

Отчёт по лабораторной работе № 3

Дисциплина: Основы информационной безопасности

Маметкадыров Ынтымак

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Выводы	15
Список литературы	16

List of Figures

0.1	Создание пользователя и установка пароля	6
0.2	Проверка групп	7
0.3	Регистрация пользователя в группе	7
0.4	Смена атрибутов	8

Цель работы

Получить навыки работы в консоли с правами и атрибутами файлов и директорий *для групп пользователей*, а также проверка необходимых прав для выполнения различных действий для работы с файлами и директориями.

Теоретическое введение

Атрибуты — это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые — для группы пользователей, последние — для всех остальных пользователей в системе.

Установка атрибутов производится командой `chmod`. Установка бита чтения (`r`) позволяет сделать файл доступным для чтения. Наличие бита записи (`w`) позволяет изменять файл. Установка бита запуска (`x`) позволяет запускать файл на исполнение.

Более подробно см. в `[@gnu-doc:bash]`.

В ОС Linux, группа — это набор пользователей. Основная цель групп — это определить права на чтение, запись и исполнение сразу для нескольких пользователей, состоящих в группе. Так же пользователи могут быть добавлены в уже существующие группы для получения их прав.

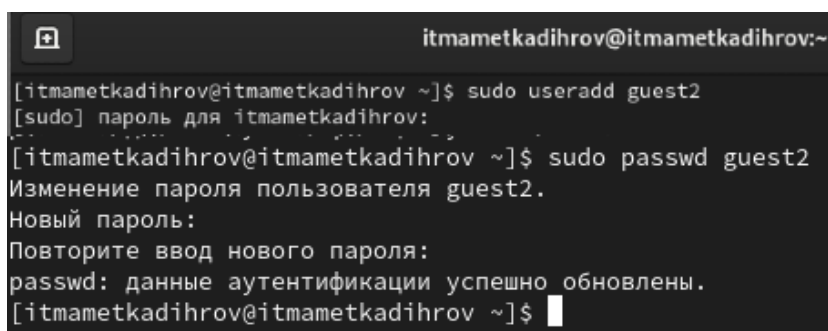
Группы бывают двух видов:

- Первичная группа — это группа, приписанная к файлам, созданным пользователем. Обычно имя первичной группы совпадает с именем пользователя. У каждого пользователя может быть только одна первичная группа.
- Вторичная группа — используется для определения прав для набора пользователей. Пользователь может состоять в нескольких вторичных группах или не состоять ни в одной.

Более подробно см. в `[@gnu-doc-1:bash]`

Выполнение лабораторной работы

Создаём нового пользователя `guest2` командой `useradd`, затем устанавливаем для него пароль с помощью команды `passwd guest2` (рис. [-@fig:001]).



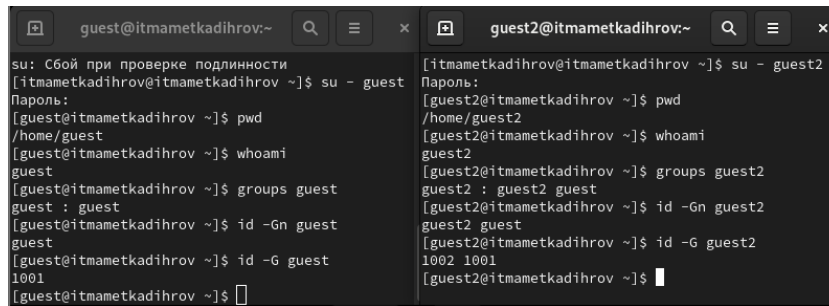
```
itmametskadihrov@itmametskadihrov:~$ sudo useradd guest2
[sudo] пароль для itmametskadihrov:
itmametskadihrov@itmametskadihrov:~$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
itmametskadihrov@itmametskadihrov:~$
```

Figure 0.1: Создание пользователя и установка пароля

Добавляем пользователя `guest2` в группу `guest` командой `gpasswd -a`.

Заходим в систему от имени пользователей `guest`, и `guest2` на двух терминалах, используя команду `su -` и только что установленный пароль.

Выполняем команду `pwd`, которая показывает, что мы находимся в соответствующих домашних каталогах пользователей. Уточняем имя пользователя командой `whoami`, ожидаемо получаем вывод `guest` и `guest2` соответственно. Определяем группы, в которых состоят пользователи командой `groups`. Пользователь `guest` состоит только в группе `guest`, а пользователь `guest2` состоит в двух группах — `guest` и `guest2`. Эту же информацию можно узнать с помощью команды `id -Gn` (рис. [-@fig:002]).

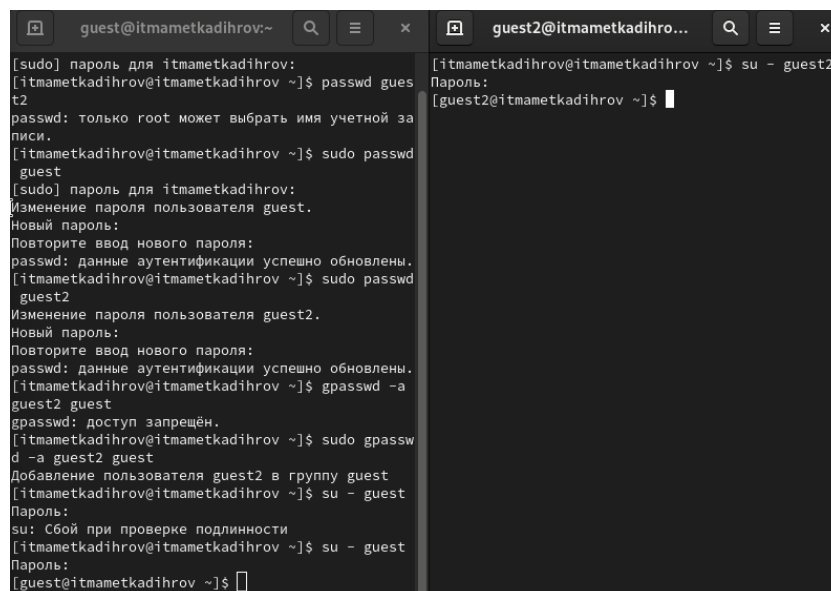


```
guest@itmametskadihrov:~$ su: Сбой при проверке подлинности
[itmametskadihrov@itmametskadihrov ~]$ su - guest
Пароль:
[guest@itmametskadihrov ~]$ pwd
/home/guest
[guest@itmametskadihrov ~]$ whoami
guest
[guest@itmametskadihrov ~]$ groups guest
guest : guest
[guest@itmametskadihrov ~]$ id -Gn guest
guest
[guest@itmametskadihrov ~]$ id -G guest
1001
[guest@itmametskadihrov ~]$

[itmametskadihrov@itmametskadihrov ~]$ su - guest2
Пароль:
[guest2@itmametskadihrov ~]$ pwd
/home/guest2
[guest2@itmametskadihrov ~]$ whoami
guest2
[guest2@itmametskadihrov ~]$ groups guest2
guest2 : guest2 guest
[guest2@itmametskadihrov ~]$ id -Gn guest2
guest2 guest
[guest2@itmametskadihrov ~]$ id -G guest2
1002 1001
[guest2@itmametskadihrov ~]$
```

Figure 0.2: Проверка групп

В содержимом файла `/etc/passwd` находим информацию о группах, в которых состоят пользователи, что соответствует данным, полученным с помощью команды `id` и `groups`. От имени пользователя `guest2` выполняем регистрацию пользователя в группе командой `newgrp` (рис. [-@fig:003]).



```
guest@itmametskadihrov:~$ [sudo] пароль для itmametskadihrov:
[itmametskadihrov@itmametskadihrov ~]$ passwd guest2
passwd: только root может выбрать имя учетной записи.
[itmametskadihrov@itmametskadihrov ~]$ sudo passwd guest
[sudo] пароль для itmametskadihrov:
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[itmametskadihrov@itmametskadihrov ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[itmametskadihrov@itmametskadihrov ~]$ gpasswd -a guest2 guest
gpasswd: доступ запрещен.
[itmametskadihrov@itmametskadihrov ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[itmametskadihrov@itmametskadihrov ~]$ su - guest
Пароль:
su: Сбой при проверке подлинности
[itmametskadihrov@itmametskadihrov ~]$ su - guest
Пароль:
[guest@itmametskadihrov ~]$

[itmametskadihrov@itmametskadihrov ~]$ su - guest2
Пароль:
[guest2@itmametskadihrov ~]$
```

Figure 0.3: Регистрация пользователя в группе

От имени пользователя `guest` изменяем права на директорию `/home/guest`, чтобы пользователи в группе получили доступ к файлам в домашнем каталоге. Также меняем директорию `dir1` атрибуты с помощью команды `chmod 000`. Далее проверяем изменения командой `ls -l` (рис. [-@fig:004]).

```
[guest@itmametkadihrov ~]$ chmod g+rwX /home/guest
[guest@itmametkadihrov ~]$ chmod 000 /home/guest/dir1
[guest@itmametkadihrov ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 16 22:58 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 Документы
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 Изображения
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 Музыка
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 16 22:47 Шаблоны
[guest@itmametkadihrov ~]$
```

Figure 0.4: Смена атрибутов

Далее изучим, как влияют различные комбинации атрибутов файлов и директории на различные действия. Будем менять атрибуты файлов от имени пользователя guest командой `chmod`. А от имени пользователя guest2 будем пытаться создать файл командой `touch`, удалить его командой `rm`, записать в файл командой `echo >`, прочитать файл командой `cat`, сменить директорию командой `cd`, просмотреть директорию командой `ls`, переименовать файл командой `rename` и сменить атрибуты командой `chattr`.

В случае успеха будет записывать `+`, в случае ошибки доступа будем записывать `-`. Соберём данные в таблицу [-@tbl:std-dir-2].

Table 0.1: Установленные права и разрешённые действия {#tbl:std-dir-2}

		Запись					Просмотр		Смена	
Права	Права	Создание	Удаление	Запись	Чтение	Смена	в	Переименование	атрибутов	атрибутов
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла	файла
d (000)	(000)	-	-	-	-	-	-	-	-	-
d -x (010)	(000)	-	-	-	-	+	-	-	-	-

		Просмотр							
		Запись				файлов		Смена	
Права	Права	Создание	Удаление	Чтение	Смена	в	Переименование	исполнение	исполнение
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла
d -w-	(000)	-	-	-	-	-	-	-	-
(020)									
d -wx	(000)	+	+	-	-	+	-	+	-
(030)									
d r-	(000)	-	-	-	-	-	+	-	-
(040)									
d r-x	(000)	-	-	-	-	+	+	-	-
(050)									
d rw-	(000)	-	-	-	-	-	+	-	-
(060)									
d rwx	(000)	+	+	-	-	+	+	+	-
(070)									
d (000)	-x	-	-	-	-	-	-	-	-
	(100)								
d -x	-x	-	-	-	-	+	-	-	-
(010)	(010)								
d -w-	-x	-	-	-	-	-	-	-	-
(020)	(010)								
d -wx	-x	+	+	-	-	+	-	+	-
(030)	(010)								
d r-	-x	-	-	-	-	-	+	-	-
(040)	(010)								
d r-x	-x	-	-	-	-	+	+	-	-
(050)	(010)								

		Просмотр							
		Запись				файлов		Смена	
Права	Права	Создание	Удаление	Чтение	Смена	в	Переименование	исполнение	исполнение
директории	файла	файла	файла	файла	файла	директории	директории	файла	файла
d rw-	-x	-	-	-	-	+	-	-	-
(060)	(010)								
d rwx	-x	+	+	-	-	+	+	+	-
(070)	(010)								
d (000)	-w-	-	-	-	-	-	-	-	-
	(020)								
d -x	-w-	-	-	+	-	+	-	-	-
(010)	(020)								
d -w-	-w-	-	-	-	-	-	-	-	-
(020)	(020)								
d -wx	-w-	+	+	+	-	+	-	+	-
(030)	(020)								
d r-	-w-	-	-	-	-	-	+	-	-
(040)	(020)								
d r-x	-w-	-	-	+	-	+	+	-	-
(050)	(020)								
d rw-	-w-	-	-	-	-	-	+	-	-
(060)	(020)								
d rwx	-w-	+	+	+	-	+	+	+	-
(070)	(020)								
d (000)	-wx	-	-	-	-	-	-	-	-
	(030)								
d -x	-wx	-	-	+	-	+	-	-	-
(010)	(030)								

		Просмотр							
		Запись				файлов		Смена	
Права	Права	Создание	Удаление	Чтение	Смена	в	Переименование	исполнение	исполнение
директории	файла	файла	файла	файла	файла	директории	директории	файла	файла
d -w-	-wx	-	-	-	-	-	-	-	-
(020)	(030)								
d -wx	-wx	+	+	+	-	+	-	+	-
(030)	(030)								
d r-	-wx	-	-	-	-	-	+	-	-
(040)	(030)								
d r-x	-wx	-	-	+	-	+	+	-	-
(050)	(030)								
d rw-	-wx	-	-	-	-	-	+	-	-
(060)	(030)								
d rwx	-wx	+	+	+	-	+	+	+	-
(070)	(030)								
d (000)	r-	-	-	-	-	-	-	-	-
	(040)								
d -x	r-	-	-	-	+	+	-	-	-
(010)	(040)								
d -w-	r-	-	-	-	-	-	-	-	-
(020)	(040)								
d -wx	r-	+	+	-	+	+	-	+	-
(030)	(040)								
d r-	r-	-	-	-	-	-	+	-	-
(040)	(040)								
d r-x	r-	-	-	-	+	+	+	-	-
(050)	(040)								

		Запись				Просмотр			
Права	Права	Создание	Удаление	Чтение	Смена	Просмотр	Смена	Переименование	Проверка
директории	файла	файла	файла	файла	файла	директории	директории	файла	файла
d rw-	r-	-	-	-	-	-	+	-	-
(060)	(040)								
d rwx	r-	+	+	-	+	+	+	+	-
(070)	(040)								
d (000)	r-x	-	-	-	-	-	-	-	-
	(050)								
d -x	r-x	-	-	-	+	+	-	-	-
(010)	(050)								
d -w-	r-x	-	-	-	-	-	-	-	-
(020)	(050)								
d -wx	r-x	+	+	-	+	+	-	+	-
(030)	(050)								
d r-	r-x	-	-	-	-	-	+	-	-
(040)	(050)								
d r-x	r-x	-	-	-	+	+	+	-	-
(050)	(050)								
d rw-	r-x	-	-	-	-	-	+	-	-
(060)	(050)								
d rwx	r-x	+	+	-	+	+	+	+	-
(070)	(050)								
d (000)	rw-	-	-	-	-	-	-	-	-
	(060)								
d -x	rw-	-	-	+	+	+	-	-	-
(010)	(060)								

		Запись					Просмотр		
Права	Права	Создание	Удаление	Чтение	Смена	в	Просмотр	Смена	Смена
директории	файла	файла	файла	файла	файла	директории	директории	файла	файла
d -w-	rw-	-	-	-	-	-	-	-	-
(020)	(060)								
d -wx	rw-	+	+	+	+	+	-	+	-
(030)	(060)								
d r-	rw-	-	-	-	-	-	+	-	-
(040)	(060)								
d r-x	rw-	-	-	+	+	+	+	-	-
(050)	(060)								
d rw-	rw-	-	-	-	-	-	+	-	-
(060)	(060)								
d rwx	rw-	+	+	+	+	+	+	+	-
(070)	(060)								
d (000)	rwX	-	-	-	-	-	-	-	-
	(070)								
d -x	rwX	-	-	+	+	+	-	-	-
(010)	(070)								
d -w-	rwX	-	-	-	-	-	-	-	-
(020)	(070)								
d -wx	rwX	+	+	+	+	+	-	+	-
(030)	(070)								
d r-	rwX	-	-	-	-	-	+	-	-
(040)	(070)								
d r-x	rwX	-	-	+	+	+	+	-	-
(050)	(070)								

						Просмотр			
		Запись				файлов		Смена	
Права	Права	Создание	Удаление	Чтение	Смена	в	Переименование	атрибутов	
директории	файла	файла	файла	файл	файла	директории	директории	файла	файла
d rw-	rwX	-	-	-	-	-	+	-	-
(060)	(070)								
d rwX	rwX	+	+	+	+	+	+	+	-
(070)	(070)								

В сравнении с таблицей из Лабораторной работы №2 мы видим, что изменилась только возможность изменять атрибуты файлов. Это связано с тем, что во всех комбинациях стоит 0 в начале, что означает отсутствие прав у владельца файла и директории. Остальные же действия доступны как владельцу, так и членам группы, в равной степени при должной конфигурации прав.

На основании этой таблицы создадим другую, в которой опишем минимальные требования на права и директорию для выполнения тех или иных действий. Внесём проанализированные данные в таблицу [-@tbl:std-dir1].

Table 0.2: Минимальные права для совершения операций {#tbl:std-dir1}

Операция	Минимальные права на директорию	Минимальные права на файл
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

Приобрели практические навыки работы с атрибутами директорий и файлов в группе пользователей через консоль, выяснили минимальные требования и права для совершения различных действий над файлами и директориями.

Список литературы

- 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>
- Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
- Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.
- Введение в информационную безопасность. Типы уязвимостей. (Д.Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Вводная лекция. Сетевая безопасность. Стек протоколов TCP/IP. (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Системы обнаружения и фильтрации компьютерных атак (IDS/IPS). (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Контроль нормального поведения приложений. Security Enhanced Linux (SELinux) (В. Сахаров, МГУ)