

Отчет по лабораторной работе №3

Информационная безопасность

Астафьева Анна Андреевна НПИбд-01-18

Содержание

1	Цель работы	5
2	Теоретические сведения	6
3	Выполнение лабораторной работы	8
4	Выводы	20

List of Tables

3.1	Установленные права и разрешённые действия для группы	13
3.2	Минимальные права для совершения операций от имени пользо- вателей входящих в группу	19

List of Figures

3.1	Создание учетной записи пользователя guest2, создание пароля .	8
3.2	Добавление пользователя guest2 в группу guest	8
3.3	Вход в систему, определение директории для guest	9
3.4	Вход в систему, определение директории для guest2	10
3.5	Уточнение информации о пользователе guest	10
3.6	Уточнение информации о пользователе guest2	11
3.7	Просмотр файла /etc/group	11
3.8	Регистрация пользователя	12
3.9	Изменение прав директории /home/guest	12
3.10	Снятие атрибутов с директории /home/guest/dir1	12
3.11	Проверка правильности снятия атрибутов	12

1 Цель работы

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

2 Теоретические сведения

Поскольку система Linux с самого начала разрабатывалась как многопользовательская система, в ней предусмотрен такой механизм, как права доступа к файлам и каталогам. Он позволяет разграничить полномочия пользователей, работающих в системе. В частности, права доступа позволяют отдельным пользователям иметь «личные» файлы и каталоги. Например, если пользователь `iegebrial` создал в своём домашнем каталоге файлы, то он является владельцем этих файлов и может определить права доступа к ним для себя и остальных пользователей. Он может, например, полностью закрыть доступ к своим файлам для остальных пользователей, или разрешить им читать свои файлы, запретив изменять и исполнять их.

У любого файла в системе есть владелец — один из пользователей. Однако каждый файл одновременно принадлежит и некоторой группе пользователей системы. Каждый пользователь может входить в любое количество групп, и в каждую группу может входить любое количество пользователей из числа определённых в системе.

Когда в системе создаётся новый пользователь, он добавляется по крайней мере в одну группу. В системе ALT Linux 2.4 Master при создании новой учётной записи создаётся специальная группа, имя которой совпадает с именем нового пользователя, и пользователь включается в эту группу. В дальнейшем администратор может добавить пользователя к другим группам.

Механизм групп может применяться для организации совместного доступа нескольких пользователей к определённым ресурсам. Например, на сервере ор-

ганизации для каждого проекта может быть создана отдельная группа, в которую войдут учётные записи (имена пользователей) сотрудников, работающих над этим проектом. При этом файлы, относящиеся к проекту, могут принадлежать этой группе и быть доступными для её членов. В системе также определено несколько групп (например, bin), которые используются для управления доступом системных программ к различным ресурсам. Как правило, членами этих групп являются системные пользователи, пользователи-люди не включаются в такие группы.

Права доступа определяются по отношению к трём типам действий: чтение, запись и исполнение. Эти права доступа могут быть предоставлены трём классам пользователей: владельцу файла (пользователю), группе, которой принадлежит файл, а также всем остальным пользователям, не входящим в эту группу. Право на чтение даёт пользователю возможность читать содержимое файла или, если такой доступ разрешён к каталогам, просматривать содержимое каталога (используя команду ls). Право на запись даёт пользователю возможность записывать или изменять файл, а право на запись для каталога — возможность создавать новые файлы или удалять файлы из этого каталога. Наконец, право на исполнение позволяет пользователю запускать файл как программу или сценарий командной оболочки (разумеется, это действие имеет смысл лишь в том случае, если файл является программой или сценарием). Владение правами на исполнение для каталога позволяет перейти (командой cd) в этот каталог.

Основные команды

Ниже перечислены важнейшие команды для решения задач, связанных с правами доступа.

chmod: Изменение прав доступа к файлу или каталогу.

chown: Изменение владельца файла.

chgroup: Изменение группы, которой принадлежит файл.

umask: определение прав доступа по умолчанию для файлов, создаваемых пользователем.

3 Выполнение лабораторной работы

1. В установленной операционной системе создала учетную запись пользователя guest (используя учетную запись администратора): `useradd guest`. Задала пароль для пользователя guest: `passwd guest`. (Это было выполнено в лабораторной работе №2) Аналогично создала второго пользователя guest2. (рис. 3.1).

```
[root@aaaastafeva ~]# useradd guest
useradd: пользователь «guest» уже существует
[root@aaaastafeva ~]# passwd guest
passwd: неизвестное имя «quest».
[root@aaaastafeva ~]# 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.
[root@aaaastafeva ~]# useradd guest2
[root@aaaastafeva ~]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@aaaastafeva ~]#
```

Figure 3.1: Создание учетной записи пользователя guest2, создание пароля

2. Добавила пользователя guest2 в группу guest: `gpasswd -a guest2 guest` (рис. 3.2).

```
[root@aaaastafeva ~]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@aaaastafeva ~]#
```

Figure 3.2: Добавление пользователя guest2 в группу guest

3. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. Для обоих пользователей командой pwd определила директорию, в которой мы находимся.(рис. 3.3), (рис. 3.4).

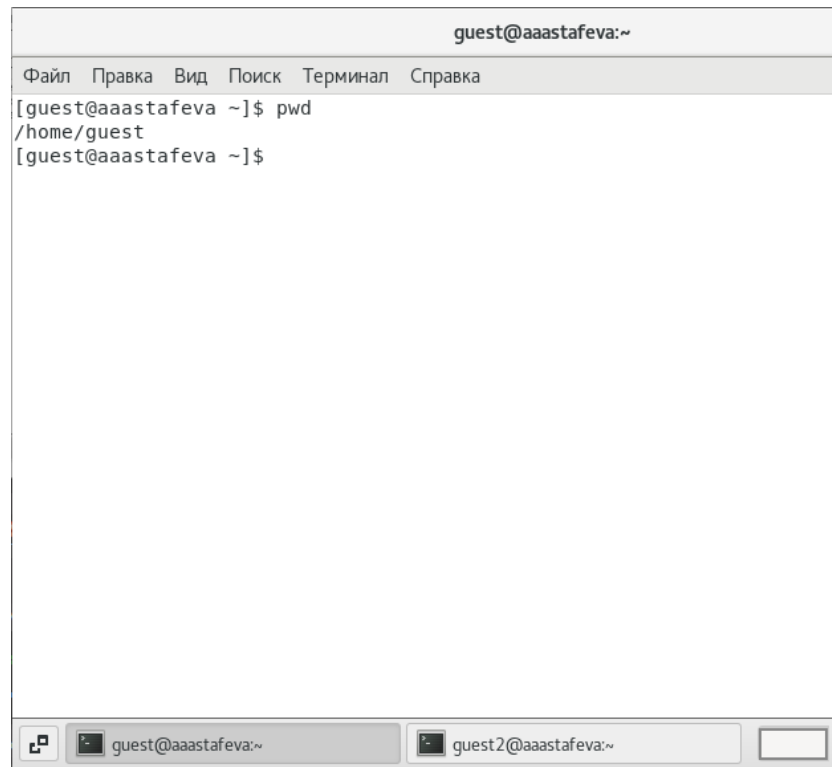


Figure 3.3: Вход в систему, определение директории для guest

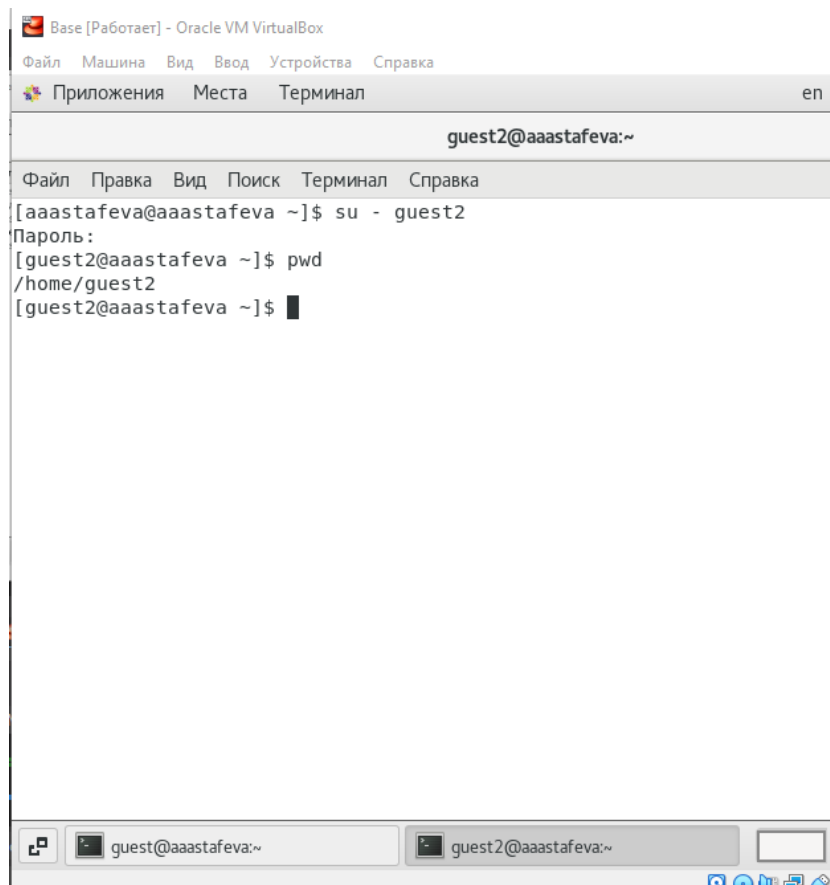


Figure 3.4: Вход в систему, определение директории для guest2

4. Уточнила имя пользователя, его группу, кто входит в нее и к каким группам принадлежит он сам. Определила командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравнила вывод команды `groups` с выводом команд `id -Gn` и `id -G` (Одинаковы)(рис. 3.5), (рис. 3.6).

```

[guest@aaastafeva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined
u:unconfined r:unconfined t:s0-s0:c0.c1023
[guest@aaastafeva ~]$ groups guest
guest : guest
[guest@aaastafeva ~]$ id -Gn
guest
[guest@aaastafeva ~]$ id -G
1001
[guest@aaastafeva ~]$

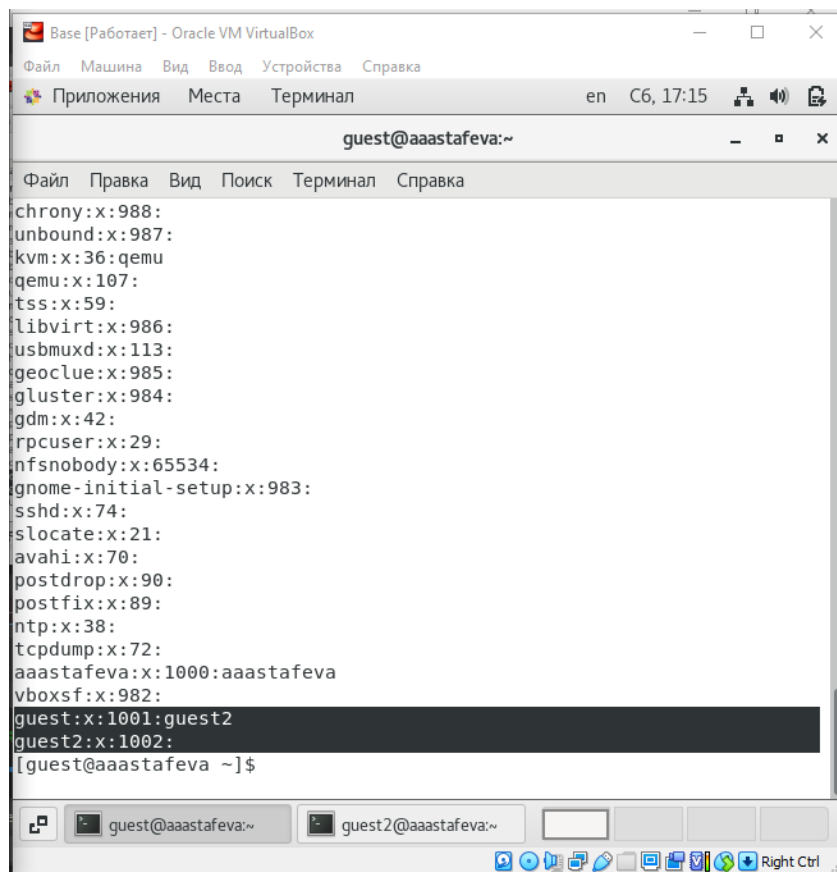
```

Figure 3.5: Уточнение информации о пользователе guest

```
[guest2@aaastafeva ~]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) конт
екст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@aaastafeva ~]$ groups guest2
guest2 : guest2 guest
[guest2@aaastafeva ~]$ id -Gn
guest2 guest
[guest2@aaastafeva ~]$ id -G
1002 1001
[guest2@aaastafeva ~]$
```

Figure 3.6: Уточнение информации о пользователе guest2

5. Сравнила полученную информацию с содержимым файла /etc/group. Просмотрела файл командой cat /etc/group. (рис. 3.7).



```
Base [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  C6, 17:15
guest@aaastafeva:~
Файл  Правка  Вид  Поиск  Терминал  Справка
chorny:x:988:
unbound:x:987:
kvm:x:36:qemu
qemu:x:107:
tss:x:59:
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
gluster:x:984:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
aaastafeva:x:1000:aaastafeva
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
[guest@aaastafeva ~]$
```

Figure 3.7: Просмотр файла /etc/group

6. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest командой: newgrp guest(рис. 3.8).

```
[guest2@aaastafeva ~]$ newgrp guest
[guest2@aaastafeva ~]$
```

Figure 3.8: Регистрация пользователя

7. От имени пользователя guest изменила права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rx /home/guest` (рис. 3.9).

```
[guest@aaastafeva ~]$ chmod g+rx /home/guest
[guest@aaastafeva ~]$
```

Figure 3.9: Изменение прав директории /home/guest

8. От имени пользователя guest сняла с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1`. (рис. 3.10).

```
[guest@aaastafeva ~]$ chmod 000 dir1
```

Figure 3.10: Снятие атрибутов с директории /home/guest/dir1

9. Проверила правильность снятия атрибутов. (рис. 3.11).

```
[guest@aaastafeva ~]$ ls -l
итого 0
d----- . 2 guest guest 19 окт  2 17:13 dir1
[guest@aaastafeva ~]$
```

Figure 3.11: Проверка правильности снятия атрибутов

10. Заполнила таблицу «Установленные права и разрешенные действия для групп», определив, какие операции разрешены, а какие нет. Если операция разрешена, занесла в таблицу знак «+», если не разрешена, знак «-». (см. табл. 3.1)

Table 3.1: Установленные права и разрешённые действия для группы

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d— (000)	— (000)	-	-	-	-	-	-	-	-
d— (000)	-x (010)	-	-	-	-	-	-	-	-
d— (000)	-w- (020)	-	-	-	-	-	-	-	-
d— (000)	-wx (030)	-	-	-	-	-	-	-	-
d— (000)	r— (040)	-	-	-	-	-	-	-	-
d— (000)	r-x (050)	-	-	-	-	-	-	-	-
d— (000)	rw- (060)	-	-	-	-	-	-	-	-
d— (000)	rwX (070)	-	-	-	-	-	-	-	-
d-x (010)	— (000)	-	-	-	-	+	-	-	-
d-x (010)	-x (010)	-	-	-	-	+	-	-	-
d-x (010)	-w- (020)	-	-	+	-	+	-	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-x (010)	-wx (030)	-	-	+	-	+	-	-	-
d-x (010)	r- (040)	-	-	-	+	+	-	-	-
d-x (010)	r-x (050)	-	-	-	+	+	-	-	-
d-x (010)	rw- (060)	-	-	+	+	+	-	-	-
d-x (010)	rwX (070)	-	-	+	+	+	-	-	-
d-w- (020)	— (000)	-	-	-	-	-	-	-	-
d-w- (020)	-x (010)	-	-	-	-	-	-	-	-
d-w- (020)	-w- (020)	-	-	-	-	-	-	-	-
d-w- (020)	-wx (030)	-	-	-	-	-	-	-	-
d-w- (020)	r- (040)	-	-	-	-	-	-	-	-
d-w- (020)	r-x (050)	-	-	-	-	-	-	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d-w- (020)	rw- (060)	-	-	-	-	-	-	-	-
d-w- (020)	rwX (070)	-	-	-	-	-	-	-	-
d-wX (030)	— (000)	+	+	-	-	+	-	+	-
d-wX (030)	-X (010)	+	+	-	-	+	-	+	-
d-wX (030)	-w- (020)	+	+	+	-	+	-	+	-
d-wX (030)	-wX (030)	+	+	+	-	+	-	+	-
d-wX (030)	r- (040)	+	+	-	+	+	-	+	-
d-wX (030)	r-X (050)	+	+	-	+	+	-	+	-
d-wX (030)	rw- (060)	+	+	+	+	+	-	+	-
d-wX (030)	rwX (070)	+	+	+	+	+	-	+	-
dr- (040)	— (000)	-	-	-	-	-	+	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
dr-	-x	-	-	-	-	-	+	-	-
(040)	(010)								
dr-	-w-	-	-	-	-	-	+	-	-
(040)	(020)								
dr-	-wx	-	-	-	-	-	+	-	-
(040)	(030)								
dr-	r-	-	-	-	-	-	+	-	-
(040)	(040)								
dr-	r-x	-	-	-	-	-	+	-	-
(040)	(050)								
dr-	rw-	-	-	-	-	-	+	-	-
(040)	(060)								
dr-	rwX	-	-	-	-	-	+	-	-
(040)	(070)								
dr-x	—	-	-	-	-	+	+	-	-
(050)	(000)								
dr-x	-x	-	-	-	-	+	+	-	-
(050)	(010)								
dr-x	-w-	-	-	+	-	+	+	-	-
(050)	(020)								
dr-x	-wx	-	-	+	-	+	+	-	-
(050)	(030)								

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
dr-x (050)	r— (040)	-	-	-	+	+	+	-	-
dr-x (050)	r-x (050)	-	-	-	+	+	+	-	-
dr-x (050)	rw- (060)	-	-	+	+	+	+	-	-
dr-x (050)	rwX (070)	-	-	+	+	+	+	-	-
drw- (060)	— (000)	-	-	-	-	-	+	-	-
drw- (060)	-x (010)	-	-	-	-	-	+	-	-
drw- (060)	-w- (020)	-	-	-	-	-	+	-	-
drw- (060)	-wX (030)	-	-	-	-	-	+	-	-
drw- (060)	r— (040)	-	-	-	-	-	+	-	-
drw- (060)	r-x (050)	-	-	-	-	-	+	-	-
drw- (060)	rw- (060)	-	-	-	-	-	+	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
drw- (060)	rwx (070)	-	-	-	-	-	+	-	-
drwx (070)	— (000)	+	+	-	-	+	+	+	-
drwx (070)	-x (010)	+	+	-	-	+	+	+	-
drwx (070)	-w- (020)	+	+	+	-	+	+	+	-
drwx (070)	-wx (030)	+	+	+	-	+	+	+	-
drwx (070)	r— (040)	+	+	-	+	+	+	+	-
drwx (070)	r-x (050)	+	+	-	+	+	+	+	-
drwx (070)	rw- (060)	+	+	+	+	+	+	+	-
drwx (070)	rwx (070)	+	+	+	+	+	+	+	-

Можем заметить что таблица из лабораторной работы №2 совпадает с данной таблицей кроме смены файлов атрибута, эта операция не для владельца файла недоступна.

12. На основании заполненной таблицы определила те или иные минималь-

но необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполнила таблицу «Минимальные права для совершения операций от имени пользователей входящих в группу» (см. табл. 3.2).

Table 3.2: Минимальные права для совершения операций от имени пользователей входящих в группу

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

4 Выводы

На основе проделанной работы получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.