**Лабораторная работа № 6. Управление пользователями**

**и группами в ОС «Linux».**

**6.1. Цель работы**

Получить представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

**6.2. Предварительные сведения**

В операционных системах типа Linux чаще всего применяется дискреционное управление доступом субъектов к объектам системы. В качестве субъектов системы чаще всего выступают пользователи или группы, а в качестве субъектов — файлы (в том числе системные), каталоги, устройства и т.п. В качестве особого субъекта выделяется суперпользователь (пользователь root), имеющий право устанавливать права владения для всех остальных субъектов системы.

Под доступом к ресурсу системы понимают чтение (read), запись (write) и выполнение (eXecute). Тот или иной тип доступа может быть применён к пользователю и/или группе, владеющими тем или иным ресурсом операционной системы, а также ко всем остальным субъектам, не являющимся владельцами ресурса.

Права доступа к ресурсу представляются в системе следующим образом:

<Флаг> < Пользователь-владелец> < Группа-владелец> < Все остальные>

# rwx rwx rwx

В качестве флага может быть указано:

Флаг Описание

- указывает на отсутствие флага

l указывает, что ресурс является символической ссылкой

d указывает, что ресурс является каталогом

b указывает, что ресурс является блочным устройством

c указывает, что ресурс является символьным устройством

p указывает, что ресурс является каналом, устройством fifo

s указывает, что ресурс является Unix сокетом

Пример отображения информации о правах доступа, владельце, группе и т.п. файла /etc/passwd:

ls -l /etc/passwd

-rw-r--r-- 1 root root 5302 ноя 13 2017 /etc/passwd

Первая колонка отображает права доступа к файлу (в данном случае -rw-r--r--), в третьей и четвёртой колонке указано, что владельцем файла является пользователь root и одноимённая группа root.

Для установки атрибутов прав доступа используется утилита chmod. При этом можно использовать как восьмеричное представление, так и символьное:

Восьмеричная запись Бинарная запись Маска

0 000 ---

1 001 --x

2 010 -w-

3 011 -wx

4 100 r--

5 101 r-x

6 110 rw-

7 111 rwx

Пример установки прав доступа rwxr--r-- для файла file1:

chmod 744 file1

или

chmod u=rwx,go+r,go-wx file1

**6.2.1. Системные базы учётных записей**

**6.2.1.1. Файл /etc/passwd**

В операционных системах типа Linux информация о пользователях располагается в файле /etc/passwd. Запись о пользователе в этом файле имеет определённую структуру в виде набора полей, разделённых двоеточием:

имя\_пользователя:пароль:UID:GID:комментарий:каталог:оболочка

Фрагмент файла /etc/passwd:

ntp:x:38:38::/etc/ntp:/sbin/nologin

chrony:x:994:993::/var/lib/chrony:/sbin/nologin

abrt:x:173:173::/etc/abrt:/sbin/nologin

pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin

gdm:x:42:42::/var/lib/gdm:/sbin/nologin

gnome-initial-setup:x:993:991::/run/gnome-initial-setup/:/sbin/nologin

postfix:x:89:89::/var/spool/postfix:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

tcpdump:x:72:72::/:/sbin/nologin

user:x:1000:1000:user:/home/user:/bin/bash

Ниже приведён краткий обзор полей файла /etc/passwd, за которым следует краткое описание их цели.

**–** *Имя пользователя* — это уникальное имя для пользователя. Имена пользователей важны для соответствия пользователю пароля, который хранится отдельно в файле /etc/shadow. В Linux не может быть пробелов в имени пользователя.

**–** *Пароль* — раньше второе поле в файле /etc/passwd использовалось для хранения хэшированного пароля пользователя. Доступ на чтение файла /etc/passwd имеют все пользователи системы, поэтому хранение пароля в этом файле создаёт угрозу безопасности. По этой причине в современных системах Linux хешированные пароли хранятся в файле /etc/shadow, а в файле /etc/passwd есть только указание на это в виде символа x.

**–** *UID, User ID* — каждый пользователь имеет уникальный числовой идентификатор пользователя (UID). Именно UID определяет возможные разрешения для пользователя. UID хранится в метаданных файла, а не в имени пользователя.

UID 0 зарезервирован для пользователя root с неограниченными правами. Бо-

лее низкие UID (обычно до 999) используются для системных учётных записей, а более высокие UID (от 1000) зарезервированы для остальных пользователей.

Диапазон UID, который используется для создания обычных учётных записей пользователей, устанавливается в файле /etc/login.defs.

**-** *GID, group ID* — в Linux каждый пользователь является членом хотя бы одной группы, называемой первичной (или основной). Первичная группа играет центральную роль в управлении разрешениями.

**–** Поле комментариев — используется для описания назначения учётной записи пользователя. Это поле является необязательным. Некоторые утилиты, например finger, могут получать информацию из этого поля. Это поле также называется *GECOS* (от названия операционной системы фирмы General Electric).

**–** *Каталог* — это начальный (домашний) каталог, в котором пользователь находится после входа в систему. Если учётная запись пользователя используется человеком, то здесь человек будет хранить свои личные файлы и программы. Для системной учётной записи этот каталог используется для хранения служебных файлов, используемых в работе.

**–** *Оболочка (shell)* — это программа, которая запускается после успешного подключения пользователя к системе. Для большинства пользователей это будет /bin/bash — стандартная оболочка Linux. Для системных учётных записей в качестве оболочки обычно выступает /sbin/nologin — это специальная команда, которая запрещает доступ злоумышленника к системе (для гарантии недоступности оболочки, а, соответственно, и невозможности внесения изменений куда бы то ни было). Можно создать файл с именем /etc/nologin.txt, содержащий сообщение, которое будет отображаться, когда пользователь с оболочкой /sbin/nologin попытается войти в систему.

**6.2.1.2. Файл /etc/shadow**

Файл /etc/shadow предназначен для хранения зашифрованных паролей пользователей системы. Поля записей в этом файле разделены двоеточием.

Фрагмент файла /etc/shadow:

ntp:!!:16420::::::

chrony:!!:16420::::::

abrt:!!:16420::::::

pulse:!!:16420::::::

gdm:!!:16420::::::

gnome-initial-setup:!!:16420::::::

postfix:!!:16420::::::

sshd:!!:16420::::::

tcpdump:!!:16420::::::

user:$6$3VZbGx1djo6FfyZo9/Trg7Q.3foIsIFYxBm6UnHuxxBrxQxHDnDuZxgS.We/

,! MAuHn8HboBZzpaMD8gfm.fmlB/ML9LnuaT7CbwVXx31:16420:0:99999:7:::

В файле /etc/shadow определены следующие поля:

1. *Имя пользователя*. В файле /etc/shadow содержатся только имена пользователей, а не UID, что позволяет работать нескольким пользователям с одинаковым UID, но разными паролями.

2. *Зашифрованный пароль* — это поле содержит пароль пользователя.

3. *Количество дней с 1 января 1970 года, когда пароль был изменён в последний раз.*

*4. Количество дней до того, как пароль может быть изменён. Это поле позволяет системным администраторам использовать более строгую политику паролей, когда невозможно сразу вернуться к исходному паролю при его изменении. Обычно это поле устанавливается в значение 0.*

*5. Количество дней, после которых необходимо изменить пароль. Это поле содержит максимальный срок действия пароля. По умолчанию установлено 99999 (около273 лет).*

*6. За сколько дней до истечения срока действия пароля пользователь получает предупреждение. Это поле используется для предупреждения пользователя о сроке, когда происходит принудительное изменение пароля. По умолчанию установлено значение 7.*

*7. Через сколько дней после истечения срока действия пароля учётная запись будет отключена. После истечения срока действия пароля пользователи больше не смогут входить в систему.*

*8. Количество дней с 1 января 1970 года, когда эта учётная запись была отключена. Администратор может установить это поле для отключения учёной записи.*

*Обычно это лучший подход, чем удаление учёной записи, так как все связанные с ней свойства и файлы учётной записи будут сохранены.*

*9. Зарезервированное поле, которое добавлено для будущего использования.*

***6.2.1.3. Файл /etc/group***

*Файл /etc/group содержит имена групп и списки членов каждой группы. Поля записей в этом файле разделены двоеточием.*

*Фрагмент файла /etc/group:*

*kvm:x:36:qemu*

*qemu:x:107:*

*libstoragemgmt:x:994:*

*rpc:x:32:*

*rpcuser:x:29:*

*В файле /etc/group используются следующие поля:*

***–*** *Название группы — это поле содержит имя группы.*

***–*** *Групповой пароль. Групповой пароль может использоваться пользователями, которые хотят временно присоединиться к группе, чтобы разрешить доступ к файлам,доступ к которым имеет группа. В настоящее время эта функциональность больше не используется.*

***–*** *Идентификатор группы (GID) — уникальный цифровой идентификационный номер группы.*

***–*** *Члены группы — здесь перечислены имена пользователей, которые являются членами этой группы (для пользователей подобная группа является вторичной).*

*Тут не отображаются пользователи, для которых данная группа является основной.*

***6.2.2. Параметры учётных записей***

*Для создания учётных записей пользователей удобно использовать утилиту типа useradd:*

*useradd -m -g [основная группа] -G [дополнительные группы]*

*-s [командная оболочка] [имя пользователя];*

*Ключ -m указывает на создание домашнего каталога пользователя вида*

*/home/[имя пользователя];*

*Ключ -g задаёт имя или номер основной группы пользователя; если параметр не указан, пользователю будет присвоена группа в соответствии с переменной USERGROUPS\_ENAB, расположенной в каталоге /etc/login.defs.*

*Ключ -G задаёт список дополнительных групп, в которые входит пользователь;*

*каждая группа отделяется от другой запятой без пробелов.*

*Ключ -s задаёт командную оболочку пользователя.*

*При этом файл /etc/default/useradd содержит устанавливаемые для новой*

*учётной записи значения по умолчанию.*

*Описание действий других возможных ключей можно посмотреть, используя команду man useradd.*

*Фрагмент файла /etc/default/useradd:*

*# useradd defaults file*

*GROUP=100*

*HOME=/home*

*INACTIVE=-1*

*EXPIRE=*

*SHELL=/bin/bash*

*SKEL=/etc/skel*

*CREATE\_MAIL\_SPOOL=yes*

*В файле /etc/login.defs устанавливаются разные переменные для команды login. Этот файл связан с настройкой соответствующей среды для новых пользователей. Ниже приведён список некоторых наиболее значимых переменных, которые могут быть установлены из /etc/login.defs:*

***–*** *MOTD\_FILE — определяет файл, который используется как файл «сообщение дня».*

*В этот файл можно включать сообщения, которые будут отображаться после того, как пользователь успешно войдёт в систему.*

***–*** *ENV\_PATH — определяет переменную $PATH, список каталогов, в которых необходимо искать исполняемые файлы после входа в систему.*

***–*** *PASS\_MAX\_DAYS, PASS\_MIN\_DAYS и PASS\_WARN\_AGE — определяют свойства по умолчанию истечения срока действия пароля при создании новых пользователей.*

***–*** *UID\_MIN — первый UID для использования при создании новых пользователей.*

***–*** *CREATE\_HOME — указывает, следует ли создавать домашний каталог для новых пользователей.*

***–*** *USERGROUPS\_ENAB — создавать ли частную группы для новых пользователей.*

*Это означает, что у нового пользователя есть группа с тем же именем, что и имя пользователя в качестве своей группы по умолчанию. Если установлено no, все пользователи становятся членами группы пользователей (users).*

***6.3. Задание***

*1. Прочитайте справочное описание man по командам ls, whoami, id, su, passwd,vi, visudo, useradd, usermod, userdel, groupadd, groupdel.*

*2. Выполните действия по переключению между учётными записями пользователей, по управлению учётными записями пользователей (раздел 6.4.1).*

*3. Выполните действия по созданию пользователей и управлению их учётными записями (раздел 6.4.2).*

*4. Выполните действия по работе с группами пользователей (раздел 6.4.3.*

***6.4. Последовательность выполнения работы***

***6.4.1. Переключение учётных записей пользователей***

*1. Войдите в систему как обычный пользователь и откройте терминал.*

*2. Определите, какую учётную запись пользователя вы используете, введя команду whoami.*

*Выведите на экран более подробную информацию, используя команду*

*id.*

*В отчёте дайте пояснение по отображённой информации.*

*3. Используйте команду su для переключения к учётной записи root. При запросе пароля введите пароль пользователя root. Наберите*

*id .В отчёте дайте пояснение по отображённой информации.*

*4. Просмотрите в безопасном режиме файл /etc/sudoers, используя, например, visudo*

*и убедитесь, что в нём присутствует строка*

*% wheel ALL = (ALL) ALL*

*В отчёте поясните, что это означает и для чего нужна группа wheel.*

*5. Создайте пользователя alice, входящего в группу wheel:*

*useradd -G wheel alice*

*6. Убедитесь, что пользователь alice добавлен в группу wheel, введя*

*id alice*

*7. Задайте пароль для пользователя alice, набрав*

*passwd alice*

*Пароль требуется ввести дважды.*

*8. Выйдите из системы (из своей учётной записи) и войдите в систему как пользователь alice.*

*9. Создайте пользователя bob:*

*sudo useradd bob*

*Введите пароль при запросе. Проверьте, что пользователь bob создан.*

***6.4.2. Создание учётных записей пользователей***

*Применим общие решения для создания учётных записей пользователей.*

*1. Откройте файл конфигурации /etc/login.defs для редактирования, используя,например, vim (не забудьте, что требуются полномочия пользователя root):*

*vim /etc/login.defs*

*Измените несколько параметров. Например, найдите параметр*

*CREATE\_HOME*

*и убедитесь, что он установлен в значение yes. Также установите параметр*

*USERGROUPS\_ENAB no*

*Это позволит не добавлять нового пользователя в группу с тем же именем, что и пользователь, а использовать группу users.*

*2. Перейдите в каталог /etc/skel:*

*cd /etc/skel*

*Создайте каталоги Pictures и Documents:*

*mkdir Pictures*

*и*

*mkdir Documents*

*Это позволит добавить эти каталоги по умолчанию во все домашние каталоги пользователей.*

*3. Измените содержимое файла .bashrc, добавив строку*

*export EDITOR=/usr/bin/vim*

*Эта запись означает, что текстовый редактор vim будет установлен по умолчанию для инструментов, которые нуждаются в изменении текстовых файлов.*

*4. Используя утилиту useradd, создайте пользователя carol:*

*useradd carol*

*Посмотрите и прокомментируйте информацию об этом пользователе:*

*id carol*

*Проверьте, в какую первоначальную группу входит пользователь carol. Так-*

*же убедитесь, что каталоги Pictures и Documents были созданы в домашнем*

*каталоге пользователя carol.*

*5. Установите пароль для пользователя carol:*

*passwd carol*

*6. Измените свойства пароля пользователя carol следующим образом:*

*passwd -n 30 -w 3 -x 90 carol*

*В этой записи срок действия пароля истекает через 90 дней (-x 90). За три дня до истечения срока действия пользователь получит предупреждение (-w 3). Пароль должен использоваться как минимум за 30 дней (-n 30) до того, как его можно будет изменить.*

*7. Создайте ещё несколько пользователей: dan, dave, david, используя скрипт:*

***for*** *i in dan dave david;* ***do*** *useradd $i;* ***done***

*8. Убедитесь, что идентификатор alice существует во всех трёх файлах:*

*grep alice /etc/passwd /etc/shadow /etc/group*

*9. Убедитесь, что идентификатор carol существует не во всех трёх файлах:*

*grep carol /etc/passwd /etc/shadow /etc/group*

***6.4.3. Работа с группами***

*В этом упражнении требуется создать две группы и добавить некоторых пользователей в эти группы.*

*1. Создайте группы main и third:*

*groupadd main*

*groupadd third*



*2. Используйте usermod для добавления пользователей alice и bob в группу main, а carol, carlos и charlie — в группу third:*

*usermod -aG main alice*

*usermod -aG main bob*

*usermod -aG third carol*

*usermod -aG third dan*

*usermod -aG third dave*

*usermod -aG third david*

*3. Убедитесь, что пользователь carol правильно добавлен в группу third:*

*id carol*

*Пользователю carol должна быть назначена основная группа с идентификатором gid = 100 (users). Определите, в какие вторичные группы входит carol.*

*4. Определите, участниками каких групп являются другие созданные вами пользователи.*

***6.5. 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;*

***–*** *результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).*

*4. Выводы, согласованные с заданием работы.*

*5. Ответы на контрольные вопросы.*

***6.6. Контрольные вопросы***

*1. Какой UID имеет пользователь root? - 0*

*2. В каком конфигурационном файле определяются параметры sudo? - /etc/****sudoers***

*3. Какую команду следует использовать для изменения конфигурации sudo?*

*4. Какие два файла можно использовать для определения параметров, которые будут*

*использоваться при создании пользователей?*

*5. Сколько групп вы можете создать в файле /etc/passwd?*

*6. Если вы хотите предоставить пользователю доступ ко всем командам администратора через sudo, членом какой группы он должен быть?*

*7. Какую команду следует использовать для изменения файла /etc/group вручную?*

*8. Какие две команды вы можете использовать для изменения информации о пароле пользователя?*

*9. В каких файлах хранятся пароли пользователей и учётные записи групп?*

***Лабораторная работа № 7. Настройка прав доступа в ОС «Linux».***

***7.1. Цель работы***

*Получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.*

***7.2. Задание***

*1. Прочитайте справочное описание man по командам ls, su, chgrp, chmod,*

*getfacl, setfacl.*

*2. Выполните действия по управлению базовыми разрешениями для групп пользвателей (раздел 7.3.1).*

*3. Выполните действия по управлению специальными разрешениями для групп пользователей (раздел 7.3.2).*

*4. Выполните действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей (раздел 7.3.3).*

***7.3. Последовательность выполнения работы***

*Предпосылки: в лабораторной работе № 6 были созданы пользователи alice и bob, входящие в группу main, и пользователь carol, входящий в группу third.*

***7.3.1. Управление базовыми разрешениями***

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

*1. Откройте терминал с учётной записью root:*

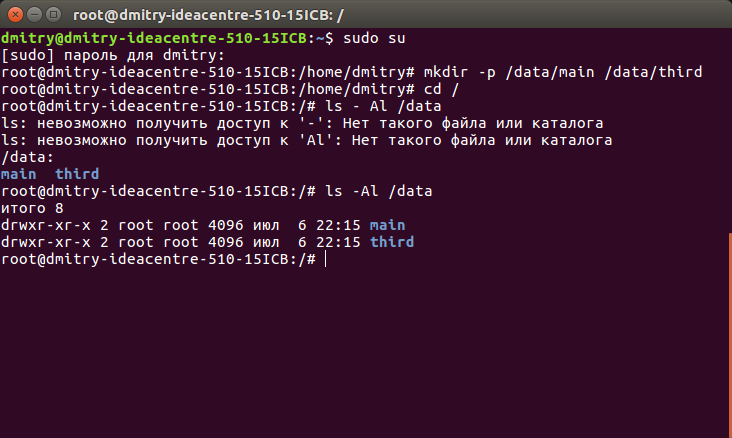
*su -*

*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.*

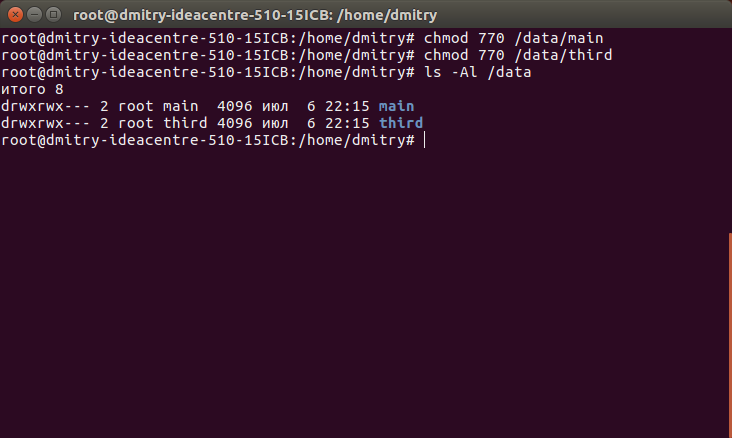


*4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:*

*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 перейдите в каталог /data/main:*

*cd /data/main*

*Попробуйте создать файл emptyfile в этом каталоге:*

*touch emptyfile*

*Опишите и поясните результат этого действия.*

*7. Под пользователем bob перейдите в каталог /data/third:*

*cd /data/third*

*Попробуйте создать файл emptyfile в этом каталоге:*

*touch emptyfile*

*Опишите и поясните результат этого действия.*

***7.3.2. 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 символьное: +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*

*фалы, 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*

*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\**

*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.*

***7.3.3. Управление расширенными разрешениями с использованием***

***списков ACL***

*В этом упражнении продолжим работать в созданных ранее каталогах /data/main*

*и /data/third.*

*В предыдущих упражнениях для группы main были установлены*

*разрешения на каталог /data/main, а у группы third —- на каталог /data/third.*

*Требуется установить для группы third разрешения на чтение в каталоге*

*/data/main, а для группы main — разрешения на чтение в каталоге /data/third.*

*Затем требуется установить права доступа по умолчанию, чтобы убедиться в правильности установки разрешений для новых элементов этих каталогов. Для этого будет использоваться пакет acl и команды setfacl (для установки прав) и getfacl(для просмотра установленных прав).*

*Кратко опишем синтаксис команды setfacl.*

*Установить разрешения для пользователя:*

*setfacl -m "u:user:permissions" <file/dir>*

*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: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*

*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/newfile1*

*Проверьте, возможно ли осуществить запись в файл:*

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

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

*Объясните результат произведённых действий.*

***7.4. 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.*

***7.5. Контрольные вопросы***

*1. Как следует использовать команду chown, чтобы установить владельца группы для файла? Приведите пример.*

*2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример.*

*3. Как применить разрешения на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп, не устанавливая никаких прав для других? Приведите пример.*

*4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?*

*5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога? Приведите пример.*

*6. Необходимо, чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они являются. С помощью какой команды можно это сделать? Приведите пример.*

*7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?*

*8. Что нужно сделать для гарантии того, что члены группы получат разрешения на чтение для всех файлов в текущем каталоге и во всех его подкаталогах, а также для всех файлов, которые будут созданы в этом каталоге в будущем? Приведите пример.*

*9. Какое значение umask нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример.*

*10. Какая команда гарантирует, что никто не сможет удалить файл myfile случайно?*