

**Отчёт по лабораторной работе №4.
Дискреционное разграничение прав в
Linux. Расширенные атрибуты**

дисциплина: Информационная безопасность

Рыбалко Элина Павловна

Содержание

Цель работы	5
Техническое обеспечение	6
Объект/Предмет исследования	7
Теоретическое введение	8
Выполнение лабораторной работы	9
Вывод	13
Список литературы	14

Список иллюстраций

1	Определение и установка атрибутов	9
2	Установка расширенных атрибутов	10
3	Последовательное выполнение команд	11
4	Последовательное выполнение команд	12

Список таблиц

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

Техническое обеспечение

Лабораторная работа подразумевает наличие на виртуальной машине VirtualBox операционной системы Linux (дистрибутив Rocky или CentOS). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (<http://www.gentoo.ru/>); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: [/afs/dk.sci.pfu.edu.ru/common/files/iso/](http://afs/dk.sci.pfu.edu.ru/common/files/iso/).

Объект/Предмет исследования

Операционная система Linux и расширенные атрибуты.

Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ. *discretion* — чье-либо усмотрение) — предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. [2].

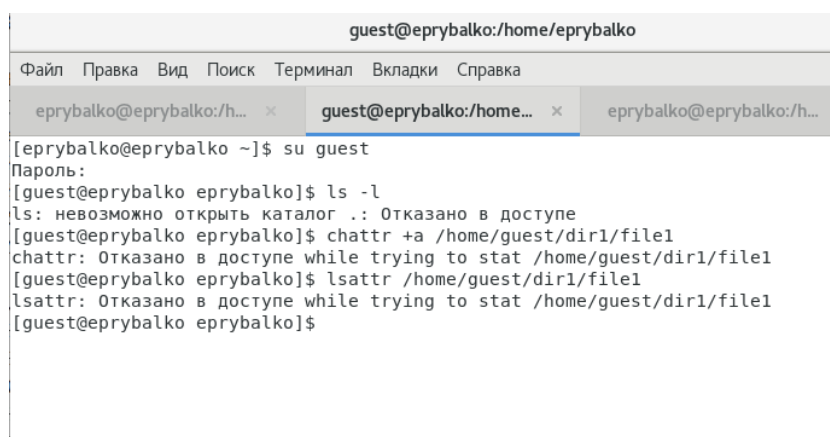
Выполнение лабораторной работы

1. От имени пользователя guest определите расширенные атрибуты файла /home/guest/dir1/file1 командой `lsattr /home/guest/dir1/file1` (см. рис. -@fig:001).
2. Установите командой `chmod 600 file1` на файл file1 права, разрешающие чтение и запись для владельца файла (см. рис. -@fig:001).

```
[root@eprybalko guest]# lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[root@eprybalko guest]# chmod 600 file1
chmod: невозможно получить доступ к «file1»: Нет такого файла или каталога
[root@eprybalko guest]# chmod 600 /home/guest/dir1/file1
[root@eprybalko guest]# █
```

Рис. 1: Определение и установка атрибутов

3. Попробуйте установить на файл /home/guest/dir1/file1 расширенный атрибут а от имени пользователя guest: `chattr +a /home/guest/dir1/file1`. В ответ получили отказ от выполнения операции (см. рис. -@fig:002).

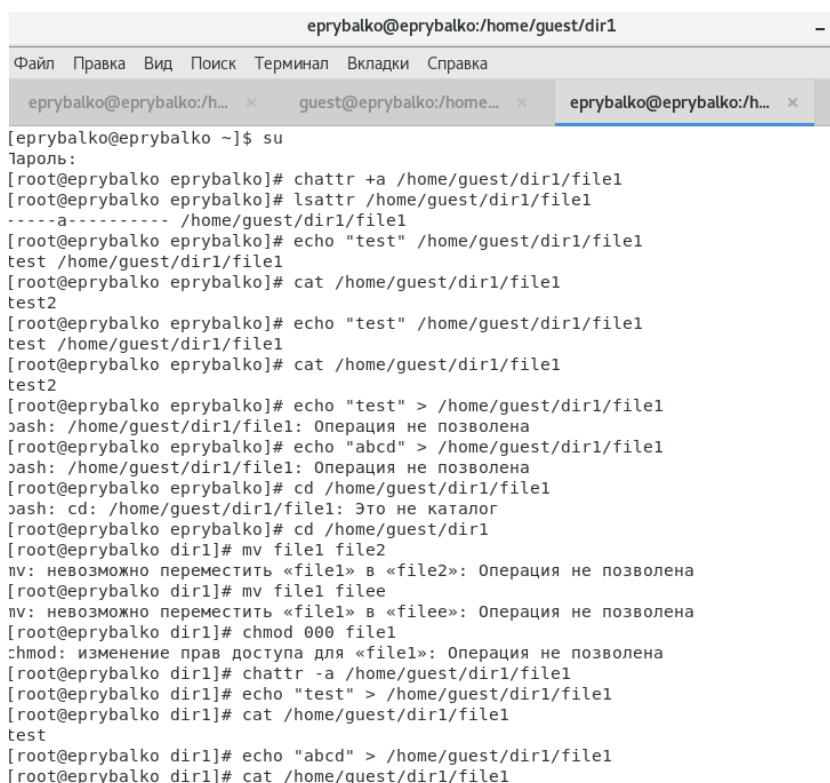


```
guest@eprybalko:/home/eprybalko
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка
eprybalko@eprybalko:/h...  ×  guest@eprybalko:/home...  ×  eprybal...@eprybalko:/h...
[eprybalko@eprybalko ~]$ su guest
Пароль:
[guest@eprybalko eprybalko]$ ls -l
ls: невозможно открыть каталог .: Отказано в доступе
[guest@eprybalko eprybalko]$ chattr +a /home/guest/dir1/file1
chattr: Отказано в доступе while trying to stat /home/guest/dir1/file1
[guest@eprybalko eprybalko]$ lsattr /home/guest/dir1/file1
lsattr: Отказано в доступе while trying to stat /home/guest/dir1/file1
[guest@eprybalko eprybalko]$
```

Рис. 2: Установка расширенных атрибутов

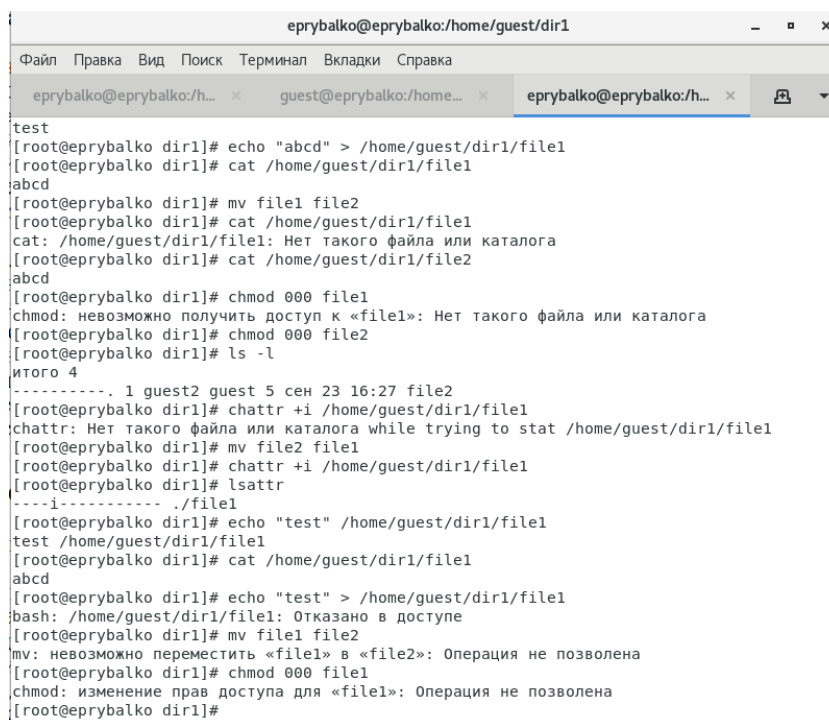
4. Зайдите на третью консоль с правами администратора либо повысьте свои права с помощью команды `su`. Попробуйте установить расширенный атрибут `a` на файл `/home/guest/dir1/file1` от имени суперпользователя: `chattr +a /home/guest/dir1/file1` (см. рис. -@fig:003).
5. От пользователя `guest` проверьте правильность установления атрибута: `lsattr /home/guest/dir1/file1` (см. рис. -@fig:003).
6. Выполните дозапись в файл `file1` слова «test» командой `echo "test" /home/guest/dir1/file1`. После этого выполните чтение файла `file1` командой `cat /home/guest/dir1/file1` (см. рис. -@fig:003).
7. Попробуйте удалить файл `file1` либо стереть имеющуюся в нём информацию командой `echo "abcd" > /home/guest/dir1/file1`. Попробуйте переименовать файл. (см. рис. -@fig:003). Не вышло.
8. Попробуйте с помощью команды `chmod 000 file1` установить на файл `file1` права, например, запрещающие чтение и запись для владельца файла (см. рис. -@fig:003). Удалось ли вам успешно выполнить указанные команды? Не удалось.

9. Снимите расширенный атрибут `a` с файла `/home/guest/dir1/file1` от имени суперпользователя командой `chattr -a /home/guest/dir1/file1` (см. рис. -@fig:003). Повторите операции, которые вам ранее не удавалось выполнить (см. рис. -@fig:003 и рис. -@fig:004).
10. Повторите ваши действия по шагам, заменив атрибут «`a`» атрибутом «`i`». Удалось ли вам дозаписать информацию в файл? (см. рис. -@fig:004). Не удалось.



```
eprybalko@eprybalko:/home/guest/dir1
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка
eprybalko@eprybalko:/h...  x  guest@eprybalko:/home...  x  eprybalko@eprybalko:/h...  x
[eprybalko@eprybalko ~]$ su
Пароль:
[root@eprybalko eprybalko]# chattr +a /home/guest/dir1/file1
[root@eprybalko eprybalko]# lsattr /home/guest/dir1/file1
-----a----- /home/guest/dir1/file1
[root@eprybalko eprybalko]# echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[root@eprybalko eprybalko]# cat /home/guest/dir1/file1
test2
[root@eprybalko eprybalko]# echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[root@eprybalko eprybalko]# cat /home/guest/dir1/file1
test2
[root@eprybalko eprybalko]# echo "test" > /home/guest/dir1/file1
ash: /home/guest/dir1/file1: Операция не позволена
[root@eprybalko eprybalko]# echo "abcd" > /home/guest/dir1/file1
ash: /home/guest/dir1/file1: Операция не позволена
[root@eprybalko eprybalko]# cd /home/guest/dir1/file1
ash: cd: /home/guest/dir1/file1: Это не каталог
[root@eprybalko eprybalko]# cd /home/guest/dir1
[root@eprybalko dir1]# mv file1 file2
mv: невозможно переместить «file1» в «file2»: Операция не позволена
[root@eprybalko dir1]# mv file1 filee
mv: невозможно переместить «file1» в «filee»: Операция не позволена
[root@eprybalko dir1]# chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
[root@eprybalko dir1]# chattr -a /home/guest/dir1/file1
[root@eprybalko dir1]# echo "test" > /home/guest/dir1/file1
[root@eprybalko dir1]# cat /home/guest/dir1/file1
test
[root@eprybalko dir1]# echo "abcd" > /home/guest/dir1/file1
[root@eprybalko dir1]# cat /home/guest/dir1/file1
```

Рис. 3: Последовательное выполнение команд



```
епрыbalko@епрыbalko:/home/guest/dir1
Файл Правка Вид Поиск Терминал Вкладки Справка
епрыbalko@епрыbalko:/h... x guest@епрыbalko:/home... x епрыbalko@епрыbalko:/h... x
test
[root@епрыbalko dir1]# echo "abcd" > /home/guest/dir1/file1
[root@епрыbalko dir1]# cat /home/guest/dir1/file1
abcd
[root@епрыbalko dir1]# mv file1 file2
[root@епрыbalko dir1]# cat /home/guest/dir1/file1
cat: /home/guest/dir1/file1: Нет такого файла или каталога
[root@епрыbalko dir1]# cat /home/guest/dir1/file2
abcd
[root@епрыbalko dir1]# chmod 000 file1
chmod: невозможно получить доступ к «file1»: Нет такого файла или каталога
[root@епрыbalko dir1]# chmod 000 file2
[root@епрыbalko dir1]# ls -l
итого 4
----- 1 guest2 guest 5 сен 23 16:27 file2
[root@епрыbalko dir1]# chattr +i /home/guest/dir1/file1
chattr: Нет такого файла или каталога while trying to stat /home/guest/dir1/file1
[root@епрыbalko dir1]# mv file2 file1
[root@епрыbalko dir1]# chattr +i /home/guest/dir1/file1
[root@епрыbalko dir1]# lsattr
----i----- ./file1
[root@епрыbalko dir1]# echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[root@епрыbalko dir1]# cat /home/guest/dir1/file1
abcd
[root@епрыbalko dir1]# echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[root@епрыbalko dir1]# mv file1 file2
mv: невозможно переместить «file1» в «file2»: Операция не позволена
[root@епрыbalko dir1]# chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
[root@епрыbalko dir1]#
```

Рис. 4: Последовательное выполнение команд

Вывод

Приобрели практические навыки работы в консоли с расширенными атрибутами.

В результате выполнения работы повысили свои навыки использования интерфейса командой строки (CLI), познакомились на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имели возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux. Составили наглядные таблицы, поясняющие какие операции возможны при тех или иных установленных правах. Опробовали действие на практике расширенных атрибутов «а» и «і».

Список литературы

1. Лабораторная работа №4
2. Дискреционное разграничение доступа Linux
3. Руководство по формуле Cmd Markdown
4. Руководство по оформлению Markdown файлов