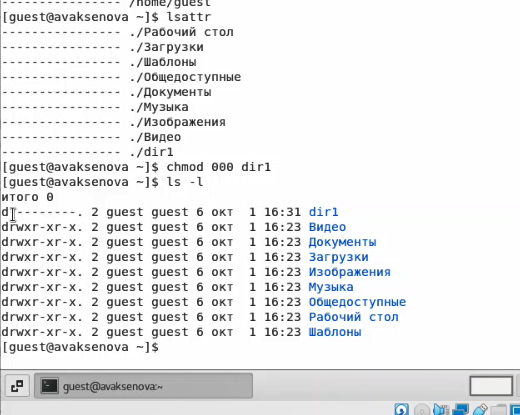


Figure 13: Проверка прав доступа и расширенных атрибутов

1. Пытаемся создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1. В результате получаем отказ в выполнении операции по созданию файла, поскольку в предыдущих пунктах с директории dir1 были сняты все атрибуты. Таким образом, файл не создался, в чем убеждаемся, применив команду ls -l /home/guest/dir1. (Рис. 14, 15).

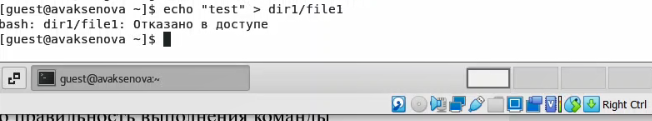


Figure 14: Создание файла в директории dir1

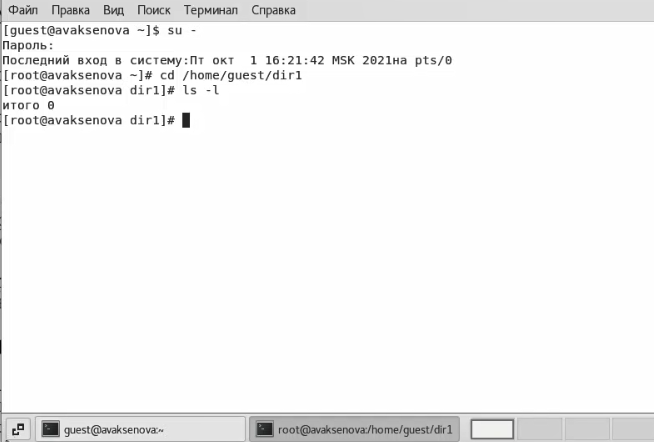


Figure 15: Проверка создания файла

1. Заполняем таблицу «Установленные права и разрешённые действия» , выполняя действия от имени владельца директории (файлов), определяем опытным путём, какие операции разрешены, а какие нет.Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-». При заполнении таблицы рассматриваем не все атрибуты файлов и директорий, а лишь «первые три»: г, w, х, для «владельца». В итоге рассматриваем 64 варианта. (Рис. 16, 17).

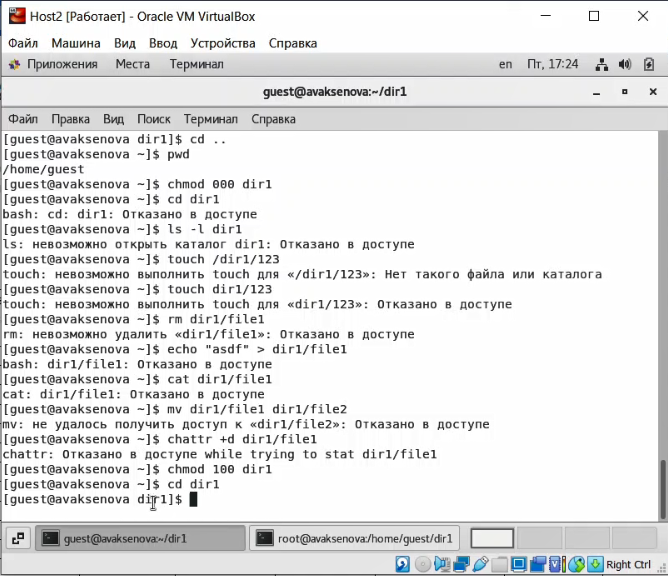


Figure 16: Процесс проверки разрешенных операций

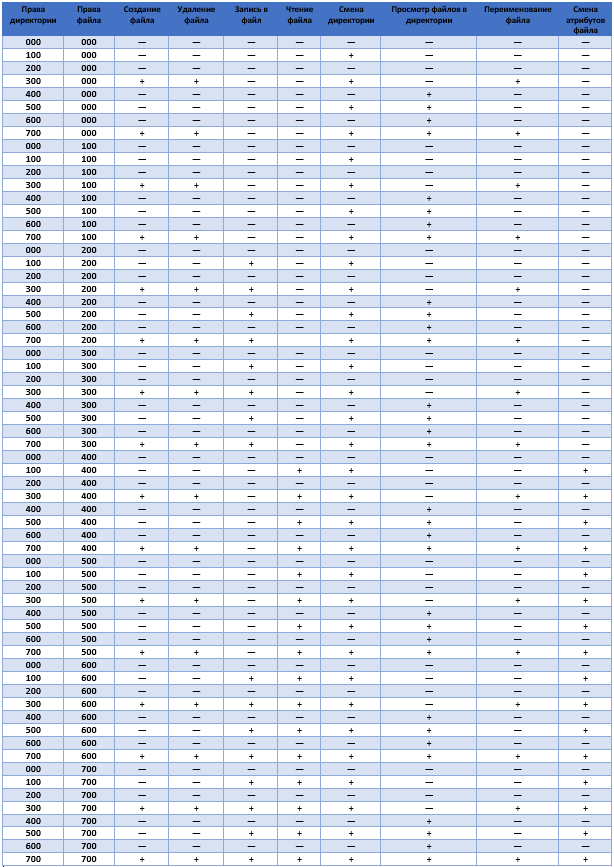


Figure 17: Заполненная таблица

1. На основании заполненной таблицы определяем те или иные минимально необходимые права для выполнения операций внутри директории dir1, внося данные во вторую таблицу. (Рис. 18).

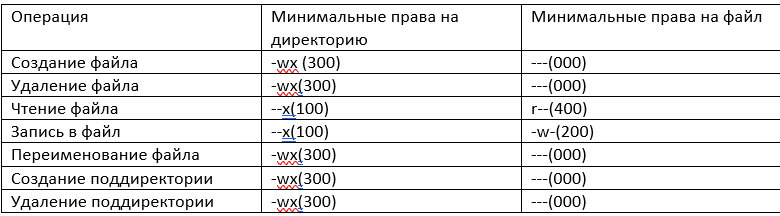


Figure 18: Проверка минимально необходимых прав для выполнения операций внутри директории

# Выводы

В результате выполнения данной работы были приобретены практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе CentOs.

# Библиографический список

1. Острейковский В. А. Информатика: учеб. для вузов / В. А. Острейковский. - 4-е изд., стер. - М.: Высш. шк., 2007. - 511 с.
2. Права в Linux [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/469667/, свободный. – Загл. с экрана.
3. Дискреционное разграничение доступа Linux [Электронный ресурс]. – Режим доступа : https://debianinstall.ru/iskretsionnoe-razgranichenie-dostupa-linux/, свободный. – Загл. с экрана.