Отчёт по лабораторной работе №2

Дисциплина: Основы администрирования операционных систем

Бызова Мария Олеговна

Содержание

# 1 Цель работы

Целью данной работы является получение представления о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

# 2 Задание

1. Прочитать справочное описание man по командам ls, whoami, id, groups, su, sudo, passwd, vi, visudo, useradd, usermod, userdel, groupadd, groupdel. Кулябов Д. С., Королькова А. В. Основы администрирования операционных систем
2. Выполнить действия по переключению между учётными записями пользователей, по управлению учётными записями пользователей (раздел 2.4.1).
3. Выполнить действия по созданию пользователей и управлению их учётными записями (раздел 2.4.2).
4. Выполнить действия по работе с группами пользователей (раздел 2.4.3).

# 3 Выполнение лабораторной работы

## 3.1 Переключение учётных записей пользователей

Я вошла в систему как обычный пользователь и открыла терминал. Определила, какую учётную запись пользователя я использую, введя команду whoami. Я использую учетную запись mobihzova (рис. 1).

Работа команды whoami

Рис. 1: Работа команды whoami

Выведем на экран более подробную информацию, используя команду id (UID – id пользователя равный 1000. GID – id группы равный 1000) (рис. 2).

Работа команды id

Рис. 2: Работа команды id

Используем команду su для переключения к учётной записи root. При запросе пароля вводим пароль пользователя root. Наберём id (UID – id пользователя равный 0. GID – id группы равный 0) (рис. 3, рис. 4.).

Работа команды su

Рис. 3: Работа команды su

Работа команды id

Рис. 4: Работа команды id

Далее просмотрим в безопасном режиме файл /etc/sudoers. Редактирование файла /etc/sudoers обычным редактором опасно из-за возможных синтаксических ошибок и проблем с правами доступа и т.д. Использование visudo является единственным безопасным способом редактирования /etc/sudoers, так как оно обеспечивает проверку синтаксиса, временную блокировку файла и возможность отмены изменений. Это гарантирует корректность конфигурации и предотвращает блокировку доступа к системе (рис. 5).

Просмотр файла в безопасном режиме

Рис. 5: Просмотр файла в безопасном режиме

После мы должны убедиться, что в открытом с помощью visudo файле присутствует строка %wheel ALL=(ALL) ALL (данная строка присутствует). Строка %wheel ALL=(ALL) ALL в файле /etc/sudoers означает, что все пользователи, входящие в группу wheel, могут выполнять любые команды от имени любого пользователя без пароля. Группа wheel обычно используется для предоставления административных привилегий пользователям (рис. 6).

Проверка наличия строки

Рис. 6: Проверка наличия строки

По закрытии файла создаём пользователя alice, входящего в группу wheel с помощью команды: useradd -G wheel alice (рис. 7).

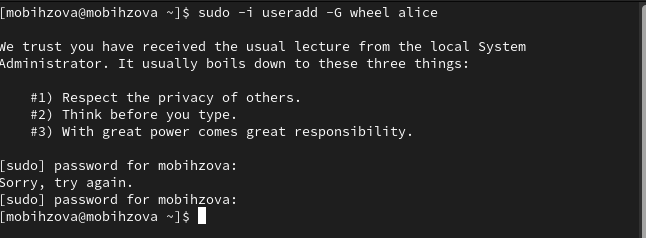


Рис. 7: Создание пользователя alice

Нужно убедиться, что пользователь alice добавлен в группу wheel. Для этого введём команду id alice (Groups = 1001(alice),10(wheel)). (рис. 8).

Информация о пользователе alice

Рис. 8: Информация о пользователе alice

Следующим шагом зададим пароль для пользователя alice, набрав passwd alice. Пароль требуется ввести дважды (рис. 9).

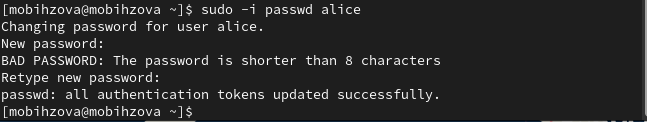


Рис. 9: Создание пароля для пользователя alice

Переключаемся на учётную запись пользователя alice командой: su alice. (рис. 10).

Смена пользователя

Рис. 10: Смена пользователя

Создаём пользователя bob: sudo useradd bob (рис. 11).

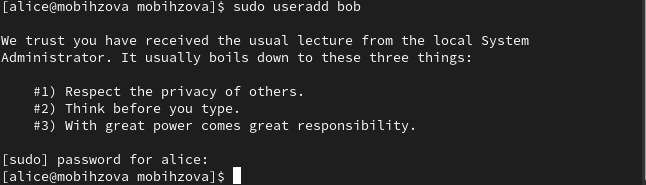


Рис. 11: Создание пользователя bob

При запросе вводим пароль пользователя. Проверяем, что пользователь bob создан (id bob) и устанавливаем пароль для пользователя: sudo passwd bob (рис. 12).

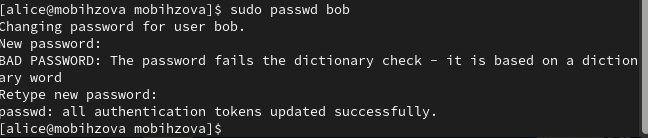


Рис. 12: Создание пароля для пользователя bob

Посмотрим, в какие группы входит пользователь bob (рис. 13).

Информация о пользователе bob

Рис. 13: Информация о пользователе bob

## 3.2 Создание учётных записей пользователей

Переключимся в терминале на учётную запись пользователя root. Откроем файл конфигурации /etc/login.defs для редактирования (рис. 14).

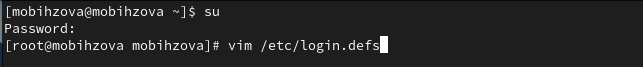


Рис. 14: Смена пользователя. Открытие файла

В файле требуется изменить несколько параметров. Для начала найдём параметр CREATE\_HOME и убедимся, что он установлен в значение yes. Теперь установим параметр USERGROUPS\_ENAB no. Это позволит не добавлять нового пользователя в группу с тем же именем, что и пользователь, а использовать группу users.(рис. 15).

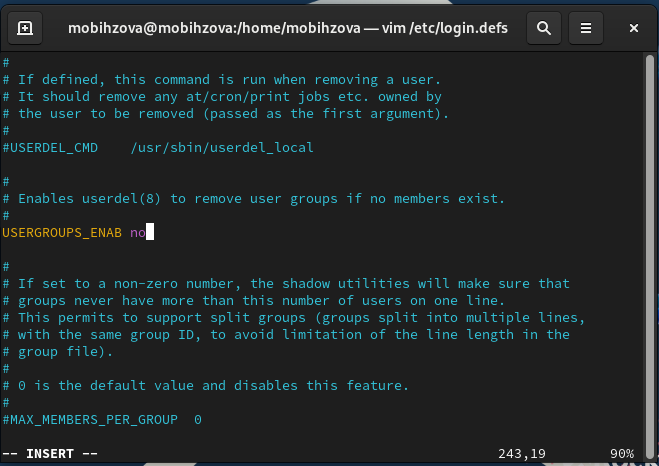


Рис. 15: Изменение параметра USERGROUPS\_ENAB и USERGROUPS\_ENAB

После закрытия файла перейдём в каталог /etc/skel: cd /etc/skel. В этом каталоге создаём подкаталоги Pictures и Documents: mkdir Pictures Documents (это позволит добавить эти каталоги по умолчанию во все домашние каталоги пользователей). Выполняем проверку создания командой: ls (рис. 16).

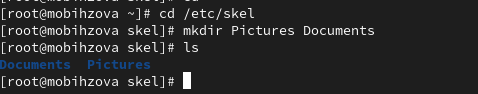


Рис. 16: Открытие каталога /etc/skel и создание подкаталогов Pictures и Documents, проверка создания

Теперь нам нужно изменить 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) (рис. 17).

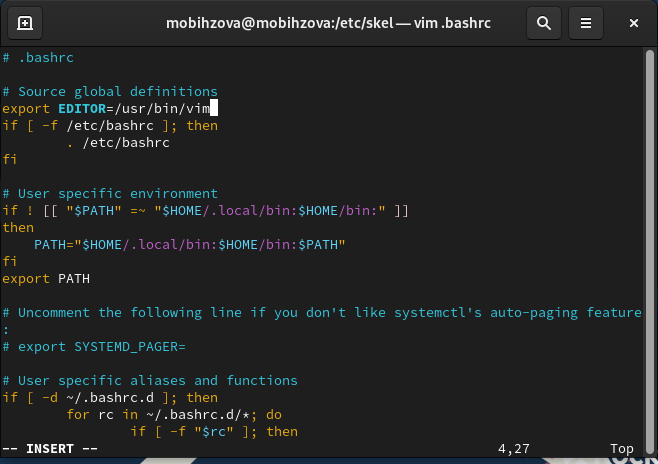


Рис. 17: Добавление строки: export EDITOR=/usr/bin/vim

Используя утилиту useradd, создаём пользователя carol: useradd carol и установим пароль для пользователя carol: passwd carol. Посмотрим информацию о пользователе carol: id carol (carol находится в группе users). Теперь нам нужно убедитесь, что каталоги Pictures и Documents были созданы в домашнем каталоге пользователя carol: su carol и ls (рис. 18).

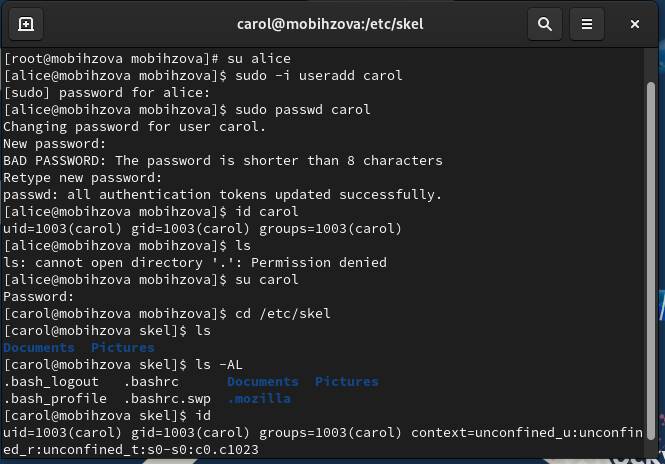


Рис. 18: Создание пользователя carol и установка пароля. Просмотр информации о пользователе carol и проверка наличия каталогов.

Строка записи о пароле пользователя carol в файле /etc/shadow содержит следующую информацию:

1. carol6ey j spMO34dMP2qMIPKc1za061HZA.LaSWBEA1b2kVn1Na27F2SyQmqDBeqIfNISKXMnsplYOVgLDNgNHhJ7r01: Это зашифрованный пароль пользователя и имя пользователя.
2. 19974: Количество дней с 1 января 1970 года, когда пароль был изменён в последний раз.
3. 0: 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.
4. 99999: Количество дней, которое может пройти, прежде чем пароль станет недействительным. Это поле содержит макси- мальный срок действия пароля. По умолчанию установлено 99999 (около 273 лет).
5. 7: 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
6. ::: Дополнительная информация о пароле. В данном случае она отсутствует (рис. 19).

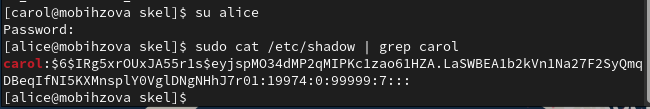


Рис. 19: Информация о пароле пользователя carol

Изменим 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) (рис. 20).

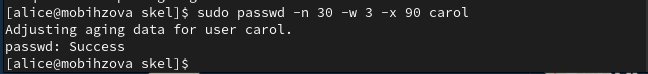


Рис. 20: Изменение свойства пароля пользователя carol

Убедимся в изменении в строке с данными о пароле пользователя carol в файле /etc/shadow (рис. 21).

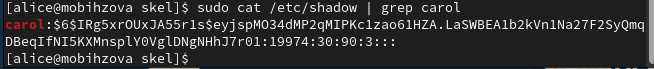


Рис. 21: Информация о пароле пользователя carol

Убедимся, что идентификатор alice существует во всех трёх файлах (рис. 22).

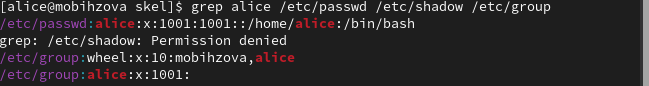


Рис. 22: Индентификатор alice

Убедимся, что идентификатор carol существует не во всех трёх файлах (рис. 23).

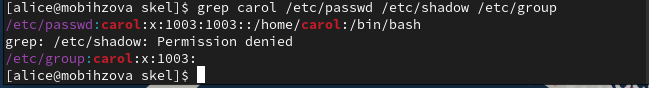


Рис. 23: Индентификатор carol

## 3.3 Работа с группами

На данном этапе требуется создать две группы и добавить некоторых пользователей в эти группы. Находясь под учётной записью пользователя root, создаём группы main и third: groupadd main, groupadd third (рис. 24).

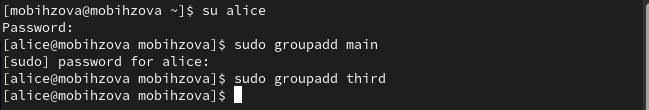


Рис. 24: Создание групп

Затем используем usermod для добавления пользователей alice и bob в группу main, а carol, dan, dave и david - в группу third (рис. 25).

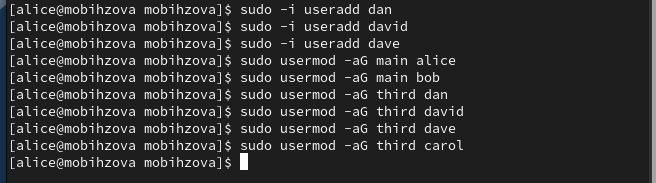


Рис. 25: Добавление пользователей в группы

Убеждаемся, что пользователь carol правильно добавлен в группу third: id carol (пользователю carol должна быть назначена основная группа с идентификатором gid = 100 (users)). Определяем, участниками каких групп являются другие созданные пользователи (alice и bob входят в группу main. dan, dave, david в группу third) (рис. 26).

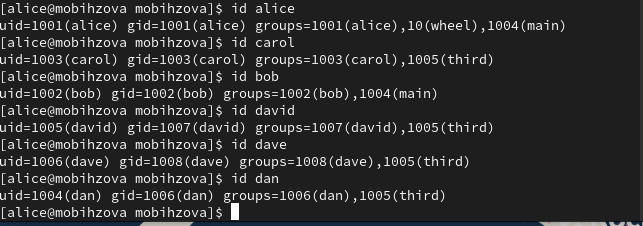


Рис. 26: Определение, участниками каких групп являются созданные пользователи.

# 4 Ответы на контрольные вопросы

1. При помощи какой команды можно получить информацию о номере, назначенном пользователю Linux, о группах, в которые включён пользователь? id.

Работа команды id

Рис. 27: Работа команды id

1. Какой UID имеет пользователь root? UID=0. Самый простой способ посмотреть идентификатор текущего пользователя - использовать команду id, она выводит не только сам UID, но и идентификатор группы пользователя, а также основные группы этого пользователя. Есть ещё несколько способов посмотреть id. Например, для текущего пользователя его можно найти в переменной окружения UID при помощи команды echo $UID. Ещё один вариант - утилита getent: getent passwd имя\_пользователя. Или смотрим содержимое файла /etc/passwd с помощью команды grep: grep имя\_пользователя /etc/passwd. Здесь первый цифровой параметр - это сам id, а второй, который расположен за двоеточием, - это GID.

Работа команды id

Рис. 28: Работа команды id

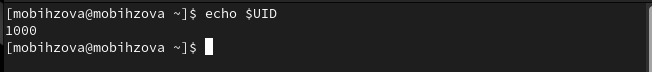


Рис. 29: Работа с переменной окружения UID

Утилита getent

Рис. 30: Утилита getent

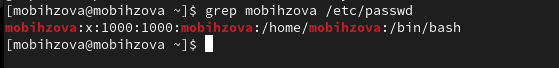


Рис. 31: Содержимое файлы /etc/passwd

1. В чём состоит различие между командами su и sudo? Основное различие между ними заключается в пароле, который им требуется: в то время как “sudo” требует пароля текущего пользователя, “su” требует ввода пароля пользователя root. Совершенно очевидно, что “sudo” является лучшей альтернативой между ними с точки зрения безопасности.
2. В каком конфигурационном файле определяются параметры sudo? /etc/sudoers.
3. Какую команду следует использовать для безопасного изменения конфигурации sudo? Visudo.
4. Если вы хотите предоставить пользователю доступ ко всем командам администратора через sudo, членом какой группы он должен быть? Admin.
5. Какие файлы/каталоги можно использовать для определения параметров, которые будут использоваться при создании учётных записей пользователей? /etc/login.defs и /etc/default/useradd. Например, в ходе данной лабораторной работы при работе с файлом /etc/login.defs мы установили параметр USERGROUPS\_ENAB на no. Это позволит не добавлять нового пользователя в группу с тем же именем, что и польователь, а использовать группу users.
6. Где хранится информация о первичной и дополнительных группах пользователей ОС типа Linux? Информация о пользователях и группах храниться в четырех файлах /etc/passwd, /etc/shadow, /etc/group, /etc/gshadow.

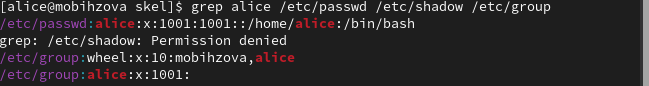


Рис. 32: Идентификатор alice в разных группах

Благодаря данным записям, мы можем узнать, в какие первичные и дополнительные группы входит пользователь alice (Groups = 1001(alice),10(wheel)).

1. Какие команды вы можете использовать для изменения информации о пароле пользователя (например о сроке действия пароля)? passwd и gpasswd.

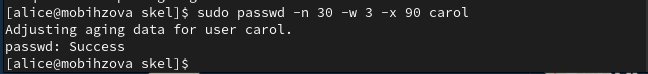


Рис. 33: Изменение информации о пароле пользователя

1. Какую команду следует использовать для прямого изменения информации в файле /etc/group и почему? emacs /etc/group или vim /etc/group. vigr

Почему мы не можем просто отредактировать их с помощью текстового редактора, такого как Vi или nano, и покончить с этим? Файл /etc/passwd в настоящее время редактируется пользователем root с помощью Vi или некоторых других текстовых редакторов. В то же время другой пользователь пытается изменить свой пароль, пока пользователь root редактирует файл /etc/passwd. Таким образом, изменение пароля в этом файле может не обновляться, и пользователь может не иметь возможности войти в систему. Именно в таком случае команды vipw и vigr приходят на помощь. Команды vipw и vigr используются для безопасного редактирования файлов /etc/passwd и /etc/group в системах Linux. Они будут устанавливать соответствующие блокировки при редактировании файлов /etc/passwd и /etc/group, чтобы другие пользователи не могли вносить в них изменения и избежать повреждения файлов. Когда вы запускаете эти команды с флагом -s, они будут редактировать shadow версии этих файлов, то есть /etc/shadow и /etc/gshadow соответственно. Чтобы безопасно отредактировать файл /etc/group, запустите: sudo vigr. Теперь команды vipw и vigr заблокируют файлы /etc/passwd и /etc/group и не позволят другим пользователям вносить какие-либо изменения. Чтобы убедиться в этом, откройте два окна терминала. Запустите «sudo vipw» в одном окне и попробуйте изменить пароль пользователя в другом окне. Пароль не будет обновлен, пока вы не закроете команду vipw. Поэтому другие пользователи не cмогут случайно или намеренно внсти какие-либо изменения в файл /etc/passwd, пока вы редактируете их от пользователя root. После закрытия /etc/passwd пароль будет успешно обновлен.

Работа команды vigr

Рис. 34: Работа команды vigr

# 5 Выводы

В ходе выполнения лабораторной работы были получены представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

# Список литературы

1. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010.
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — (Системный администратор).
3. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — (Классика Computer Science).
4. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016.
5. Unix и Linux: руководство системного администратора / Э. Немет, Г. Снайдер, Т.Хейн, Б. Уэйли, Д. Макни. — 5-е изд. — СПб. : ООО «Диалектика», 2020.