

Лабораторная работа №3

настройка прав доступа

Кхари жекка кализая арсе

01 января 1970

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

ЦЕЛЬ РАБОТЫ

- Получить навыки о настройке прав доступа для разных пользователей в разных каталогах и файлах

Управление базовыми разрешениями

терминал под пользователем root

The image shows a desktop environment with a terminal window and a web browser. The terminal window, titled 'Terminal', shows a user at the prompt `[qjarishekk@localhost ~]$ su -` entering a password and becoming root, indicated by the prompt `[root@localhost ~]#`. The web browser, titled 'Курс: Основы администр...', displays a document titled '004-permissions.pdf' from the URL `https://esystem.rudn.ru/pluginfile.php/2400`. The document content is in Russian and discusses file permissions.

3.3. Последовательность выполнения работы

Предпосылки: в лабораторной работе № 2 были созданы пользователи `alice` и `bob`, входящие в группу `main`, и пользователь `carol`, входящий в группу `third`.

3.3.1. Управление базовыми разрешениями

Требуется создать структуру каталогов с разными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью `root`:
`su -`
2. В корневом каталоге создайте каталоги `/data/main` и `/data/third`:
`mkdir -p /data/main /data/third`
Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
`ls -Al /data`
3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с `root` на `main` и `third` соответственно:
`chgrp main /data/main`
`chgrp third /data/third`
Посмотрите, кто теперь является владельцем этих каталогов:
`ls -Al /data`
4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
`chmod 770 /data/main`
`chmod 770 /data/third`
Проверьте установленные права доступа.
5. В другом терминале перейдите под учётную запись пользователя `bob`:
`su - bob`
6. Под пользователем `bob` попробуйте перейти в каталог `/data/main` и создать файл `emptyfile` в этом каталоге:

изменение владельцев каталогов

The screenshot shows a Linux desktop environment. On the left is a terminal window titled 'Terminal' with the prompt 'root@localhost:~'. The terminal shows the following commands and output:

```
[qjarishekk@localhost ~]$ su -
Password:
[root@localhost ~]# mkdir -p /data/main /data/third
[root@localhost ~]# ls
anaconda-ks.cfg
[root@localhost ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Sep 18 18:09 main
drwxr-xr-x. 2 root root 6 Sep 18 18:09 third
[root@localhost ~]# chgrp main /data/main
[root@localhost ~]#
[root@localhost ~]# chgrp third /data/third
[root@localhost ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Sep 18 18:09 main
drwxr-xr-x. 2 root third 6 Sep 18 18:09 third
[root@localhost ~]#
```

On the right is a web browser window titled 'Курс: Основы администр...' and '004-permissions.pdf'. The address bar shows 'https://esystem.rudn.ru/pluginfile.php/2400...'. The page content includes:

3.3. Последовательность выполнения работы

Предпосылки: в лабораторной работе № 2 были созданы пользователи *alice* и *bob*, входящие в группу *main*, и пользователь *carol*, входящий в группу *third*.

3.3.1. Управление базовыми разрешениями

Требуется создать структуру каталогов с разными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью *root*:
`su -`
2. В корневом каталоге создайте каталоги `/data/main` и `/data/third`:
`mkdir -p /data/main /data/third`
Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
`ls -Al /data`
3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с *root* на *main* и *third* соответственно:
`chgrp main /data/main`
`chgrp third /data/third`
Посмотрите, кто теперь является владельцем этих каталогов:
`ls -Al /data`
4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
`chmod 770 /data/main`
`chmod 770 /data/third`
Проверьте установленные права доступа.
5. В другом терминале перейдите под учётную запись пользователя *bob*:
`su - bob`
6. Под пользователем *bob* попробуйте перейти в каталог `/data/main` и создать файл `emptyfile` в этом каталоге:

настройка разрешений

команда chmod

The image shows a desktop environment with a terminal window and a web browser. The terminal window, titled 'root@localhost:~', displays the following commands and output:

```
[qjarishekk@localhost ~]$ su -
Password:
[root@localhost ~]# mkdir -p /data/main /data/third
[root@localhost ~]# ls
anaconda-ks.cfg
[root@localhost ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Sep 18 18:09 main
drwxr-xr-x. 2 root root 6 Sep 18 18:09 third
[root@localhost ~]# chgrp main /data/main
[root@localhost ~]#
[root@localhost ~]# chgrp third /data/third
[root@localhost ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root main 6 Sep 18 18:09 main
drwxr-xr-x. 2 root third 6 Sep 18 18:09 third
[root@localhost ~]# chmod 770 /data/main
[root@localhost ~]# chmod 770 /data/third
[root@localhost ~]#
```

The web browser window, titled 'Курс: Основы администр...', shows a PDF document titled '004-permissions.pdf' from the URL <https://esystem.rudn.ru/pluginfile.php/2400>. The document content includes:

Посмотрите, кто является владельцем этих каталогов. Для этого используйте:

```
ls -Al /data
```

3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:

```
chgrp main /data/main
chgrp third /data/third
```

Посмотрите, кто теперь является владельцем этих каталогов:

```
ls -Al /data
```

4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:

```
chmod 770 /data/main
chmod 770 /data/third
```

Проверьте установленные права доступа.

5. В другом терминале перейдите под учётную запись пользователя Bob:

```
su - bob
```

6. Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

```
cd /data/main
touch emptyfile
ls -Al
```

Опишите и поясните результат этого действия.

7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.

Опишите и поясните результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется использовать специальные разрешения для групп пользователей, обеспечить

команда chmod

The image shows a desktop environment with a terminal window and a web browser. The terminal window, titled "Terminal", shows the command `ls -Al /data` being executed, resulting in the following output:

```
total 0
drwxrwx---, 2 root main  6 Sep 18 18:09 main
drwxrwx---, 2 root third 6 Sep 18 18:09 third
[root@localhost ~]#
```

The web browser window, titled "Курс: Основы администр...", shows a PDF document titled "004-permissions.pdf". The document content includes the following steps:

- Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
`ls -Al /data`
- Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно:
`chgrp main /data/main`
`chgrp third /data/third`
- Посмотрите, кто теперь является владельцем этих каталогов:
`ls -Al /data`
- Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
`chmod 770 /data/main`
`chmod 770 /data/third`
- Проверьте установленные права доступа.
- В другом терминале перейдите под учётную запись пользователя Bob:
`su - bob`
- Под пользователем Bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге:

Below the list, the terminal output for the user Bob is shown:

```
cd /data/main
touch emptyfile
ls -Al
```

The document also includes a section titled "3.3.2. Управление специальными разрешениями" and a note about using special permissions for group users.

терминал под пользователем bob

Проверка разрешений доступа

Terminal 1 (root@localhost):

```
[root@localhost ~]# ls -l /data
total 0
drwxrwx---. 2 root main 6 Sep 18 18:09 main
drwxrwx---. 2 root third 6 Sep 18 18:09 third
[root@localhost ~]#
```

Terminal 2 (bob@localhost/data/main):

```
[qjarishekk@localhost ~]$ su - bob
Password:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ ls
[bob@localhost main]$ touch emptyfile
[bob@localhost main]$ ls
emptyfile
[bob@localhost main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ cd /third
-bash: cd: /third: No such file or directory
[bob@localhost main]$ cd /data/third
-bash: cd: /data/third: Permission denied
[bob@localhost main]$
```

Web Browser (https://esystem.rudn.ru/pluginfile.php/2400...):

Лабораторная работа № 3. Настройка прав доступа

```
cd /data/main
touch emptyfile
ls -l
```

Опишите и поясните результат этого действия.

7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Опишите и поясните результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также *sticky bit*.

Sticky bit – дополнительный атрибут файлов или каталогов в ОС типа Linux, применяющийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита *chmod*. Восьмеричное значение *sticky*-бита: 1000, а символическое: *+*t.

1. Откройте новый терминал под пользователем alice.
2. Перейдите в каталог /data/main:

```
cd /data/main
```

Создайте два файла, владельцем которых является alice:

```
touch alice1
touch alice2
```
3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):

```
su - bob
```
4. Перейдите в каталог /data/main:

```
cd /data/main
```

и в этом каталоге введите:

```
ls -l
```

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:

```
rm -f alice*
```

Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:

```
touch bob1
touch bob2
```

Управление специальными разрешениями

терминал под пользователем alice

создание файлов

Terminal 1 (root@localhost):

```
[root@localhost ~]# ls -Al /data
total 0
drwxrwx---. 2 root main 6 Sep 18 18:09 main
drwxrwx---. 2 root third 6 Sep 18 18:09 third
[root@localhost ~]#
```

Terminal 2 (alice@localhost/data/main):

```
[qjarishekk@localhost ~]$ su - alice
Password:
[alice@localhost ~]$ cd /data/main
[alice@localhost main]$ touch alice1
[alice@localhost main]$ touch alice2
[alice@localhost main]$ ls -Al /data/main
total 0
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$
```

Web Browser (https://esystem.rudn.ru/pluginfile.php/2400...):

Опишите и поясните результат этого действия.

7. Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге.

Опишите и поясните результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также *sticky bit*.

Sticky bit – дополнительный атрибут файлов или каталогов в ОС типа Linux, применяющийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита *chmod*. Восьмеричное значение stiky-бита: 1000, а символическое: *+*.

1. Откройте новый терминал под пользователем alice.
2. Перейдите в каталог /data/main:
`cd /data/main`
Создайте два файла, владельцем которых является alice:
`touch alice1`
`touch alice2`
3. В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice):
`su - bob`
4. Перейдите в каталог /data/main:
`cd /data/main`
и в этом каталоге введите:
`ls -l`
Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:
`rm -f alice*`
Убедитесь, что файлы будут удалены пользователем bob.
5. Создайте два файла, которые принадлежат пользователю bob:
`touch bob1`
`touch bob2`
6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы:
`chmod g+s,o+t /data/main`
7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:
`touch alice3`
`touch alice4`

терминал под пользователем bob

удаление файлов пользователя alice

The image shows a Linux desktop environment with two windows. The left window is a terminal with two tabs: 'bob@localhost:/data/main' and 'alice@localhost:/data/main'. The right window is a web browser showing a document titled '004-permissions.pdf' from 'esystem.rudn.ru'.

Terminal Window 1 (bob@localhost:/data/main):

```
[qjarishekk@localhost ~]$ su - bob
Password:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ rm -f alice*
[bob@localhost main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$
```

Terminal Window 2 (alice@localhost:/data/main):

```
[qjarishekk@localhost ~]$ su - alice
Password:
[alice@localhost ~]$ cd /data/main
[alice@localhost main]$ touch alice1
[alice@localhost main]$ touch alice2
[alice@localhost main]$ ls -Al /data/main
total 0
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$
```

Web Browser Window (004-permissions.pdf):

атрибута используется утилита `chmod`. Восьмеричное значение sticky-бита: 1000, а символическое: `+t`.

1. Откройте новый терминал под пользователем `alice`.
2. Перейдите в каталог `/data/main`:
`cd /data/main`
Создайте два файла, владельцем которых является `alice`:
`touch alice1`
`touch alice2`
3. В другом терминале перейдите под учётную запись пользователя `bob` (пользователь `bob` является членом группы `main`, как и `alice`):
`su - bob`
4. Перейдите в каталог `/data/main`:
`cd /data/main`
и в этом каталоге введите:
`ls -l`
Вы увидите два файла, созданные пользователем `alice`. Попробуйте удалить файлы, принадлежащие пользователю `alice`:
`rm -f alice*`
Убедитесь, что файлы будут удалены пользователем `bob`.
5. Создайте два файла, которые принадлежат пользователю `bob`:
`touch bob1`
`touch bob2`
6. В терминале под пользователем `root` установите для каталога `/data/main` бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:
`chmod g+s,o+t /data/main`
7. В терминале под пользователем `alice` создайте в каталоге `/data/main` файлы `alice3` и `alice4`:
`touch alice3`
`touch alice4`
`ls -l`
Теперь вы должны увидеть, что два созданных вами файла принадлежат группе `main`, которая является группой-владельцем каталога `/data/main`.
8. В терминале под пользователем `alice` попробуйте удалить файлы, принадлежащие пользователю `bob`:
`rm -rf bob*`

новые защищенные файлы

The screenshot shows a Linux desktop environment with two windows open. The top window is a terminal titled "bob@localhost:/data/main". The bottom window is a terminal titled "alice@localhost:/data/main". To the right, a web browser window is open, displaying a document titled "004-permissions.pdf" from the URL "https://esystem.rudn.ru/pluginfile.php/2400...". The document contains a list of instructions for a permissions exercise.

Terminal 1 (bob@localhost:/data/main):

```
[qjarishekk@localhost ~]$ su - bob
Password:
[bob@localhost ~]$ cd /data/main
[bob@localhost main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ rm -f alice*
[bob@localhost main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$ touch bob1
[bob@localhost main]$ touch bob2
[bob@localhost main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[bob@localhost main]$
```

Terminal 2 (alice@localhost:/data/main):

```
[qjarishekk@localhost ~]$ su - alice
Password:
[alice@localhost ~]$ cd /data/main
[alice@localhost main]$ touch alice1
[alice@localhost main]$ touch alice2
[alice@localhost main]$ ls -Al /data/main
total 0
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$
```

Web Browser (004-permissions.pdf):

атрибута используется утилита `chmod`. Восьмеричное значение `sticky`-бита: `1000`, а символическое: `+t`.

1. Откройте новый терминал под пользователем `alice`.
2. Перейдите в каталог `/data/main`:
`cd /data/main`
Создайте два файла, владельцем которых является `alice`:
`touch alice1`
`touch alice2`
3. В другом терминале перейдите под учётную запись пользователя `bob` (пользователь `bob` является членом группы `main`, как и `alice`):
`su - bob`
4. Перейдите в каталог `/data/main`:
`cd /data/main`
и в этом каталоге введите:
`ls -l`
Вы увидите два файла, созданные пользователем `alice`. Попробуйте удалить файлы, принадлежащие пользователю `alice`:
`rm -f alice*`
Убедитесь, что файлы будут удалены пользователем `bob`.
5. Создайте два файла, которые принадлежат пользователю `bob`:
`touch bob1`
`touch bob2`
6. В терминале под пользователем `root` установите для каталога `/data/main` бит идентификатора группы, а также `sticky`-бит для разделяемого (общего) каталога группы:
`chmod g+s,o+t /data/main`
7. В терминале под пользователем `alice` создайте в каталоге `/data/main` файлы `alice3` и `alice4`:
`touch alice3`
`touch alice4`
`ls -l`
Теперь вы должны увидеть, что два созданных вами файла принадлежат группе `main`, которая является группой-владельцем каталога `/data/main`.
8. В терминале под пользователем `alice` попробуйте удалить файлы, принадлежащие пользователю `bob`:
`rm -rf bob*`

новые защищенные файлы

Activities Terminal

Sep 18 18:21

en 🔊 🔌

root@localhost:~

```
[root@localhost ~]# ls -Al /data
total 0
drwxrwx---. 2 root main 6 Sep 18 18:09 main
drwxrwx---. 2 root third 6 Sep 18 18:09 third
[root@localhost ~]# chmod g+s,o+t /data/main
[root@localhost ~]#
```

alice@localhost:/data/main

```
[qjarishekk@localhost ~]$ su - alice
Password:
[alice@localhost ~]$ cd /data/main
[alice@localhost main]$ touch alice1
[alice@localhost main]$ touch alice2
[alice@localhost main]$ ls -Al /data/main
total 0
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice1
-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$
```

Kypc: Основы администр: x 004-permissions.pdf x + v x

https://esystem.rudn.ru/pluginfile.php/2400

Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit

2 of 5 - + 140%

ls -l

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:

```
rm -f alice*
```

Убедитесь, что файлы будут удалены пользователем bob.

5. Создайте два файла, которые принадлежат пользователю bob:

```
touch bob1
touch bob2
```

6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:

```
chmod g+s,o+t /data/main
```

7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:

```
touch alice3
touch alice4
ls -l
```

Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.

8. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob:

```
rm -rf bob*
```

Кулаков Д. С., Королькова А. В. Основы администрирования операционных систем 29

Убедитесь, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов. Обратите внимание: поскольку пользователь alice является владельцем каталога /data/main, то он может удалить все свои файлы в любом случае.

3.3.3. Управление расширенными разрешениями с использованием списков ACL

новые созданные файлы пользователем alice

Activities

Terminal

Sep 18 18:22

en

🔊 🔌

root@localhost:~

ls -Al /data

total 0

drwxrwx---. 2 root main 6 Sep 18 18:09 main

drwxrwx---. 2 root third 6 Sep 18 18:09 third

[root@localhost ~]# chmod g+s,o+t /data/main

[root@localhost ~]#

alice@localhost:/data/main

touch alice1

touch alice2

ls -Al /data/main

total 0

-rw-r--r--. 1 alice alice 0 Sep 18 18:18 alice1

-rw-r--r--. 1 alice alice 0 Sep 18 18:22 alice2

-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile

[alice@localhost main]# touch alice3

[alice@localhost main]# touch alice4

[alice@localhost main]# ls

alice3 alice4 bob1 bob2 emptyfile

[alice@localhost main]# ls -l

total 0

-rw-r--r--. 1 alice main 0 Sep 18 18:21 alice3

-rw-r--r--. 1 alice main 0 Sep 18 18:22 alice4

-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1

-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2

-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile

[alice@localhost main]#

Kyrc: Основы администр: x 004-permissions.pdf x + v x

https://esystem.rudn.ru/pluginfile.php/2400

Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit

2 of 5 - + 140%

ls -l

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:

rm -f alice*

Убедитесь, что файлы будут удалены пользователем bob.

5. Создайте два файла, которые принадлежат пользователю bob:

touch bob1

touch bob2

6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы:

chmod g+s,o+t /data/main

7. В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4:

touch alice3

touch alice4

ls -l

Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.

8. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob:

rm -rf bob*

Кулабов Д. С., Королькова А. В. Основы администрирования операционных систем 29

Убедитесь, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов. Обратите внимание: поскольку пользователь alice является владельцем каталога /data/main, то он может удалить все свои файлы в любом случае.

3.3.3. Управление расширенными разрешениями с использованием списков ACL

Показ атрибута sticky bit

The screenshot displays a Linux desktop environment. On the left, a terminal window is open, showing a root user at a localhost. The user has switched to the 'alice' user and navigated to the '/data/main' directory. They have listed the directory contents, showing files 'alice3', 'alice4', 'bob1', and 'bob2' owned by 'bob'. Attempts to remove 'bob1' and 'bob2' failed with the message 'Operation not permitted', demonstrating the effect of the sticky bit. On the right, a web browser window is open, displaying a page from 'https://esystem.rudn.ru/pluginfile.php/2400'. The page contains instructions in Russian for setting and removing ACLs using 'setfacl' and 'getfacl' commands, and a list of tasks for a lab work.

```
[root@localhost ~]#  
[alice@localhost main]$ ls -l  
total 0  
-rw-r--r--. 1 alice main 0 Sep 18 18:21 alice3  
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alice4  
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1  
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2  
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile  
[alice@localhost main]$ rm -rf bob*  
rm: cannot remove 'bob1': Operation not permitted  
rm: cannot remove 'bob2': Operation not permitted  
[alice@localhost main]$
```

установить разрешения для группы:
setfacl -m "g:group:permissions" <file/dir>
Наследование записи ACL родительского каталога:
setfacl -dm "entry" <dir>
Удаление записи ACL:
setfacl -x "entry" <file/dir>
Синтаксис команды getfacl:
getfacl <file/dir>
Применим команды setfacl и getfacl для выполнения поставленной задачи.

1. Откройте терминал с учётной записью root
su -
2. Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third:
setfacl -m g:third:rx /data/main
setfacl -m g:main:rx /data/third
3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:
getfacl /data/main
getfacl /data/third
4. Создайте новый файл с именем newfile1 в каталоге /data/main:
touch /data/main/newfile1
Используйте
getfacl /data/main/newfile1
для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему.
Выполните аналогичные действия для каталога /data/third. Дайте пояснения.
5. Установите ACL по умолчанию для каталога /data/main:
setfacl -m d:g:third:rxw /data/main
6. Добавьте ACL по умолчанию для каталога /data/third:
setfacl -m d:g:main:rxw /data/third
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:
touch /data/main/newfile2

Управление расширенными разрешениями с использованием списков ACL

Команда setfacl

The screenshot shows a Linux desktop environment with two windows open.

Terminal Window (Top):

```
root@localhost:~  
[root@localhost ~]# setfacl -m g:third:rx /data/main  
[root@localhost ~]# setfacl -m g:main:rx /data/third  
[root@localhost ~]#
```

Terminal Window (Bottom):

```
alice@localhost:/data/main  
[alice@localhost main]$ ls -l  
total 0  
-rw-r--r--. 1 alice main 0 Sep 18 18:21 alice3  
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alice4  
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1  
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2  
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile  
[alice@localhost main]$ rm -rf bob.  
rm: cannot remove 'bob1': Operation not permitted  
rm: cannot remove 'bob2': Operation not permitted  
[alice@localhost main]$
```

Web Browser Window:

The browser shows a page from <https://esystem.rudn.ru/pluginfile.php/2400/>. The page content includes instructions for using the `setfacl` and `getfacl` commands.

Page Content:

установить разрешения для группы:
`setfacl -m "g:group:permissions" <file/dir>`
Наследование записи ACL родительского каталога:
`setfacl -dm "entry" <dir>`
Удаление записи ACL:
`setfacl -x "entry" <file/dir>`
Синтаксис команды `getfacl`:
`getfacl <file/dir>`
Применим команды `setfacl` и `getfacl` для выполнения поставленной задачи.

1. Откройте терминал с учётной записью `root`
`su -`
2. Установите права на чтение и выполнение в каталоге `/data/main` для группы `third` и права на чтение и выполнение для группы `main` в каталоге `/data/third`:
`setfacl -m g:third:rx /data/main`
`setfacl -m g:main:rx /data/third`
3. Используйте команду `getfacl`, чтобы убедиться в правильности установки разрешений:
`getfacl /data/main`
`getfacl /data/third`
4. Создайте новый файл с именем `newfile1` в каталоге `/data/main`:
`touch /data/main/newfile1`
Используйте
`getfacl /data/main/newfile1`
для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему.
Выполните аналогичные действия для каталога `/data/third`. Дайте пояснения.
5. Установите ACL по умолчанию для каталога `/data/main`:
`setfacl -m d:g:third:rxw /data/main`
6. Добавьте ACL по умолчанию для каталога `/data/third`:
`setfacl -m d:g:main:rxw /data/third`
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог `/data/main`:
`touch /data/main/newfile2`

команда getfacl

The screenshot shows a Linux desktop environment with a terminal window and a web browser.

Terminal Window (root@localhost):

```
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other::---
```

```
[root@localhost ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rwx
group::rwx
group:main:r-x
mask::rwx
other::---
```

```
[root@localhost ~]#
```

Terminal Window (alice@localhost):

```
alice@localhost:~/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 18 18:21 alice3
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
alice@localhost main$ rm -rf bob
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
alice@localhost main$
```

Web Browser (https://esystem.rudn.ru/pluginfile.php/2400...):

установить разрешения для группы:

```
setfacl -m "g:group:permissions" <file/dir>
```

Наследование записи ACL родительского каталога:

```
setfacl -dm "entry" <dir>
```

Удаление записи ACL:

```
setfacl -x "entry" <file/dir>
```

Синтаксис команды getfacl:

```
getfacl <file/dir>
```

Применим команды setfacl и getfacl для выполнения поставленной задачи.

1. Откройте терминал с учётной записью root
2. Установите права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third:

```
setfacl -m g:third:rx /data/main
setfacl -m g:main:rx /data/third
```
3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:

```
getfacl /data/main
getfacl /data/third
```
4. Создайте новый файл с именем newfile1 в каталоге /data/main:

```
touch /data/main/newfile1
```

Используйте

```
getfacl /data/main/newfile1
```

для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему.
Выполните аналогичные действия для каталога /data/third. Дайте пояснения.
5. Установите ACL по умолчанию для каталога /data/main:

```
setfacl -m d:g:third:rwx /data/main
```
6. Добавьте ACL по умолчанию для каталога /data/third:

```
setfacl -m d:g:main:rwx /data/third
```
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:

```
touch /data/main/newfile2
```

создание примерный файл

The image shows a Linux desktop environment with a terminal window and a web browser. The terminal window is split into two panes. The top pane shows the root user at localhost in the /data/main directory. The user creates a new file named 'newfile1' and lists the directory contents. The output shows a list of files and their permissions: -rw-r--r--. 1 alice main 0 Sep 18 18:21 alice3, -rw-r--r--. 1 alice main 0 Sep 18 18:22 alice4, -rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1, -rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2, -rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile, and -rw-r--r--. 1 root main 0 Sep 18 18:30 newfile1. The user then runs 'getfacl /data/main/newfile1', which shows the file's ACL: Removing leading '/' from absolute path names, # file: data/main/newfile1, # owner: root, # group: main, user::rw-, group::r--, other::r--.

The bottom pane of the terminal shows the alice user at localhost in the /data/main directory. The user lists the directory contents, which shows the same list of files as the top pane. The user then runs 'rm -rf bob', which fails with the message 'rm: cannot remove 'bob1': Operation not permitted' and 'rm: cannot remove 'bob2': Operation not permitted'. The user then creates a new file named 'newfile2' and lists the directory contents, which shows the same list of files as the top pane.

The web browser window shows a tutorial for setting permissions. The URL is <https://esystem.rudn.ru/pluginfile.php/2400/>. The tutorial is titled '004-permissions.p' and is part of a series of 5 pages. The current page is page 3 of 5. The tutorial contains the following steps:

3. Используйте команду `getfacl`, чтобы убедиться в правильности установки разрешений:
`getfacl /data/main`
`getfacl /data/third`
4. Создайте новый файл с именем `newfile1` в каталоге `/data/main`:
`touch /data/main/newfile1`
Используйте
`getfacl /data/main/newfile1`
для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему.
5. Установите ACL по умолчанию для каталога `/data/main`:
`setfacl -m d:g:third:rxw /data/main`
6. Добавьте ACL по умолчанию для каталога `/data/third`:
`setfacl -m d:g:main:rxw /data/third`
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог `/data/main`:
`touch /data/main/newfile2`

Используйте
`getfacl /data/main/newfile2`
для проверки текущих назначений полномочий. Выполните аналогичные действия для каталога `/data/third`.

8. Для проверки полномочий группы `third` в каталоге `/data/third` войдите в другом терминале под учётной записью члена группы `third`:
`su - carol`
Проверьте операции с файлами:
`rm /data/main/newfile1`
`rm /data/main/newfile2`
Проверьте, возможно ли осуществить запись в файл:
`echo "Hello, world" >> /data/main/newfile1`
`echo "Hello, world"`

установка ACL

Activities

Terminal

Sep 18 18:38

en

🔊

🔄

root@localhost:/data/third

🔍

☰

✕

```
[root@localhost main]# setfacl -m d:g:third:rw /data/main
[root@localhost main]# cd /data/third
[root@localhost third]# setfacl -m d:g:main:rw /data/third
[root@localhost third]# touch /data/main/newfile2
[root@localhost third]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rw-
group::rw-
group:third:rw-
mask::rw-
other::---
```

alice@localhost:/data/main

🔍

☰

✕

```
[alice@localhost main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 18 18:21 alice3
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
[alice@localhost main]$ rm -rf bob
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
[alice@localhost main]$ touch /data/main/newfill
[alice@localhost main]$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Sep 18 18:21 alice3
-rw-r--r--. 1 alice main 0 Sep 18 18:22 alice4
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob1
-rw-r--r--. 1 bob bob 0 Sep 18 18:20 bob2
-rw-r--r--. 1 bob bob 0 Sep 18 18:13 emptyfile
-rw-r--r--. 1 alice main 0 Sep 18 18:30 newfill
[alice@localhost main]$ rm newfill
[alice@localhost main]$ ls
alice2 alice4 bob1 bob2 emptyfile
```

Курс: Основы

004-permissions.p

В этом упражнени

✕

+

▼

✕

🔍

🔗

🔒

🌐

https://esystem.rudn.ru/pluginfile.php/2400

🔖

🔔

🔖

☰

Rocky Linux

Rocky Wiki

Rocky Forums

Rocky Mattermost

Rocky Reddit

📄

^

▼

3 of 5

—

+

140%

▼

🔍

🔗

🔗

🔗

setfacl -m g:main:rx /data/third

3. Используйте команду getfacl, чтобы убедиться в правильности установки разрешений:

getfacl /data/main

getfacl /data/third

4. Создайте новый файл с именем newfile1 в каталоге /data/main:

touch /data/main/newfile1

Используйте

getfacl /data/main/newfile1

для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему.

5. Установите ACL по умолчанию для каталога /data/main:

setfacl -m d:g:third:rw /data/main

6. Добавьте ACL по умолчанию для каталога /data/third:

setfacl -m d:g:main:rw /data/third

7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:

touch /data/main/newfile2

30

Лабораторная работа № 3. Настройка прав доступа

Используйте

getfacl /data/main/newfile2

для проверки текущих назначений полномочий.

Выполните аналогичные действия для каталога /data/third.

8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:

su - carol

Проверьте операции с файлами:

rm /data/main/newfile1

rm /data/main/newfile2

Проверьте, возможно ли осуществить запись в файл:

echo "Hello, world" >> /data/main/newfile1

echo "Hello, world"

17/19

Проверка работы ACL

Проверка работы ACL

The screenshot shows a terminal window with the following output:

```
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile3
# owner: root
# group: root
user::rw-
group::rwx          #effective:rw-
group:main:rwx      #effective:rw-
mask::rw-
other::---
```

Then, the user runs the command:

```
[root@localhost third]# setfacl -m d:g:main:rwx /data/third
```

The output is:

```
[root@localhost third]# getfacl /data/third/newfile3
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile3
# owner: root
# group: root
user::rw-
group::rwx          #effective:rw-
group:main:rwx      #effective:rw-
mask::rw-
other::---
```

Below the terminal, a second terminal window shows the user 'carol' attempting to remove files:

```
[carol@localhost ~]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
[carol@localhost ~]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@localhost ~]$
```

On the right, a web browser window displays a document titled '004-permissions.p' with the following content:

6. Добавьте ACL по умолчанию для каталога /data/third:

```
setfacl -m d:g:third:rwx /data/main
```

7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main:

```
touch /data/main/newfile2
```

30

Лабораторная работа № 3. Настройка прав доступа

Используйте

```
getfacl /data/main/newfile2
```

для проверки текущих назначений полномочий.

Выполните аналогичные действия для каталога /data/third.

8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:

```
su - carol
```

Проверьте операции с файлами:

```
rm /data/main/newfile1
```

```
rm /data/main/newfile2
```

Проверьте, возможно ли осуществить запись в файл:

```
echo "Hello, world" >> /data/main/newfile1
```

```
echo "Hello, world" >> /data/main/newfile2
```

Объясните результат произведённых действий.

3.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - подробное описание произведённых в соответствии с заданием настроек;
 - результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы (по возможности подтверждённые скриншотами).

Результаты

- используя команду `chgrp` изменить группу владельцев можно
- `chmod` используется чтобы дать права доступа
- `sticky bit` защищает файлы от изменений другими пользователями
- `setfacl` даёт специальные права доступа