

Цель работы

1. Получение практических навыков работы в консоли с атрибутами файлов.
2. Закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Выполнение лабораторной работы

Выполнение задания

Создаём новую учётную запись `guest`, используя команду `useradd guest`

```
[vyzhukova@user ~]$ sudo useradd guest
```

Мы полагаем, что ваш системный администратор изложил вам основы безопасности. Как правило, всё сводится к трём следующим правилам:

- №1) Уважайте частную жизнь других.
- №2) Думайте, прежде что-то вводить.
- №3) С большой властью приходит большая ответственность.

```
[sudo] пароль для vyzhukova:  
[vyzhukova@user ~]$ █
```

Рис. 1. Создание учётной записи

После этого зададим пароль с помощью команды `passwd guest`, используя учетную запись администратора.

```
[vyzhukova@user ~]$ sudo passwd guest  
Изменяется пароль пользователя guest.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.  
[vyzhukova@user ~]$ █
```

Рис. 2. Установка пароля

Входим в систему от имени пользователя `guest`

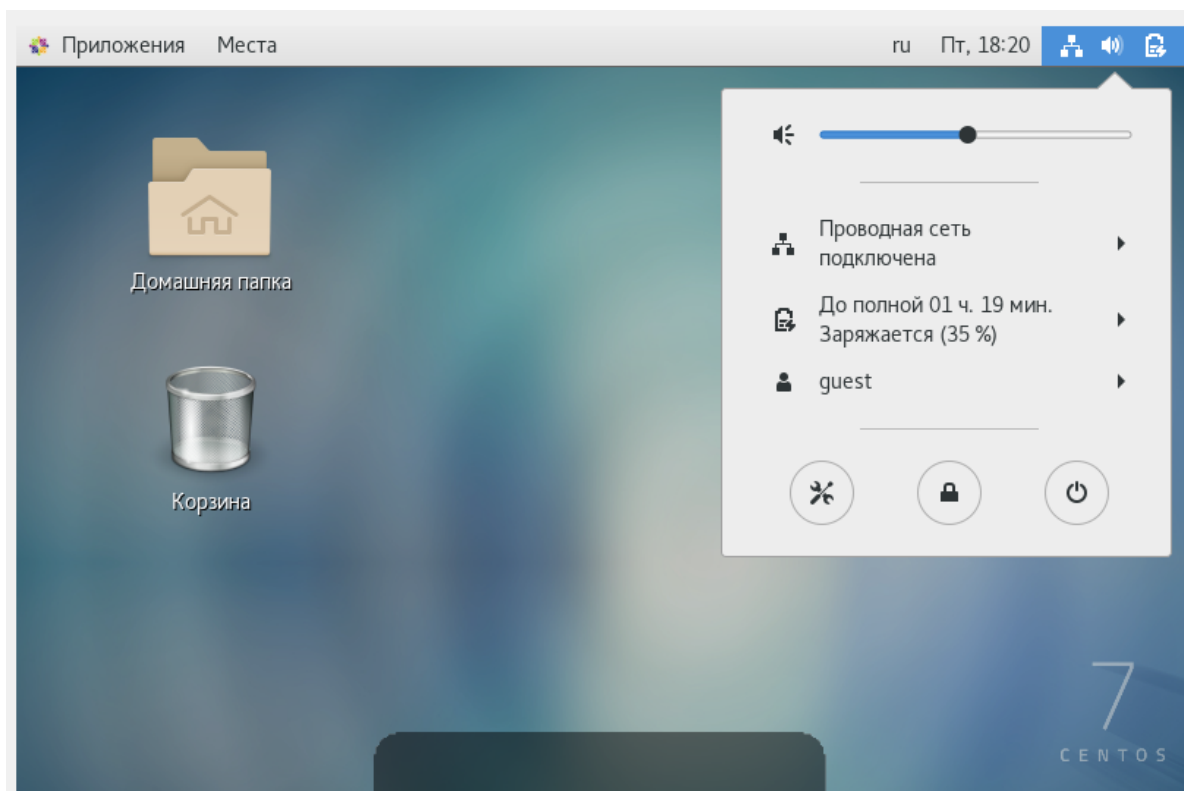


Рис. 3. Вход в систему

и определяем директорию, в которой находимся, с помощью команды `pwd`.

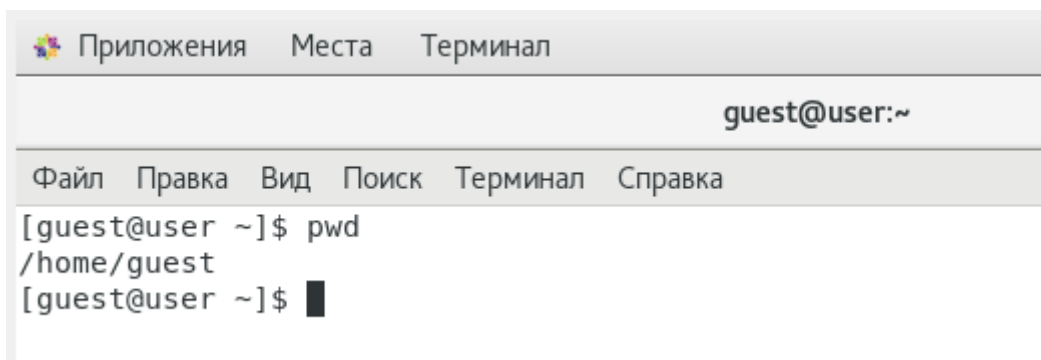


Рис. 4. Определение директории

Сравнивая с приглашением командной строки, определяем сходство и факт, что это наша домашняя директория.

Командой `whoami` уточняем имя пользователя - `guest`.

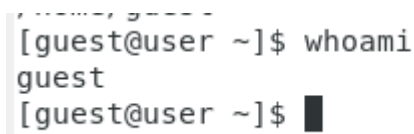


Рис. 5. Уточнение имени пользователя

Уточним имя пользователя, его группы, а также группы, куда входит пользователь, командой `id`. Получаем результат 1001.



Рис. 6. Уточняем имя и атрибуты

Далее сравним вывод id с приглашением командной строки, обнаружим, что имя пользователя повторяется.

Посмотрим файл /etc/passwd командой cat /etc/passwd.

```
guest:x:1001:1001::/home/guest:/bin/bash
[guest@user ~]$ cat /etc/passwd | grep "1001"
guest:x:1001:1001::/home/guest:/bin/bash
[guest@user ~]$
```

Рис. 7. Просмотр файла /etc/passwd

Найдём в нём свою учётную запись. Определим uid пользователя = 1001. Определим gid пользователя = 1001. Сравним найденные значения с полученными в предыдущих пунктах - они одинаковые.

Определим существующие в системе директории командой ls -l /home/.

```
[guest@user ~]$ ls -l /home/
итого 8
drwx-----. 15 guest      guest      4096 сен  9 18:34 guest
drwx-----. 15 vyzhukova vyzhukova 4096 сен  9 18:26 vyzhukova
[guest@user ~]$
```

Рис. 8. Определение существующих директорий

Нам удалось получить список поддиректорий. У каждой из них установлены права на чтение, запись и выполнение только для самого пользователя.

Проверяем, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home

```
[guest@user ~]$ lsattr /home/
lsattr: Отказано в доступе While reading flags on /home/vyzhukova
----- /home/guest
[guest@user ~]$
```

Рис. 9. Проверка атрибутов

Нам удалось увидеть расширенные атрибуты директории, но не удалось увидеть расширенные атрибуты директорий других пользователей.

Создадим в домашней директории поддиректорию dir1 командой mkdir dir1

```
[guest@user ~]$ mkdir dir1
[guest@user ~]$
```

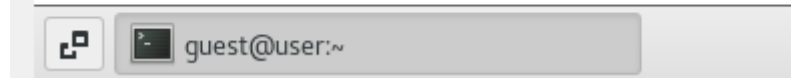


Рис. 10. Создание поддиректории dir1

Определим командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
[guest@user ~]$ ls -l | grep dir1
drwxrwxr-x. 2 guest guest 6 сен  9 18:43 dir1
[guest@user ~]$ lsattr | grep dir1
----- ./dir1
[guest@user ~]$
```

Рис. 11. Определение прав доступа и расширенных атрибутов

Снимем с директории dir1 все атрибуты командой `chmod 000 dir1` и проверим с её помощью правильность выполнения команды `ls -l`.

```
[guest@user ~]$ chmod 000 dir1
[guest@user ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен  9 18:43 dir1
```

Рис. 12. Снятие атрибутов

Попытаемся создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`, но получим отказ от выполнения, так как шагом ранее сняли все атрибуты с директории. Проверим, действительно ли файл не создался, с помощью команды `ls -l /home/guest/dir1`.

```
[guest@user ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@user ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@user ~]$
```

Рис. 13. Попытка создать файл.

Заполним таблицу «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)	----- (000)	+	+
-	-	+	-
-	+	+	-
dr----- (400)	----- (000)	-	-
-	-	-	+
-	-	-	-
dr-x----- (500)	----- (000)	-	-
-	-	+	+
-	-	+	-
drw----- (600)	----- (000)	-	-
-	-	-	+
-	-	-	-
drwx----- (700)	----- (000)	+	+
-	-	+	+
-	+	+	-
d----- (000)	--x----- (100)	-	-
-	-	-	-
-	-	-	-

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

dr----- (400)	-wx----- (300)	+	-
+	+	+	+
+	+	-	
dr-x----- (500)	-wx----- (300)	+	-
+	-	-	+
+	+	-	
drw----- (600)	-wx----- (300)	+	+
-	+	+	+
+	+	+	
drwx----- (700)	-wx----- (300)	+	+
-	+	-	+
+	+	-	
d----- (000)	r----- (400)	-	-
-	+	-	+
+	+	+	
d--x----- (100)	r----- (400)	+	+
-	-	-	+
+	+	-	
d-w----- (200)	r----- (400)	-	+
+	+	+	-
+	+	+	
d-wx----- (300)	r----- (400)	+	-
+	+	-	-
+	+	-	
dr----- (400)	r----- (400)	-	-
+	-	+	-
+	+	+	
dr-x----- (500)	r----- (400)	+	+
+	+	+	-
+	+	-	
drw----- (600)	r----- (400)	+	+
-	-	+	-
+	+	-	
drwx----- (700)	r----- (400)	-	+
+	+	-	-
+	+	+	
d----- (000)	r-x----- (500)	-	-
-	+	+	-
+	+	-	
d--x----- (100)	r-x----- (500)	-	-
-	-	-	+
+	+	+	
d-w----- (200)	r-x----- (500)	-	-
+	-	-	+
-	+	-	
d-wx----- (300)	r-x----- (500)	-	-
+	+	-	+
-	+	+	
dr----- (400)	r-x----- (500)	+	-
+	-	-	-
-	+	-	
dr-x----- (500)	r-x----- (500)	-	+
+	+	+	-
+	+	+	
drw----- (600)	r-x----- (500)	-	-
+	-	+	+
-	+	-	

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

Заполним таблицу «Минимальные права для совершения операций».

Операция файл	минимальные права на директорию	минимальные права на
----- -----	----- -----	----- -----
Создание файла	d-wx----- (300)	----- (000)
удаление файла	d-wx----- (300)	----- (000)
чтение файла	d--x----- (100)	r----- (400)
Запись в файл	d--x----- (100)	-w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
удаление поддиректории	d-wx----- (300)	----- (000)

Выводы

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

Список литературы

- Кулябов Д. С., Королькова А. В., Геворкян М. Н. Лабораторная работа №2