Отчет по лаборатной работе №3

по предмету Информационная безопасность

Алхимова Дарья Сергеевна

Содержание

[Цель работы 1](#__RefHeading___Toc54746_1205269578)

[Задание 1](#__RefHeading___Toc54748_1205269578)

[Теоретическое введение 2](#__RefHeading___Toc54750_1205269578)

[Выполнение лабораторной работы 2](#__RefHeading___Toc54752_1205269578)

[Выводы 9](#__RefHeading___Toc54754_1205269578)

[Список литературы 9](#__RefHeading___Toc54756_1205269578)

# Цель работы

Целью данной работы является получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

# Задание

1. В установленной операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора):  
   useradd guest
2. Задайте пароль для пользователя guest (используя учётную запись администратора): passwd guest
3. Аналогично создайте второго пользователя guest2.
4. Добавьте пользователя guest2 в группу guest: gpasswd -a guest2 guest
5. Осуществите вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли.
6. Для обоих пользователей командой pwd определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки.
7. Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравните вывод команды groups с выводом команд id -Gn и id -G.
8. Сравните полученную информацию с содержимым файла /etc/group. Просмотрите файл командой cat /etc/group
9. От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой newgrp guest
10. От имени пользователя guest измените права директории /home/guest, разрешив все действия для пользователей группы: chmod g+rwx /home/guest
11. От имени пользователя guest снимите с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl

# Теоретическое введение

Для всех файлов и директорий Linux устанавливаются следующие права доступа:

* разрешение чтение содержимого файла;
* разрешение на изменение (запись) содержимого файла;
* разрешение на исполнение файла.

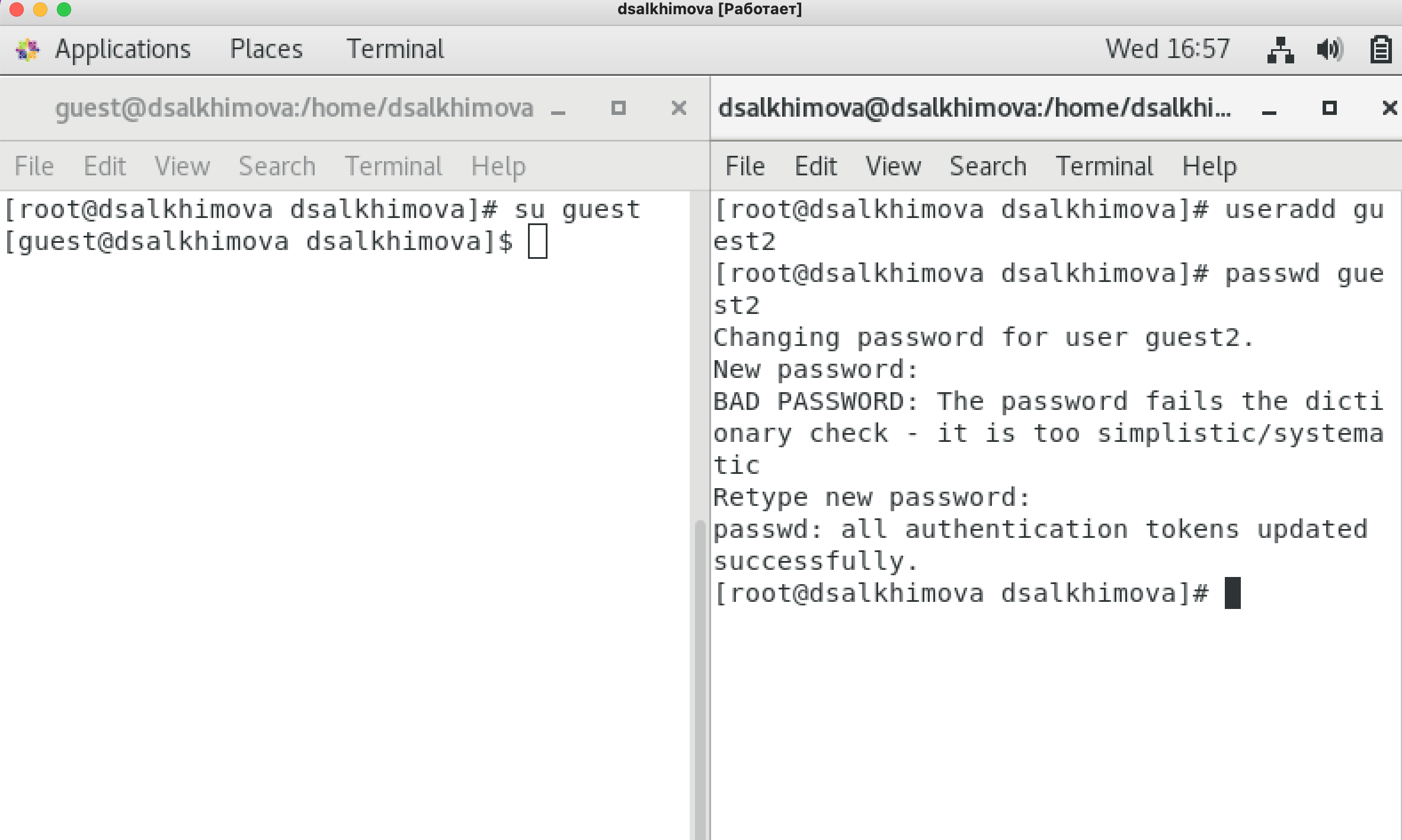
В свойствах каждого файла и директории эти три разрешения устанавливаются отдельно для:

* владельца файла
* группы владельцев файла, которой принадлежит этот файл
* всех остальных.

Просмотреть права доступа, а также владельца и группу, к которой относится файл, можно командой ls с опцией -l. Чтобы изменить режим (права доступа) файла или каталога, используется команда chmod с параметрами. Три цифры соответствуют трём параметрам режима доступа: чтение, запись, выполнение. Поэтому права доступа можно представить в виде трёх двоичных цифр, которые можно записать как одну восьмеричную цифру. Используя три восьмеричных цифры, мы можем установить режим файла для владельца, группы владельцев и всех остальных. Хотя запоминание восьмеричного бинарного отображения может показаться неудобным, обычно нужно использовать только несколько часто используемых: 7 (rwx), 6 (rw-), 5 (r-x), 4 (r–) и 0 (—). Либо можно запомнить значение одиночных прав доступа и складывать их значения для получения любых комбинаций: 4 (r–), 2 (-w-), 1 (–x). После можно получить любую комбинацию, для прав чтения и записи это 6 (4+2) (rw-), для прав записи и выполнения это 3 (2+1) (-wx), для прав чтения и выполнения это 5 (4+1) (r-x)

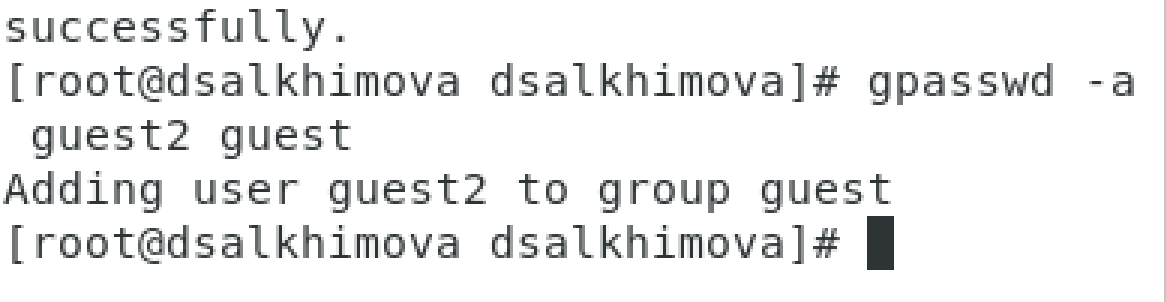
# Выполнение лабораторной работы

1. Т.к. в рамках предыдущей лабораторной работы в установленной операционной системе я создала учетную запись пользователя guest и задала пароль для нее, то в данной работе я аналогично создала второго пользователя guest2, задала пароль и выполнила вход в эту учетную запись. ([рис. 1](images3/1.png))



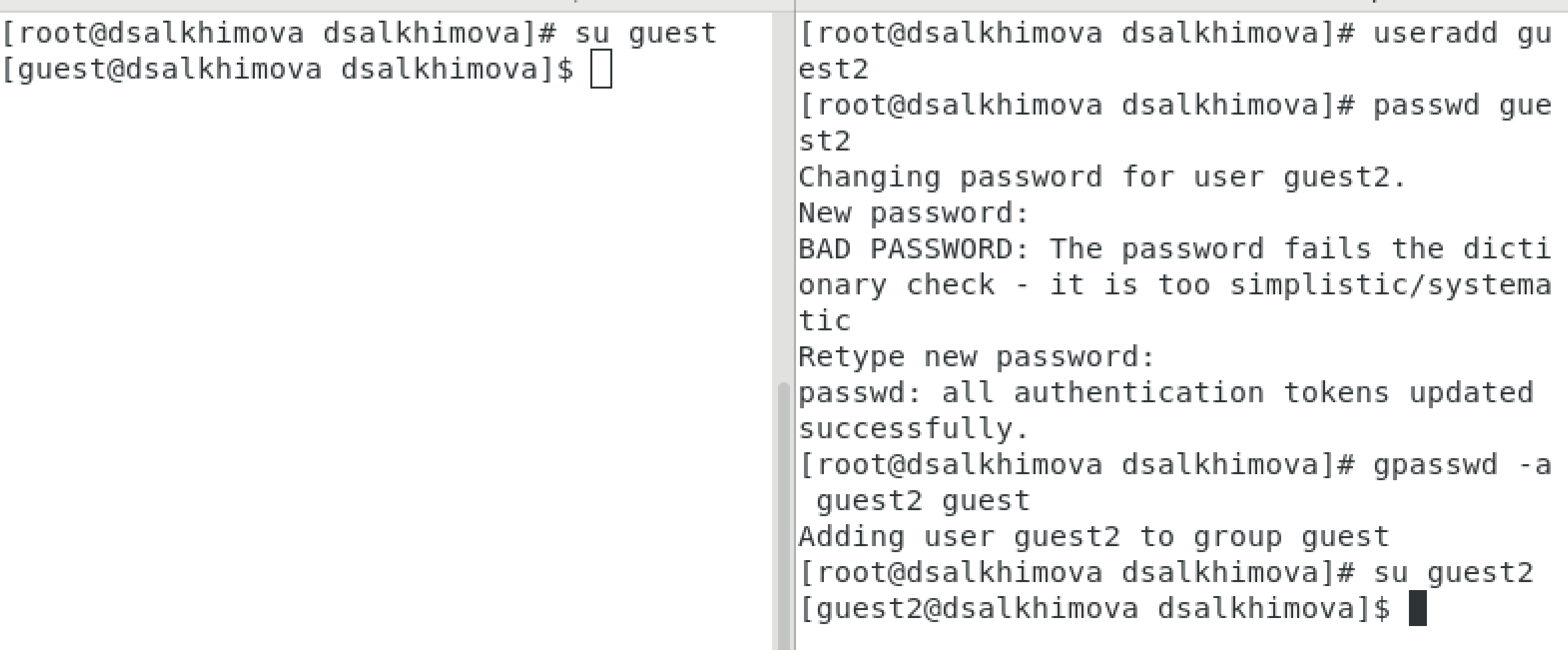
Создание второго пользователя

1. Добавила пользователя guest2 в группу guest с помощью команды  
   gpasswd -a guest2 guest. ([рис. 2](images3/2.png))



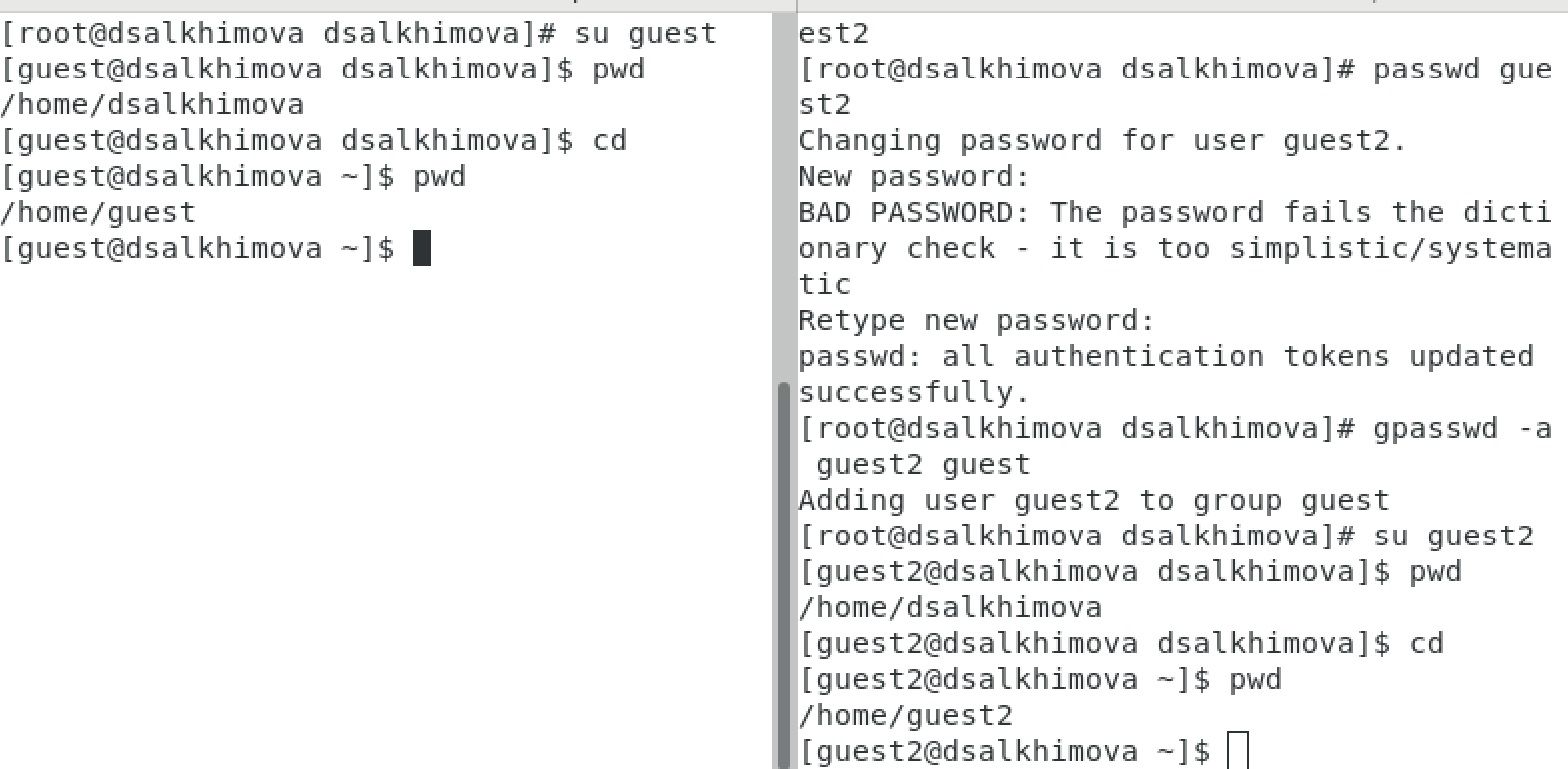
Добавление пользователя в группу

1. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. ([рис. 3](images3/3.png))



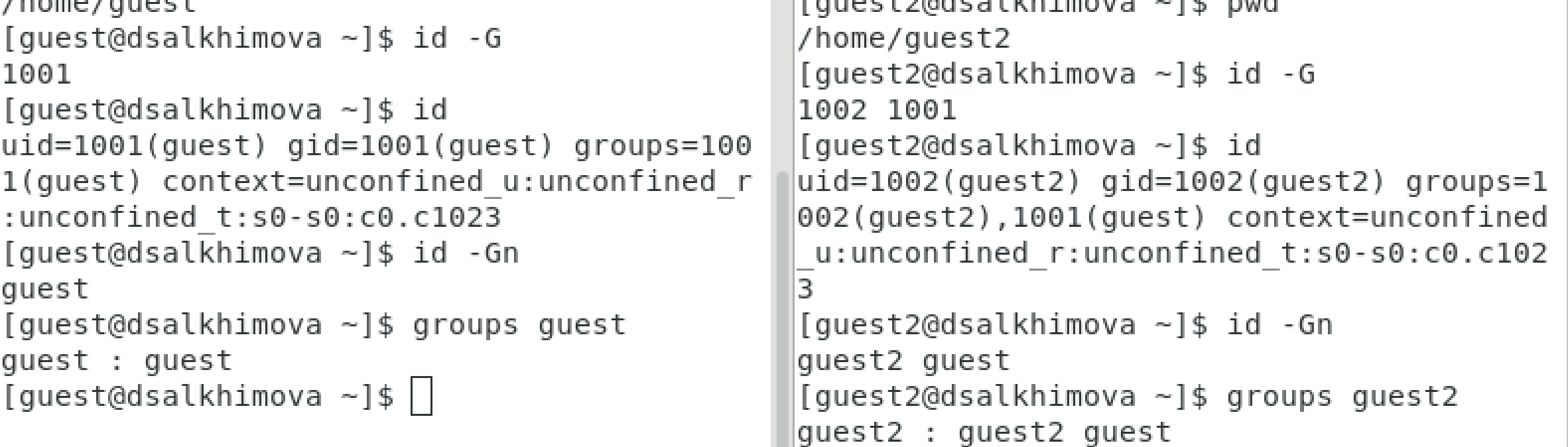
Авторизация под разными пользователями

1. Для обоих пользователей определила директорию,в которой я нахожусь, командой pwd - в домашней директории пользователя, под которым осуществлен вход в ОС. Для каждого пользователя перешла в домашнюю директорию с помощью команды cd и еще раз проверила текущую директорию. ([рис. 4](images3/4.png))



Проверка текущей директории

1. Уточнила имя каждого пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определила командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Информация, выводимая командами groups и id -Gn и id -G касательно групп пользователей совпадает. id -G выводит идентификаторы групп, куда входит пользователь, а id -Gn - имена этих групп. Пользователь guest входит только в группу guest (1001), а пользователь guest2 - в guest (1001) и guest2 (1002). ([рис. 5](images3/5.png))



Данные групп пользователей

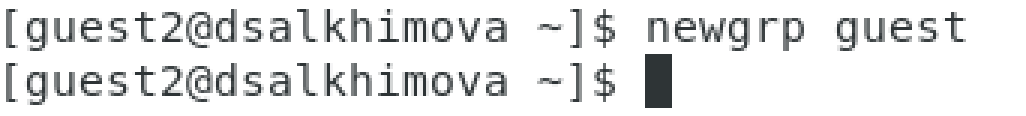
1. Просмотрела файл group командой  
   cat /etc/group. ([рис. 6](images3/6.png))



Просмотр файла group

Информация, содержащаяся в файле, совпадает с той, что мы получили на предыдущем шаге (учетные записи созданных пользователей находятся в самом низу вывода).

1. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой newgrp guest. ([рис. 7](images3/7.png))



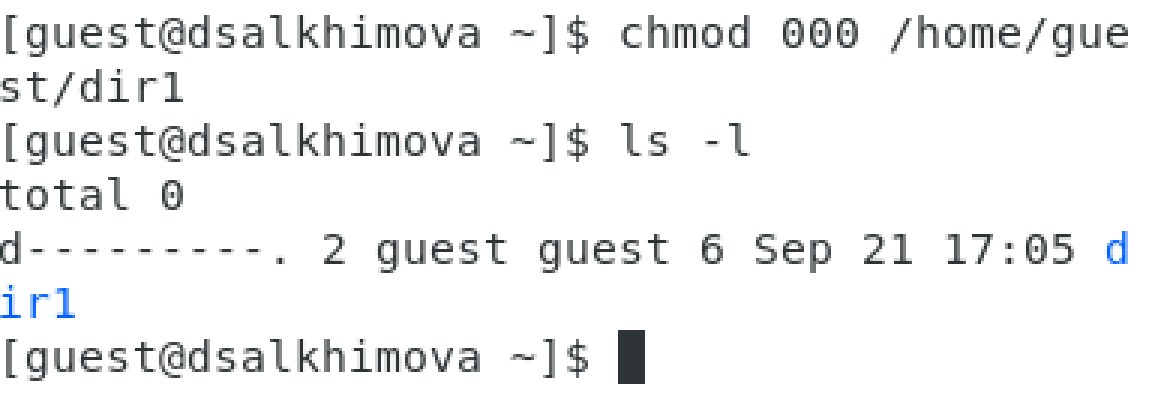
Регистрация пользователя в группе

1. От имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы владельца: chmod g+rwx /home/guest. ([рис. 8](images3/8.png))



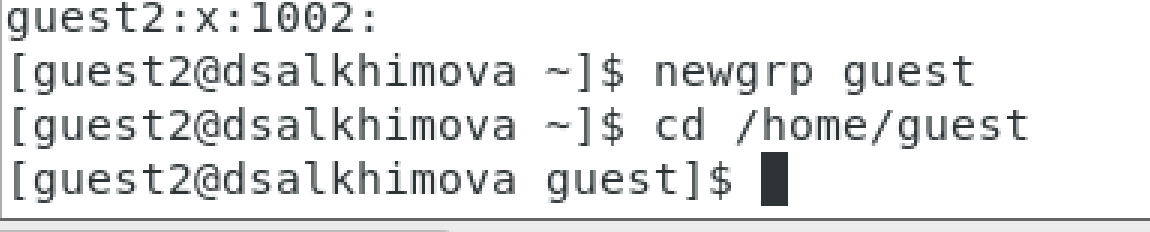
Изменение прав на директорию для группы

1. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой chmod 000 dirl и проверила правильность выполнения команды через ls -l ([рис. 9](images3/9.png))



Редактрирование и проверка прав на директорию

1. Проверила, что у пользователя guest2 есть доступ в домашнюю директорию пользователя guest как у члена группы владельца. ([рис. 10](images3/10.png))



Проверка доступа в директорию

1. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполнила таблицу “Установленные права и разрешенные действия для групп”, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносила в таблицу знак «+», если не разрешена, знак «-».

* Обозначения в таблице:
  1. Создание файла
  2. Удаление файла
  3. Запись в файл
  4. Чтение файла
  5. Смена директории
  6. Просмотр файлов в директории
  7. Переименование файл
  8. Смена атрибутов файла

Установленные права и разрешённые действия для групп

| Права директории | Права файла | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| d--------- (000) | ---------- (000) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ---------- (000) | - | - | - | - | + | - | - | + |
| d----w---- (020) | ---------- (000) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ---------- (000) | + | + | - | - | + | - | + | + |
| d---r----- (040) | ---------- (000) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ---------- (000) | - | - | - | - | + | + | - | + |
| d---rw---- (060) | ---------- (000) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ---------- (000) | + | + | - | - | + | + | + | + |
| d--------- (000) | ------x--- (010) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ------x--- (010) | - | - | - | - | + | - | - | + |
| d----w---- (020) | ------x--- (010) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ------x--- (010) | + | + | - | - | + | - | + | + |
| d---r----- (040) | ------x--- (010) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ------x--- (010) | - | - | - | - | + | + | - | + |
| d---rw---- (060) | ------x--- (010) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ------x--- (010) | + | + | - | - | + | + | + | + |
| d--------- (000) | -----w---- (020) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | -----w---- (020) | - | - | + | - | + | - | - | + |
| d----w---- (020) | -----w---- (020) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | -----w---- (020) | + | + | + | - | + | - | + | + |
| d---r----- (040) | -----w---- (020) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | -----w---- (020) | - | - | + | - | + | + | - | + |
| d---rw---- (060) | -----w---- (020) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | -----w---- (020) | + | + | + | - | + | + | + | + |
| d--------- (000) | -----wx--- (030) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | -----wx--- (030) | - | - | + | - | + | - | - | + |
| d----w---- (020) | -----wx--- (030) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | -----wx--- (030) | + | + | + | - | + | - | + | + |
| d---r----- (040) | -----wx--- (030) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | -----wx--- (030) | - | - | + | - | + | + | - | + |
| d---rw---- (060) | -----wx--- (030) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | -----wx--- (030) | + | + | + | - | + | + | + | + |
| d--------- (000) | ----r----- (040) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----r----- (040) | - | - | - | + | + | - | - | + |
| d----w---- (020) | ----r----- (040) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----r----- (040) | + | + | - | + | + | - | + | + |
| d---r----- (040) | ----r----- (040) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----r----- (040) | - | - | - | + | + | + | - | + |
| d---rw---- (060) | ----r----- (040) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----r----- (040) | + | + | - | + | + | + | + | + |
| d--------- (000) | ----r-x--- (050) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----r-x--- (050) | - | - | - | + | + | - | - | + |
| d----w---- (020) | ----r-x--- (050) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----r-x--- (050) | + | + | - | + | + | - | + | + |
| d---r----- (040) | ----r-x--- (050) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----r-x--- (050) | - | - | - | + | + | + | - | + |
| d---rw---- (060) | ----r-x--- (050) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----r-x--- (050) | + | + | - | + | + | + | + | + |
| d--------- (000) | ----rw---- (060) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----rw---- (060) | - | - | + | + | + | - | - | + |
| d----w---- (020) | ----rw---- (060) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----rw---- (060) | + | + | + | + | + | - | + | + |
| d---r----- (040) | ----rw---- (060) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----rw---- (060) | - | - | + | + | + | + | - | + |
| d---rw---- (060) | ----rw---- (060) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----rw---- (060) | + | + | + | + | + | + | + | + |
| d--------- (000) | ----rwx--- (070) | - | - | - | - | - | - | - | - |
| d-----x--- (010) | ----rwx--- (070) | - | - | + | + | + | - | - | + |
| d----w---- (020) | ----rwx--- (070) | - | - | - | - | - | - | - | - |
| d----wx--- (030) | ----rwx--- (070) | + | + | + | + | + | - | + | + |
| d---r----- (040) | ----rwx--- (070) | - | - | - | - | - | + | - | - |
| d---r-x--- (050) | ----rwx--- (070) | - | - | + | + | + | + | - | + |
| d---rw---- (060) | ----rwx--- (070) | - | - | - | - | - | + | - | - |
| d---rwx--- (070) | ----rwx--- (070) | + | + | + | + | + | + | + | + |

1. На основании заполненной таблицы я определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила таблицу “Минимальные права для совершения операций” [-@tbl:min-rig]. Для заполнения последних двух строк опытным путем проверила минимальные права для создания и удаления поддиректории.

Минимальные права для совершения операций

| Операция | Мин. права на директорию | Мин. права на файл |
| --- | --- | --- |
| Создание файла | d----wx--- (030) | ---------- (000) |
| Удаление файла | d----wx--- (030) | ---------- (000) |
| Чтение файла | d-----x--- (010) | ----r----- (040) |
| Запись в файл | d-----x--- (010) | -----w---- (020) |
| Переименование файла | d----wx--- (030) | ---------- (000) |
| Создание поддиректории | d----wx--- (030) | ---------- (000) |
| Удаление поддиректории | d----wx--- (030) | ---------- (000) |

Сравнивая данную таблицу с такой же таблицей из предыдущей лабораторной работы, можно сделать вывод, что они идентичны. Единственное различие в том, что в предыдущей лабораторной работе права присваивались владельцу, а в этой - группе владельца.

# Выводы

В процессе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.

# Список литературы

1. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
2. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
3. Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.