

# **Отчет по лабораторной работе №3**

**Основы информационной безопасности**

Федоров Андрей Андреевич, НБИбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
4.1	Заполнение таблицы 3.1 . . . . .	12
4.2	Заполнение таблицы 3.2 . . . . .	19
<b>5</b>	<b>Выводы</b>	<b>21</b>
<b>6</b>	<b>Список литературы. Библиография</b>	<b>22</b>

## Список иллюстраций

4.1	Создание пользователя . . . . .	9
4.2	Добавление пользователя в группу . . . . .	9
4.3	Вход в терминал от имени другого пользователя . . . . .	10
4.4	Текущая директория для guest . . . . .	10
4.5	Текущая директория для guest2 . . . . .	10
4.6	Информация о пользователе guest2 . . . . .	11
4.7	Информация о пользователе guest . . . . .	11
4.8	Содержимое файла etc/group . . . . .	11
4.9	Регистрация пользователя в группе . . . . .	12
4.10	Изменение прав директории . . . . .	12
4.11	Изменение прав директории . . . . .	12
4.12	Пример заполнения таблицы 3.1 . . . . .	13

## **Список таблиц**

# 1 Цель работы

Получить практические навыки работы в консоли с атрибутами файлов для групп пользователей.

## 2 Задание

1. Создание пользователя guest2, добавление его в группу пользователей guest
2. Заполнение таблицы 3.1
3. Заполнение таблицы 3.2 на основе таблицы 3.1.

### 3 Теоретическое введение

**Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [1]

**Группы пользователей Linux** кроме стандартных root и users, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен. [2]

- daemon - от имени этой группы и пользователя daemon запускаются сервисы, которым необходима возможность записи файлов на диск.
- sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
- sync - позволяет выполнять команду /bin/sync
- games - разрешает играм записывать свои файлы настроек и историю в определенную папку
- man - позволяет добавлять страницы в директорию /var/cache/man
- lp - позволяет использовать устройства параллельных портов
- mail - позволяет записывать данные в почтовые ящики /var/mail/

- `proxy` - используется прокси серверами, нет доступа записи файлов на диск
- `www-data` - с этой группой запускается веб-сервер, она дает доступ на запись `/var/www`, где находятся файлы веб-документов
- `list` - позволяет просматривать сообщения в `/var/mail`
- `nogroup` - используется для процессов, которые не могут создавать файлов на жестком диске, а только читать, обычно применяется вместе с пользователем `nobody`.
- `adm` - позволяет читать логи из директории `/var/log`
- `tty` - все устройства `/dev/vcsa` разрешают доступ на чтение и запись пользователям из этой группы
- `disk` - открывает доступ к жестким дискам `/dev/sd*` `/dev/hd*`, можно сказать, что это аналог `root` доступа.
- `dialout` - полный доступ к серийному порту
- `cdrom` - доступ к CD-ROM
- `wheel` - позволяет запускать утилиту `sudo` для повышения привилегий
- `audio` - управление аудиодрайвером
- `src` - полный доступ к исходникам в каталоге `/usr/src/`
- `shadow` - разрешает чтение файла `/etc/shadow`
- `utmp` - разрешает запись в файлы `/var/log/utmp` `/var/log/wtmp`
- `video` - позволяет работать с видеодрайвером
- `plugdev` - позволяет монтировать внешние устройства USB, CD и т.д.
- `staff` - разрешает запись в папку `/usr/local`



## 4 Выполнение лабораторной работы

1. Пользователь guest был создан в лабораторной работе №2, поэтому в этой лабораторной работе его не создаем заново
2. Пароль для пользователя guest тоже был задан в лабораторной работе №2.
3. С правами администратора создаю пользователя guest с помощью команды `useradd`, далее с помощью команды `passwd` задаю пароль пользователю (рис. 1).

```
[afedorov@localhost ~]$ sudo useradd guest2
[sudo] пароль для afedorov:
Попробуйте ещё раз.
[sudo] пароль для afedorov:
[afedorov@localhost ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
passwd: ошибка при операциях с маркером проверки подлинности
[afedorov@localhost ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Рис. 4.1: Создание пользователя

4. Добавляю пользователя guest2 в группу guest (рис. 2).

```
[afedorov@localhost ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
```

Рис. 4.2: Добавление пользователя в группу

5. Зашёл на двух разных консолях от имени двух разных пользователей с помощью команды `su <имя пользователя>` (рис. 3).



Рис. 4.3: Вход в терминал от имени другого пользователя

6. Проверяю путь директории, в которой я нахожусь с помощью `pwd`.

Проверка для пользователя `guest` (рис. 4).

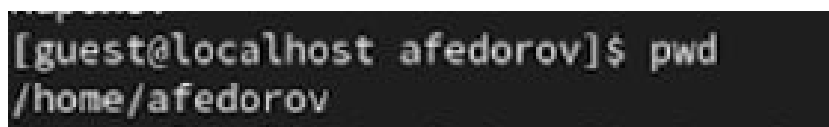


Рис. 4.4: Текущая директория для `guest`

Проверка для пользователя `guest2` (рис. 5).

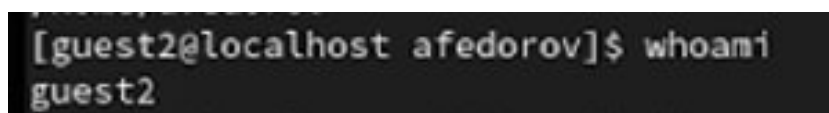


Рис. 4.5: Текущая директория для `guest2`

Стоит отметить, что вход в терминал от имени пользователей был выполнен в домашней директории пользователя `evdvorkina`, которую команда `pwd` вывела. Домашней директорией пользователей она не является. Текущая директория с приглашением командной строки совпадает.

7. Проверяю имя пользователей с помощью команды `whoami`, с помощью команды `id` могу увидеть группы, к которым принадлежит пользователь и коды этих групп (`gid`), команда `groups` просто выведет список групп, в которые входит пользователь.

`id -Gn` - выведет названия групп, которым принадлежит пользователь

`id -G` - выведет только код групп, которым принадлежит пользователь.

Проверка для пользователя `guest2` (рис. 6).

```
[guest2@localhost afedorov]$ whoami
guest2
[guest2@localhost afedorov]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@localhost afedorov]$ groups
guest2 guest
[guest2@localhost afedorov]$ id -Gn
guest2 guest
[guest2@localhost afedorov]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@localhost afedorov]$ id -G
1002 1001
```

Рис. 4.6: Информация о пользователе guest2

Проверка для пользователя guest (рис. 7).

```
[guest@localhost afedorov]$ whoami
guest
[guest@localhost afedorov]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost afedorov]$ group guest2
bash: group: команда не найдена...
[guest@localhost afedorov]$ groups guest2
guest2 : guest2 guest
[guest@localhost afedorov]$ groups
guest
[guest@localhost afedorov]$ id -Gn
guest
[guest@localhost afedorov]$ id -G
1001
```

Рис. 4.7: Информация о пользователе guest

Пользователь guest2 входит в две группы пользователей: в группу guest, потому что я сама его туда добавила, и в группу guest2, которая создавалась автоматически при создании пользователя.

8. Вывел интересное меня содержимое файла etc/group, видно, что в группе guest два пользователя, а в группе guest2 один (рис. 8).

```
[guest2@localhost afedorov]$ cat /etc/group | grep "guest"
guest:x:1001:guest2
guest2:x:1002:
```

Рис. 4.8: Содержимое файла etc/group

9. От имени пользователя guest2 регистрирую его в группе guest с помощью команды newgrp (рис. 9).

```
[guest2@localhost afedorov]$ newgrp guest
[guest2@localhost afedorov]$ pwd
/home/afedorov
[guest2@localhost afedorov]$ chmod g+rx /home/guest
chmod: изменение прав доступа для '/home/guest': операция не позволена
```

Рис. 4.9: Регистрация пользователя в группе

10. Добавляю права на чтение, запись и исполнение группе пользователей guest (guest, guest2) на директорию home/guest в которой находятся все файлы для последующей работы (рис. 10).

```
[guest@localhost afedorov]$ chmod g+rx /home/guest
[guest@localhost afedorov]$ ls
```

Рис. 4.10: Изменение прав директории

11. От имени пользователя guest снимаю все атрибуты с директории dir1, созданной в предыдущей лабораторной работе. Проверяю, что права действительно сняты (рис. 11).

```
[guest@localhost afedorov]$ cd
[guest@localhost ~]$ ls
dir1  Видео  Загрузки  Музыка  'Рабочий стол'
test  Документы  Изображения  Общедоступные  Шаблоны
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls
dir1  Видео  Загрузки  Музыка  'Рабочий стол'
test  Документы  Изображения  Общедоступные  Шаблоны
[guest@localhost ~]$ ls -l
итого 4
d-----, 3 guest guest 18 июн 17 21:33 dir1
```

Рис. 4.11: Изменение прав директории

## 4.1 Заполнение таблицы 3.1

Далее проверяю как пользователь guest2 будет взаимодействовать с файлами в этой директории (рис. 12).

```
[guest@localhost guest2]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@localhost guest2]$ ls dir1
ls: невозможно получить доступ к 'dir1': Отказано в доступе
[guest@localhost guest2]$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
[guest@localhost guest2]$ chmod 020 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@localhost guest2]$
```

Рис. 4.12: Пример заполнения таблицы 3.1

Права директории	Права файла	Права на файлах							
		Создание файлов	Удаление файлов	Запись в файл	Чтение файлов	Смещение рекордов	Смещение рекордов	Печать на бумагу	Смещение атрибутов
d-----	(000)	-	-	-	-	-	-	-	-
(000)	(000)								
d-----x--	(000)	-	-	-	-	-	-	-	+
(010)	(000)								
d----w---	(000)	-	-	-	-	-	-	-	-
(020)	(000)								
d----wx--	(000)	+	+	-	-	+	-	+	+
(030)	(000)								
d---r----	(000)	-	-	-	-	-	+	-	-
(040)	(000)								
d---r-x--	(000)	-	-	-	-	+	+	-	+
(050)	(000)								
d---rw---	(000)	-	-	-	-	-	+	-	-
(060)	(000)								

		Права							
		Сме- на ат-	Про- смотр ре-	Сме- лов ди-	Уда- За- Чте- на ди-	Со- зда- ние фай-	ла	Прав а фай ла	Прав а фай ла
Права директории	Права файла	ри- бу- тов фай-	име- но- ва- ние файл	рек- рек- то- рии	фа- йл ла	фа- йл ла	фа- йл ла	фа- йл ла	фа- йл ла
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)	-	-	-	-	-	-	-	-

		Права							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Пе- ре- име- но- вание файл	Сме- на ат- ри- бу- тов фай- ла
Права директории	Права файла								
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)	-	-	-	-	-	-	-	-

		Про- смотр фай- Пе- на Сме- лов ре- ат- на в име- ри- ди- ди- но- бу- рек- рек- ва- тов фай- фай- в фай- то- то- ние фай-							
Права директории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- ди- рек- то- рии	на в ди- рек- то- рии	име- но- ва- ние файл	ри- бу- тов фай- ла
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)	-	-	-	-	-	+	-	-



		Про- смотр фай- Пе- на Сме- лов ре- ат- на в име- ри- ди- ди- но- бу- рек- рек- ва- тов фай- фай- ла ла файл ла рии рии файл ла							
Права директории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	на ди- рек- то- рии	в ди- рек- то- рии	име- но- ва- ние файл	ри- бу- тов фай- ла
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)	-	-	-	-	-	+	-	-

		Про- смотр фай- Пе- на Сме- лов ре- ат- на в име- ри- ди- ди- но- бу- рек- рек- ва- тов фай- фай- ла ла файл ла рии рии файл ла							
Права директории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- ди- рек- то- рии	на ди- рек- то- рии	име- но- ва- ние файл	ри- бу- тов фай- ла
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)	-	-	-	-	-	-	-	-

Права директории	Права файла	<div> <div>Про- смотр фай-</div> <div>Сме- на ре- ат-</div> <div>Сме- лов ре- ва-</div> <div>на в име- но- бу-</div> <div>на ди- рек-</div> <div>ди- рек-</div> <div>Чте- ние фай-</div> <div>За- пись в файл</div> <div>Уда- ле- ние фай-</div> <div>Со- зда- ние фай-</div> </div>							
		ла	ла	файл	ла	рии	рии	файл	ла
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)								
d---rw---	----rwx--	-	-	-	-	-	+	-	-
(060)	(070)								
d---rwx--	----rwx--	+	+	+	+	+	+	+	+
(070)	(070)								

Таблица 3.1 «Установленные права и разрешённые действия для групп»

## 4.2 Заполнение таблицы 3.2

На основе таблицы 3.1 заполняю таблицу 3.2.

Операция	Права на директорию	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)

Таблица 3.2 «Минимальные права для совершения операций от имени пользователей входящих в группу»

## 5 Выводы

Были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей

## 6 Список литературы. Библиография

[0] Методические материалы курса

[1] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>

[2] Группы пользователей: [https://losst.pro/gruppy-polzovatelej-linux#Что\\_такое\\_группы](https://losst.pro/gruppy-polzovatelej-linux#Что_такое_группы)