

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет Информатика и вычислительная техника

(наименование факультета)

Кафедра Кибербезопасность информационных систем

(наименование кафедры)

**ОТЧЕТ**

по лабораторным работам по предмету: Компьютерные сети

Выполнил:

ст. гр. ВКБ31 Котелевец К.А.

Ростов-на-Дону

2025

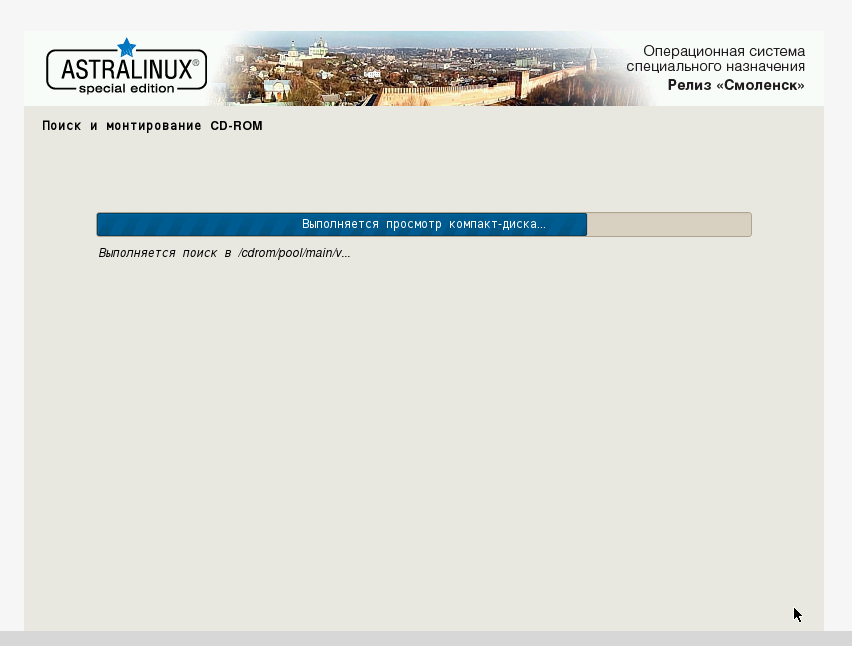
Лабораторная работа 1

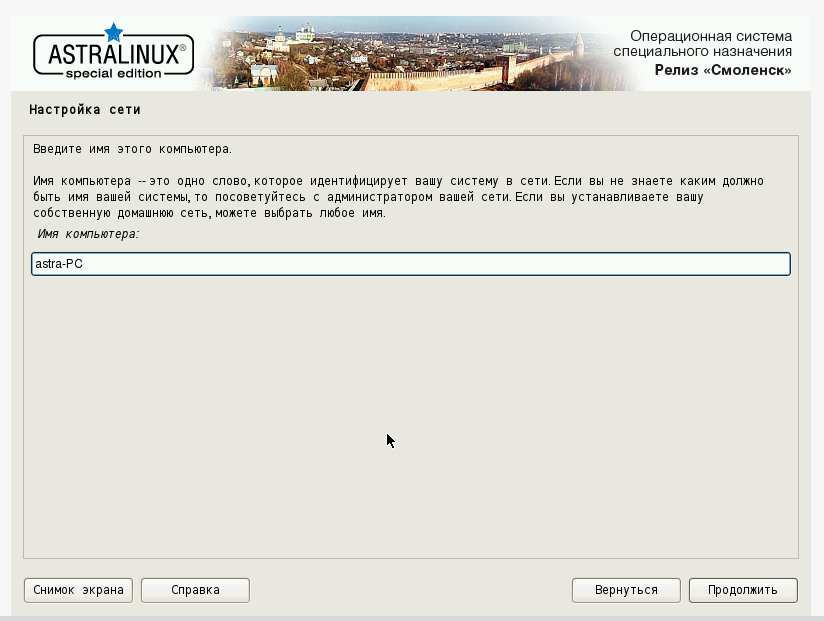
Установка и настройка операционной системы AstraLinuxSE

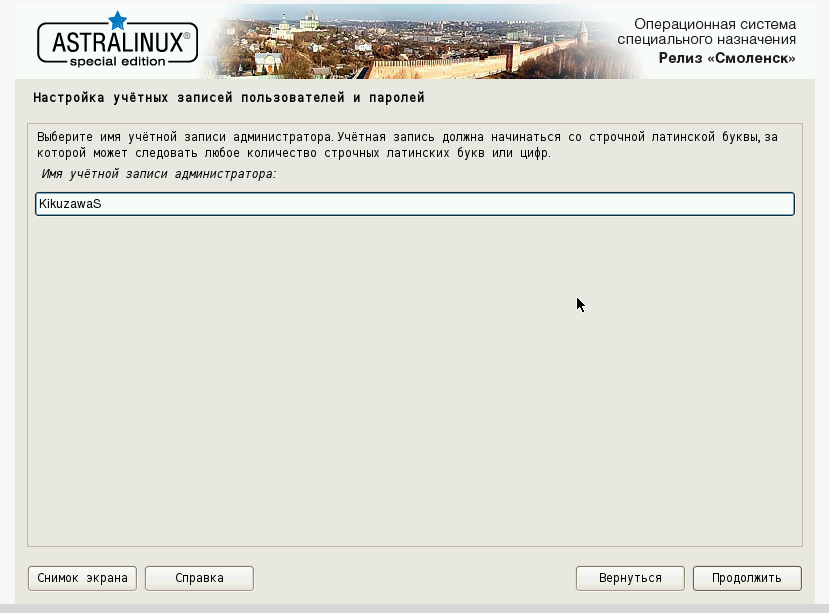
**Цель работы –** изучение требований к целевому компьютеру и подготовка к установке, установка ОС, настройка дополнительных параметров в Astra Linux SE.

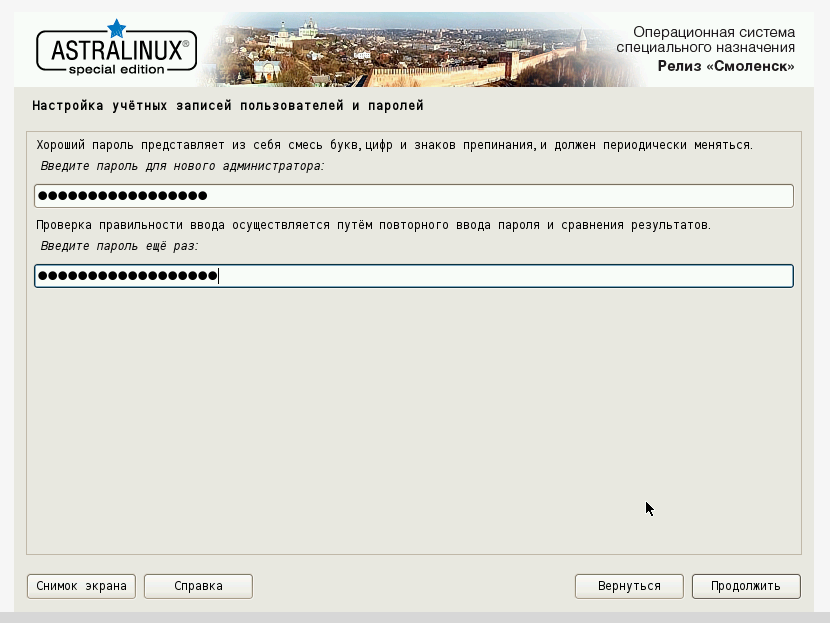
**Ход работы**

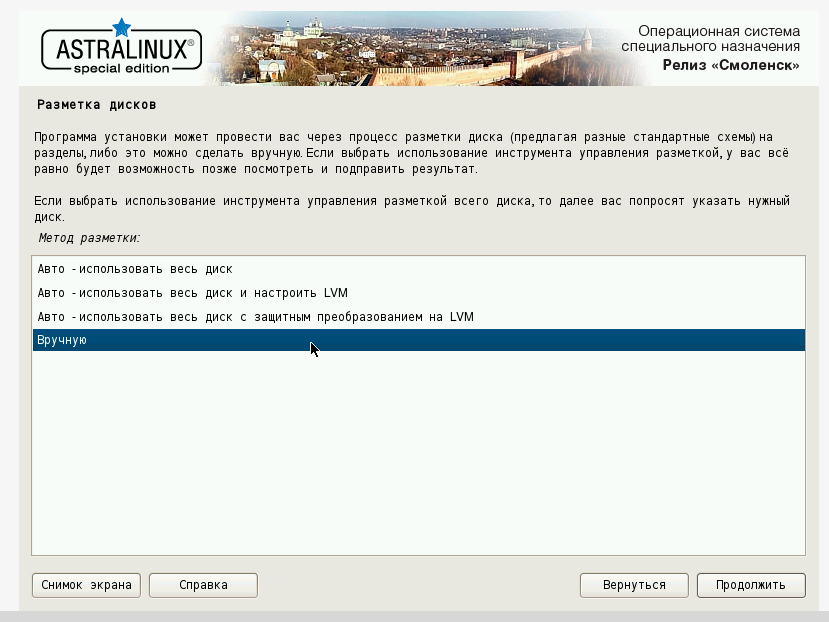
1. Выполнить поэтапную установку Astra Linux SE с **ручной разметкой накопителя!** (уметь рассказать процесс) согласно п. 2 Теоретических сведений.

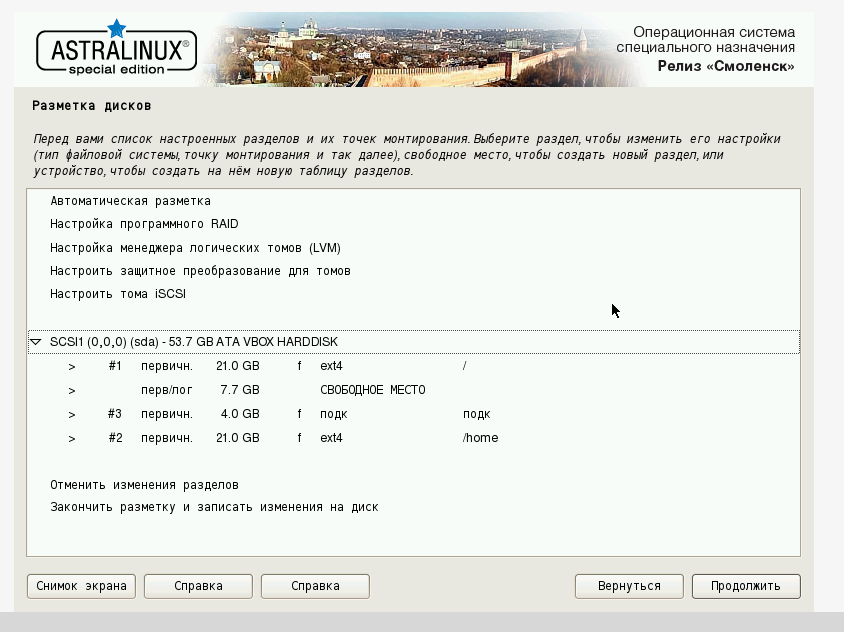




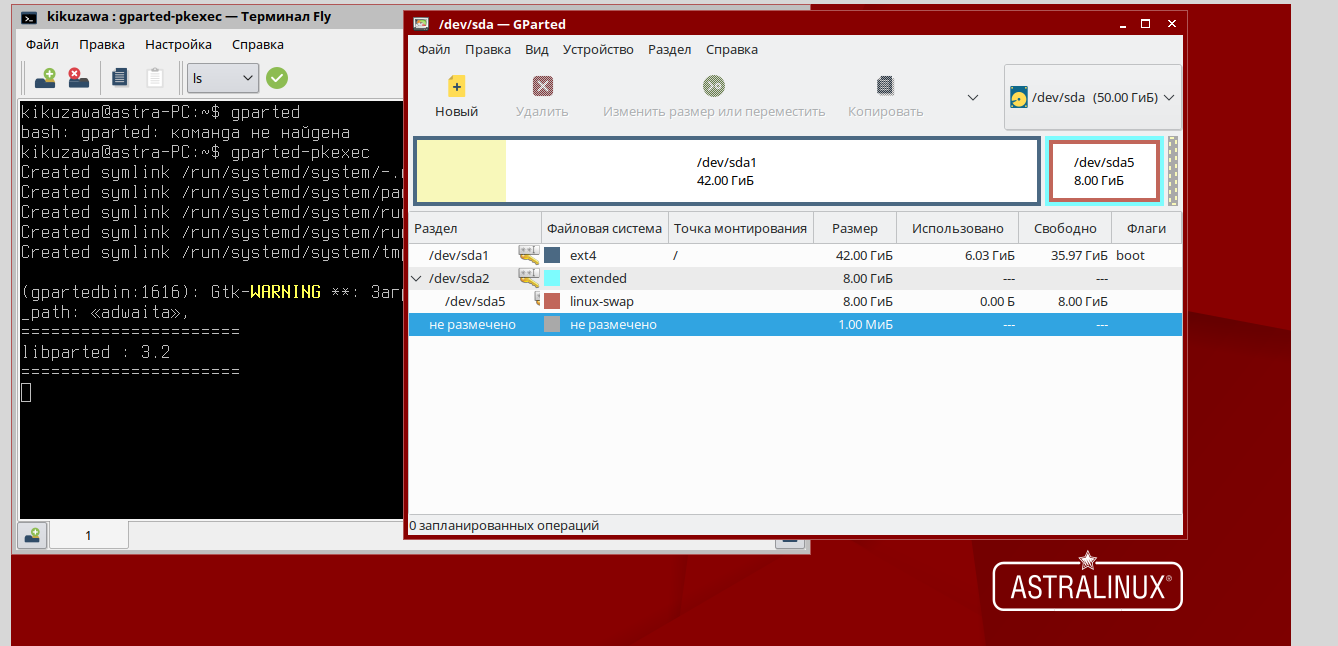








5. Установить и запустить утилиту GParted (сделать скриншот).



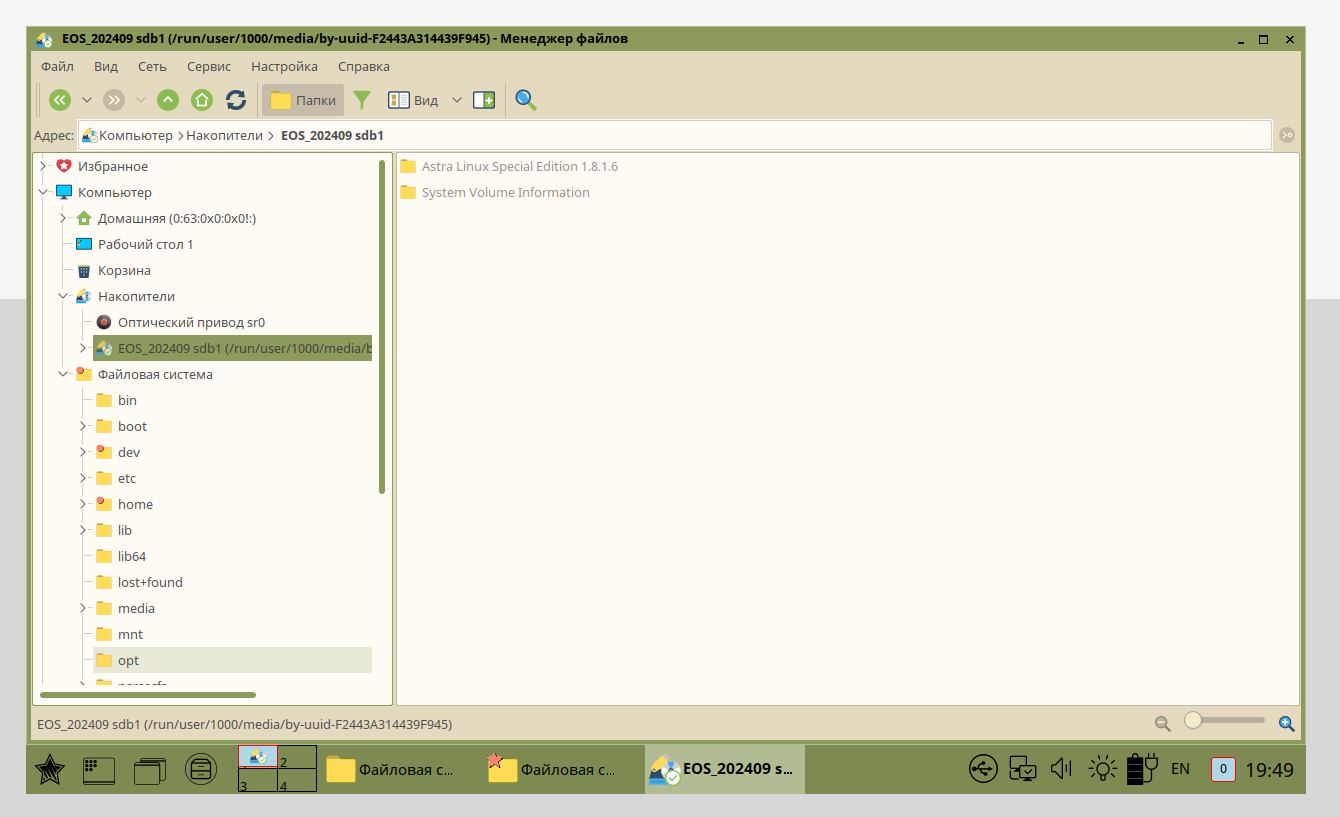
6. Осуществить вход в систему (рассказать типы сессий, меню, все уровни конфидециальности и целостности, категории)

7. Выполнить пользовательские настройки интерфейса работы.

Я ничего не буду менять, меня и так всё устраивает. Поставил для галочки зеленую тему.

8. Показать навыки монтирования/размонтирования сьемных носителей.

На рисунке я показал монтирование флешки



9. Ознакомиться с работой LibreOffice, создать и оформить документы приложений LibreOffice.

Я не буду вставлять сюда скриншоты, я уже этот отчет сделал в LibreOffice

Лабораторная работа №2

Конвейеры И перенаправление ввода-вывода, архивирование и сжатие

Цель работы – научиться работать с командами поиска и архивами. Рассмотреть практические примеры применения конвейеров и использования перенаправления ввода-вывода. Научиться работать с архивами. Изучить утилиты для сжатия и архивирования файлов. Научиться применять данные утилиты совместно с другими командами.

Ход работы:

Задание 1. Найти строку, содержащую слово student в файле /etc/group

Если я введу в терминал команду cat /etc/group | grep “student”, то она ничего не покажет, т.к. просто нет этого слова, однако можно вставить мой никнейм



Задание 2. Отоброзить все строки, содержащие слово root из файлов /etc/passwd и /etc/group



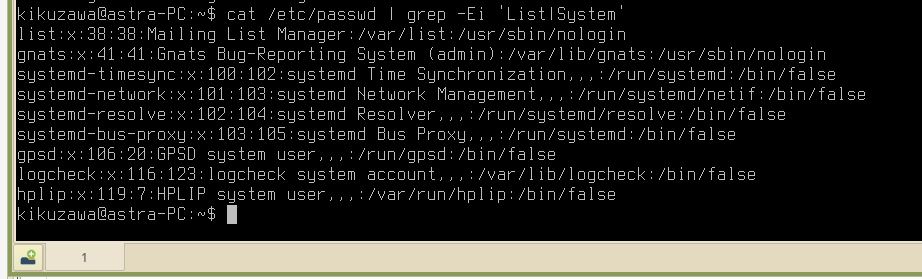
Задание 3. Подсчитать количество строк, в которых содержится пользователь (любой, кроме root) в файле /etc/group



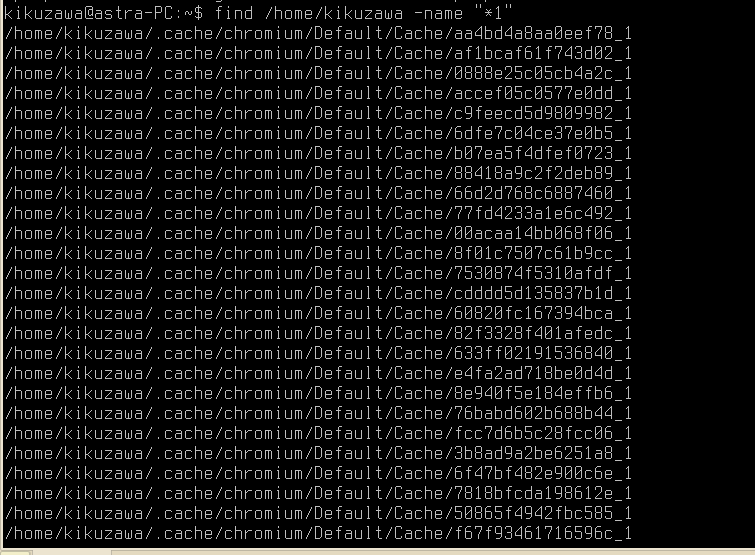
Задание 4. Подсчитать количество строк, в которых не содержатся пользователь в том же файле



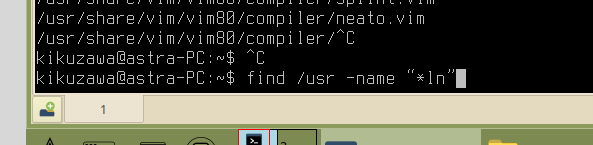
Задание 5. Используя команду grep, отобразить все строки, содержащие слово List или слово System в файле /etc/passwd



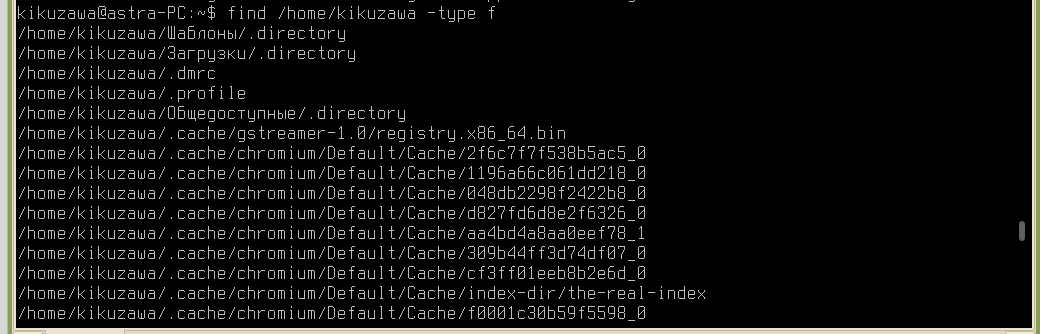
Задание 6. Найти в домашней директории пользователя все файлы и директории, имя которых заканчивается на 1



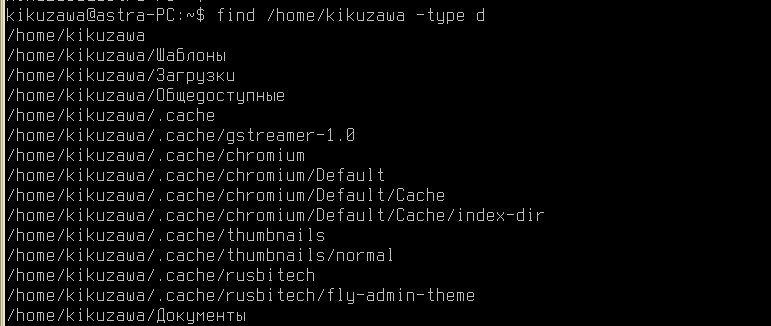
Задание 7. Найдите в директории /usr все файлы и директории ,имя который заканчивается на 1n



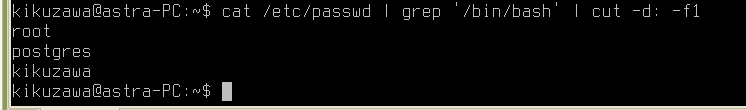
Задание 8. Найдите в домашней директории пользователя student(любого, кроме root) только файлы



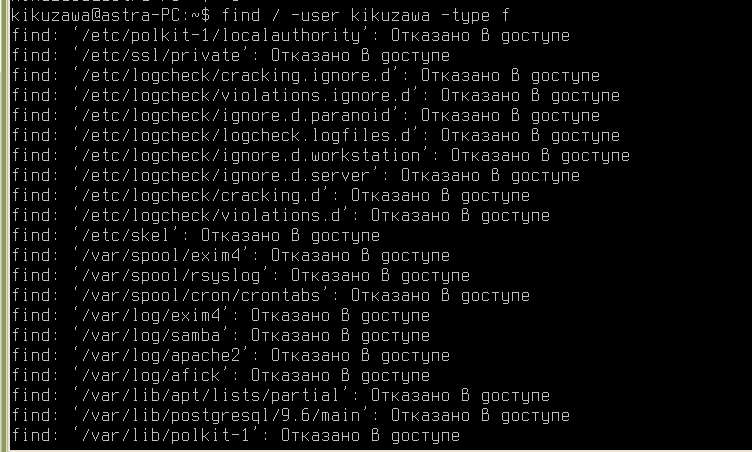
Задание 9. Найдите в домашней директории пользователя только директории



Задание 10. У кого из пользователей в качестве оболочки используется bash

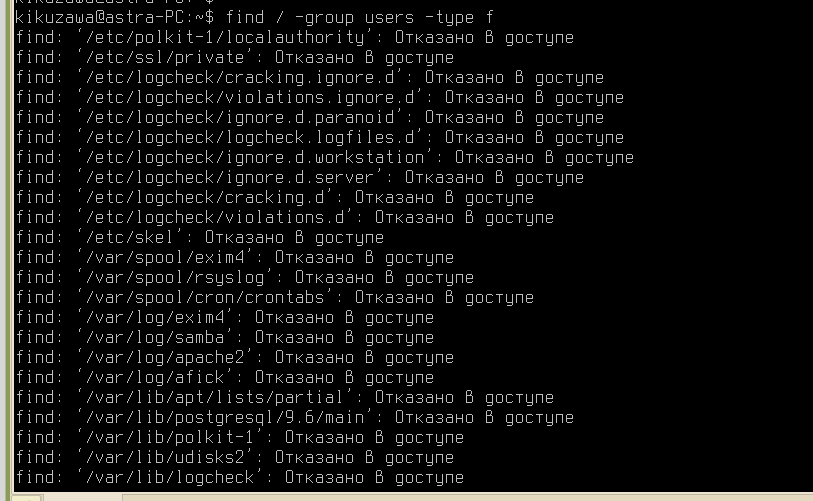


Задание 11. Найдите все файлы, принадлежащие пользователю



Задание 12. Найдите все файлы, принадлежащие любой другой группе,

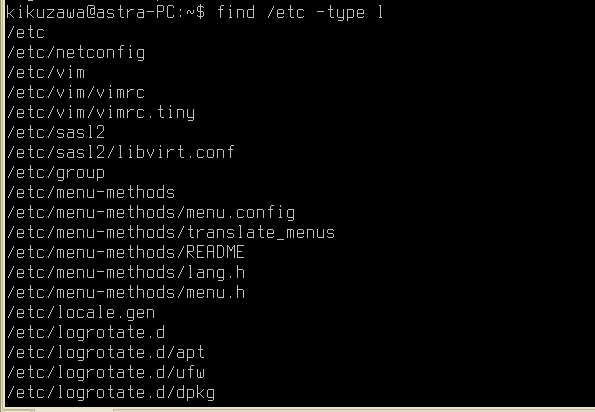
например ftp



Задание 13. Найдите все файлы несуществующих пользователей или групп.

Задание 14. Найдите все файлы, являющиеся символическими ссылками в

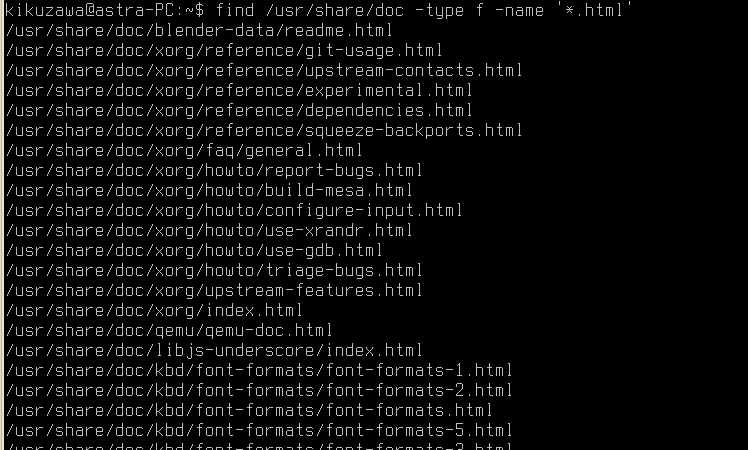
директории /etc



Задание 15. Найдите все файлы в системе размером более 200Mб

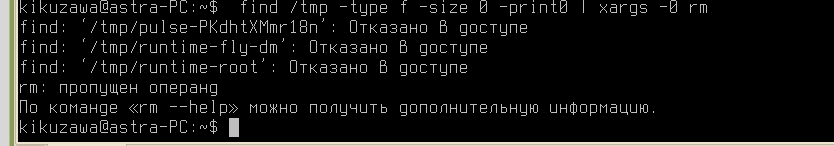


Задание 16. Найдите все файлы с расширением .html в директории /usr/share/doc

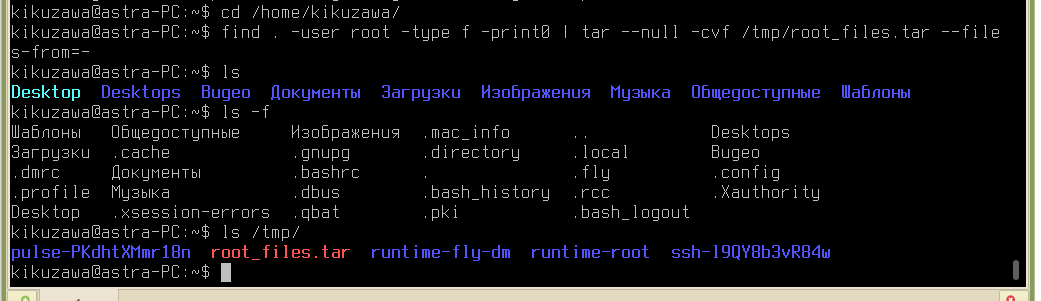


Задание 17. Найдите в директории /tmp файлы нулевого размера, а затем

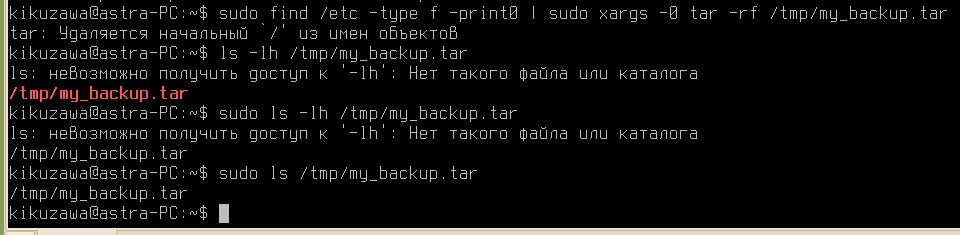
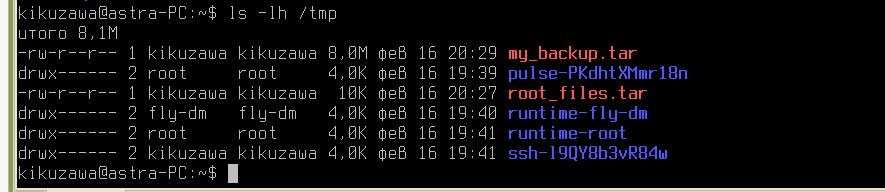
удалите не нужные из них.



Задание 18. . Используйте команду find, чтобы определить местонахождение всех файлов, принадлежащих пользователю root в домашней директории пользователя student, а затем создайте архив с помощью команды tar. Архив должен находиться в каталоге /tmp

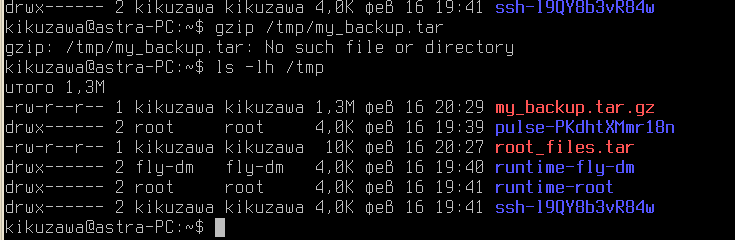


Задание 19. Добавьте содержимое каталога /etc в архив в директорию /tmp. Посмотрите размер полученных файлов (сделать скриншот).

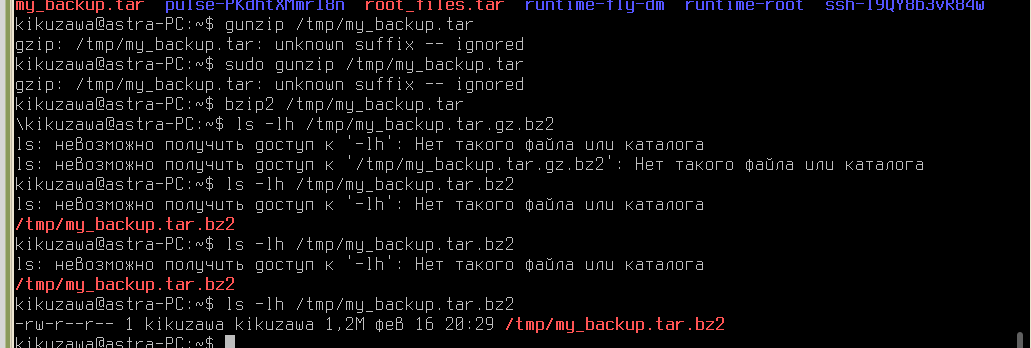
 

Задание 20. Используйте gzip для сжатия ваших архивов и снова посмотрите

получившийся размер файлов.



Задание 21. Отмените сжатие существующих файлов и сожмите их снова с помощью утилиты bzip2, и снова посмотрите размер (сделать скриншот).



Лабораторная работа №3

Управление процессами и планирование

Цель работы – научиться управлять процессами ОС, передавать сигналы процессам. Разобраться в текущем состоянии ОС, насколько система загружена, какие процессы имеют приоритеты. Научиться управлять приоритетами процессов. Рассмотреть разные возможности планирования задач. Научится планировать задания, требующие периодичного выполнения (например, создание бэкапа системы), а также задачи, которые запускаются только один раз в заранее установленное время.

Задание 1.

Из консоли пользователя командой `ps -efl | more` выведите расширенный поэкранный список исполняемых процессов (перечень параметров для расширенного вывода информации можно уточнить с помощью электронного справочника `man`).

Разберитесь с выводимой информацией и объясните преподавателю.

Определите и осуществите вывод процессов согласно выбору преподавателя:

- по типу: системные, демоны, пользовательские (тип процесса определяется по косвенным признакам, в частности, по имени);

- по состоянию S: (исполняющиеся, ожидающие записи на диск, ожидающие событий, приостановленные, зомби);

- по текущему динамическому приоритету `PRI` (наименьшее значение у высокоприоритетных процессов);

- по относительному приоритету `N1`.

Системные процессы (root):

ps -efl | awk 'NR==1{print $0}; $3=="root" {print $0}'

Демоны:

ps -efl | awk 'NR==1{print $0}; $3=="daemon" {print $0}'

Пользовательские процессы:

ps -efl | awk 'NR==1{print $0}; $3=="kikuzawa" {print $0}'

Пример для процессов в состоянии ожидания (D):

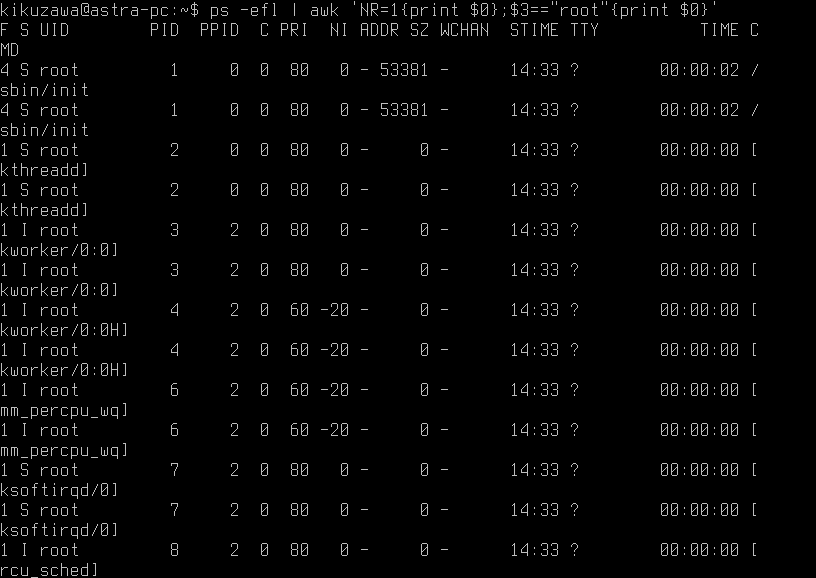
ps -efl | awk 'NR==1{print $0}; $2=="D" {print $0}'

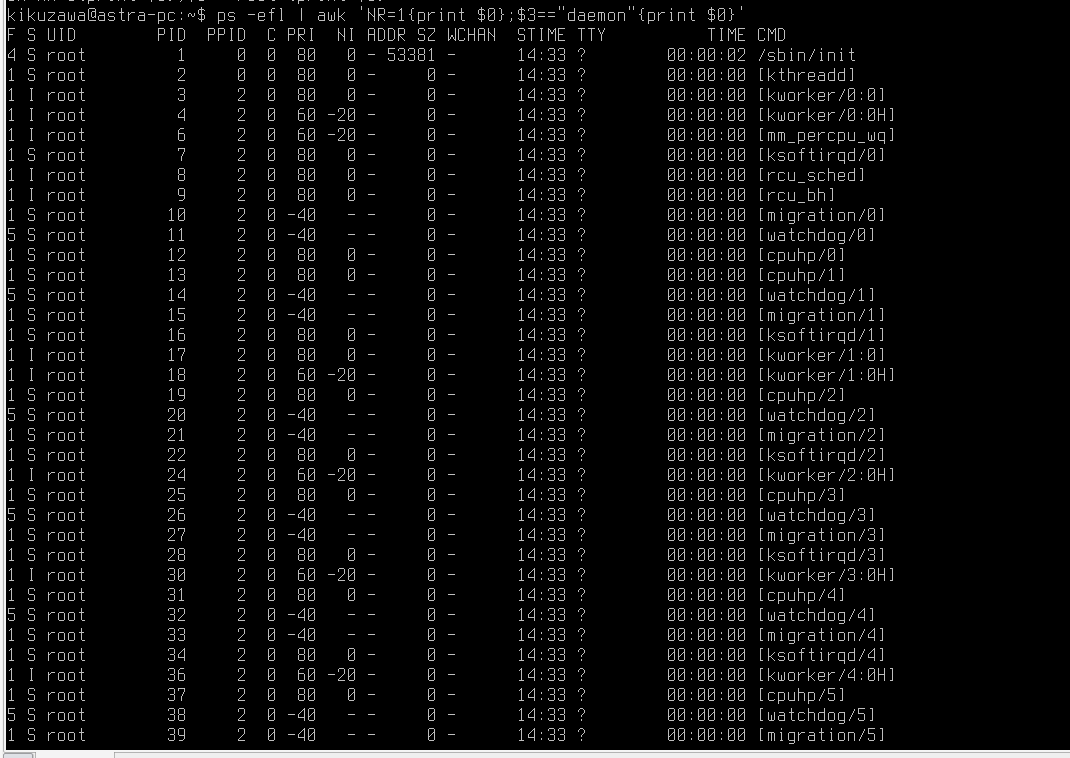
Теперь сделаем вывод по текущему динамическому приоритету PRI.

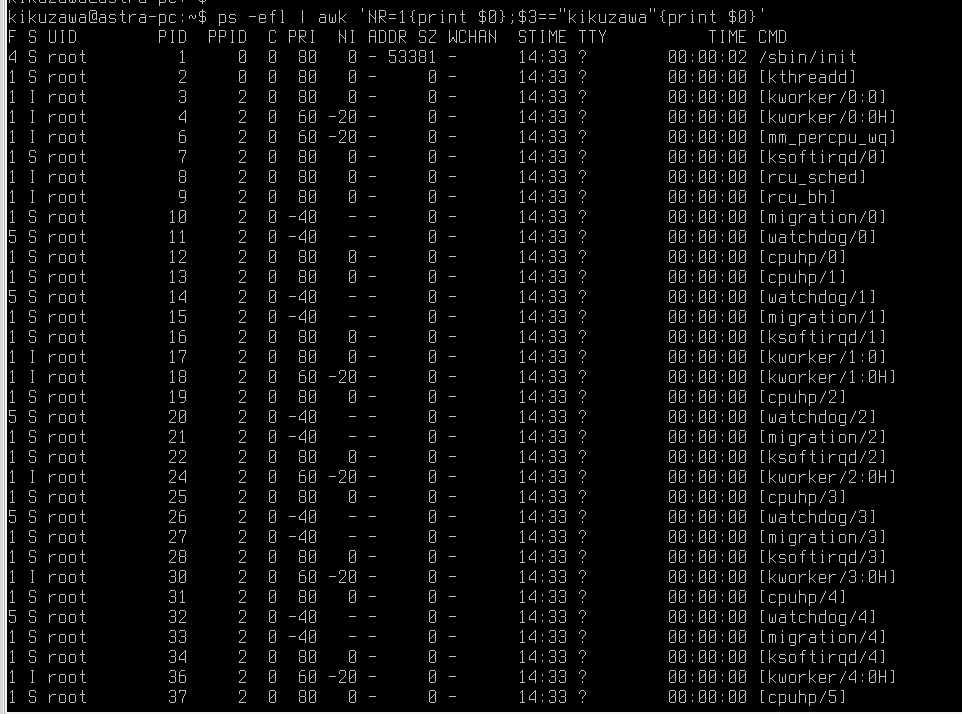
ps -l | sort -k 4

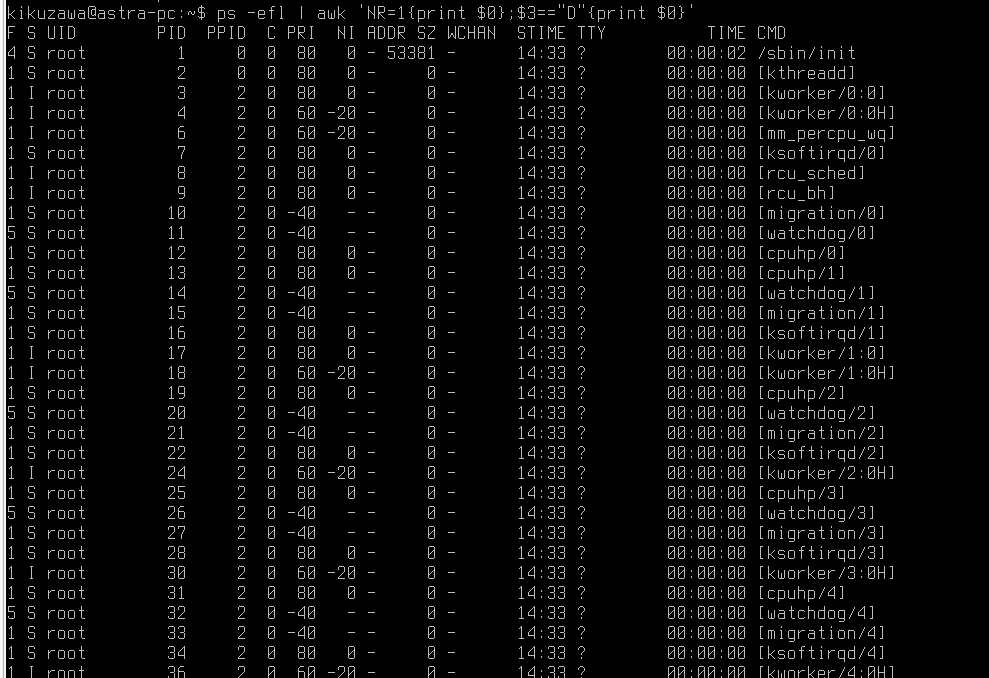
По относительному паритету N1

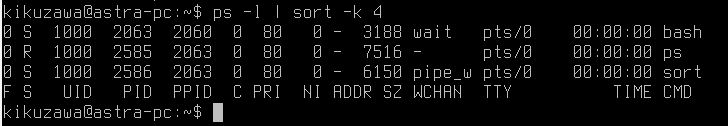
ps -l | sort -k 18

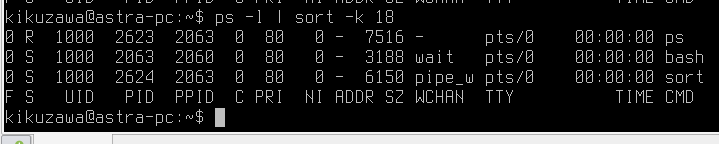












Задание 2.

С помощью `Ctrl+Alt+F2` `(Alt+F2)` откройте второй текстовый терминал и зарегистрируйтесь в нем как суперпользователь, запустите утилиту `top` для текущего контроля процессов.

Чтобы выйти из текстового терминала, нажми `CTRL + ALT + F7`

Задание 3.

Нажатием Ctrl+Alt-Fl (Alt-Fl) вернитесь в первую консоль. Из первой консоли создайте процесс `od /dev/zero > /dev/null`. В соответствии с введенной командой утилита `od` читает и выводит непрерывный поток нулевых байт из «рога изобилия» в нулевое устройство. Переключившись в другую консоль, с помощью команды `top` просмотрите список наиболее активных процессов. Найдите и идентифицируйте запущенный процесс, найдите по идентификатору `PPID` его «родителя», определите его приоритет (возможно это - величина переменная), долю загрузки центрального процессора `%CPU` и оперативной памяти `%МЕМ`.

Команда для удобного копирования: od /dev/zero > /dev/null

Задание 4.

Поочередно из первой и второй консолей с правами администратора и пользователя с помощью команды `od /dev/zero > /dev/null &` создайте по 2-3 одинаковых фоновых процесса. По мере создания новых процессов отслеживайте в третьей консоли их текущий приоритет, загрузку процессора и памяти. Имеются ли различия в приоритете процессов, выполняемых от имени администратора и пользователя?

od /dev/zero > /dev/null &

> `&` - фоновый процесс. Вам нужно 2-3 раза запустить

Чтобы посмотреть появились ли новые процессы, нужно вбить команду ниже:

Top

Чтобы убить процесс, используйте команду ниже:

kill [PID]

> `PID` - уникальный идентификатор процесса

Задание 5.

В консоли пользователя измените приоритет одного из принадлежащих ему процессов. Для этого воспользуйтесь командой `renice -10 PID`. Изменился ли относительный приоритет процесса?

Команда для использования в терминале: renice -10 PID

В `Linux` приоритеты процессов задаются с помощью значений, где более низкие числа означают более высокий приоритет. Таким образом, значение -10 действительно указывает на более высокий приоритет, чем 0. Обычный пользователь не может установить приоритет выше 0.

До этого создайте процесс, используя команду, которая представлена ниже:

od /dev/zero > /dev/null &

У Вас появится снизу `PID`, который вы должны добавить в `renice`. Например, у Вас может быть так:

renice -10 7199

Вы увидете, что ничего не поменялось, потому что не хватает уровня доступа.

Задание 6.

Повторите предыдущий пункт с правами администратора и ответьте на вопрос.

Команда для использования в терминале: sudo renice -10 PID

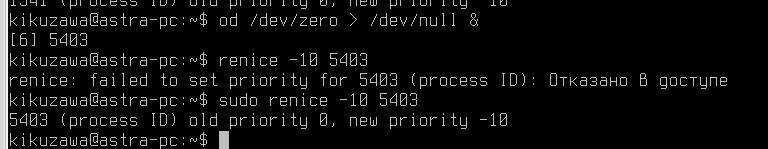
Задание 7.

Переключитесь в консоль пользователя и измените приоритет одного из принадлежащих ему процессов командой `renice 5 PID`. Произошло ли изменение приоритета?

Воспользуйтесь командой ниже: renice 5 -p PID

Здесь произошло изменение приоритета, так как у нас значение не меньше 0. Для пользователя такое вполне допустимо.

Для проверки приоритета можете воспользоваться командой ниже: ps -l -p PID



Задание 8.

Проконтролируйте из третьей консоли изменение приоритетов запущенных процессов. Что произошло?

Тут абсолютно разное поведение могло произойти. Для открытия 3 терминала, воспользуйтесь сочетанием клавиш,

которое представлено ниже:

CTRL + ALT + F3

Задание 9.

Удалите созданные процессы командой `kill`.

Посмотрите `ID` созданных процессов до этого. Теперь можете выполнить удаление.

Теперь перейдем к возможным вариантам удаления. Выбирайте любую команду на ваш вкус:

- `kill [PID1] [PID2] [PID3]`

- `killall od`

- `pkill -f 'od /dev/zero > /dev/null'`

- `killall -9 od`

- `pkill -9 -f 'od /dev/zero > /dev/null'`

> `-9` - сильный сигнал принудительного завершения

Лично я использовал 1 команду, где явно задаются `ID` для удаления процессов.

Задание 10.

С правами пользователя создайте в своей директории сценарий с именем `abсd`. Сценарий можно создать с помощью редактора `nano`

Перейдите в удобную Вам директорию, используя команду `cd`, пример представлен ниже:

cd /path/to/your/directory

Теперь создайте файл `abcd` в редакторе `nano`. Для этого в терминале просто вбейте команду: nano abcd

После этого вставьте код, который представлен ниже:

```bash

#! /bin/bash

while :

do

echo HELLO!

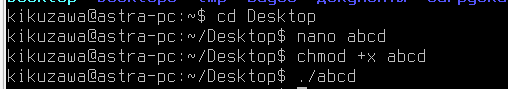
done

```

Теперь нам нужно сделать файл выполняемым, для этого вбейте команду, которая представлена ниже:

chmod +x abcd

Ну и для запуска воспользуйтесь командой, которая представлена ниже: ./abcd



Задание 11.

Используя команду `chmod`, присвойте пользователю полные права на чтение, запись и исполнение данного сценария. Запустите сценарий на исполнение (на экран должны непрерывно выводиться приветствия `HELLO!`)

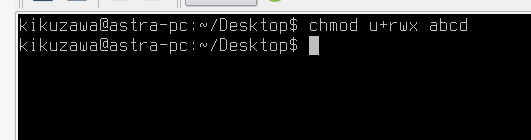
Мы уже до этого создали файл, нам нужно выдать полные права на выполнение. Для этого воспользуйтесь командой ниже:

chmod u+rwx abcd

> Здесь `u` обозначает владельца (`user`), `+rwx` добавляет права на чтение (`r`), запись (`w`) и исполнение (`x`).

Теперь для запуска скрипта можете воспользоваться командой, которая представлена ниже:

./abcd



Задание 12.

Перейдите в третью консоль, с помощью команды top просмотрите список процессов и найдите в нем «зависший» процесс, запущенный пользователем (на самом деле это только имитация зависания, которое пользователь легко может прекратить сам). Прочитайте идентификатор процесса PID.

Опять-таки все описано в условии. Команда, которой Вам нужно воспользоваться: top

Задание 13.

Нажатием Ctrl+C из второй консоли остановите процесс. Как изменилось при этом состояние процесса?

Он перестает окончательно работать, падает полностью нагрузка, после этого процесс пропадает с экрана.

Как же это происходит?

Когда вы нажимаете `CTRL + C`, то ОС отправляет сигнал `SIGINT`, который по умолчанию предназначен для прерывания сигнала.

Бывает такое, что процесс может переопределить данный сигнал для своего поведения.

Задание 14.

Повторно запустите из второй консоли процесс, перейдите в первую консоль и отправьте "зависшему" процессу сигнал на останов (команда kill -15 PID\_process).

Перейдем во 2 консоль. Для этого используйте комбинацию клавиш, которая представлена ниже: CTRL + ALT + F2

Как только перешли во вторую консоль, набираем команду в терминале для запуска процесса.

Это будет тот же наш скрипт, который до этого писали: ./abcd

Теперь перейдем в 1 консоль. Для этого используйте комбинацию клавиш, которая представлена ниже: CTRL + ALT + F1

Теперь остается Вам только убить процесс, узнав заранее его идентификатор.

kill -15 PID

> `PID` - номер процесса, его можно узнать через `top`

> `kill - 15 PID` - стандартное

Задание 15.

Перейдите в другую консоль и отправьте процессу сигнал kill -20 PID. Как реагирует процесс на данный сигнал? Что означает данный сигнал?

Перейдем во 2 консоль. Для этого используйте комбинацию клавиш, которая представлена ниже: CTRL + ALT + F2

Как только перешли во вторую консоль, набираем команду в терминале для запуска процесса.

Это будет тот же наш скрипт, который до этого писали: ./abcd

Теперь перейдем в 1 консоль. Для этого используйте комбинацию клавиш, которая представлена ниже: CTRL + ALT + F1

Теперь остается Вам только убить процесс, узнав заранее его идентификатор. kill -20 PID

> `PID` - номер процесса, его можно узнать через `top`

> `kill -20 PID` - сигнал временного завершения (заморозка процесса). Обычно такое можно повторить с помощью `CTRL + Z`.

Задание 16.

С помощью команды kill -9 PID отправьте этому процессу сигнал принудительного завершения. С другой консоли проконтролируйте выполнение команды. Остановился ли процесс? Остался ли он в списке процессов? Какая программа на самом деле перехватывает и исполняет команду kill -9 PID?

Перейдем во 2 консоль. Для этого используйте комбинацию клавиш, которая представлена ниже: CTRL + ALT + F2

Как только перешли во вторую консоль, набираем команду в терминале для запуска процесса.

Это будет тот же наш скрипт, который до этого писали: ./abcd

Теперь перейдем в 1 консоль. Для этого используйте комбинацию клавиш, которая представлена ниже: CTRL + ALT + F1

Теперь остается Вам только убить процесс, узнав заранее его идентификатор.

kill -9 PID

> `PID` - номер процесса, его можно узнать через `top`

> `kill -9 PID` - принудительное завершение без перехвата.

Задание 17

С помощью команды `echo $PATH` поочередно из консоли администратора и пользователя `userl` выведите список директорий, в которых производится поиск исполняемых файлов, заданных только по имени. В чем заключается различие выведенных списков? Почему в списке `PATH` администратора отсутствует текущий каталог (.)? Почему в списке `PATH` пользователя отсутствует каталог `/sbin`? Имеет ли пользователь возможность изменить порядок проверки каталогов для администратора?

Я, так понимаю, нового пользователя создавать не надо. Работаем дальше под текущим.

Введите команду для вывода директорий в консоли: echo $PATH

Почему в списке `PATH` у администратора отсутствует текущий каталог?

Исключение текущего каталога из `PATH` для администратора является мерой безопасности.

Путь администратора обычно включает директории, содержащие системные и административные утилиты, такие как `/sbin`, `/usr/sbin`.

Эти каталоги содержат программы для управления системой, которые не предназначены для запуска не привилегированными пользователями.

Почему в списке `PATH` пользователя отсутствует каталог `sbin`?

Каталог `/sbin` и подобные ему (`/usr/sbin`, `/usr/local/sbin`) содержат программы для администрирования системы,

которые обычно не предназначены для использования обычными пользователями.

Пользователь не может напрямую изменить порядок проверки каталогов для администратора без соответствующих привилегий.

Однако любой пользователь может изменить свой собственный `PATH`, используя команды типа `export PATH=...` в своем

`.bashrc`, `.bash\_profile` или других конфигурационных файлах оболочки.

Задание 18.

Попробуйте запустить несколько утилит из второй консоли с правами пользователя (например, `renice -10 PID`, `date -s O`). Как реагирует система на ваши попытки? Опишите.

Чтобы сменить приоритет на высокий, нужно пользоваться командой: renice -10 PID

> `PID`- номер процесса.

> Команда `renice` изменяет приоритет запущенных процессов.

Чтобы сменить время на начало эпохи `Unix`, нужно: date -s O

> Вместо '0' может быть любое значение в секундах, начиная с эпохи `Unix`

Попытка обычного пользователя изменить данные параметры приводит к ошибке. Для этого нужно `sudo`.

Задание 19.

Перейдите в административную консоль и повторите запуск утилит с правами суперпользователя. Что произошло?

Чтобы сменить приоритет на высокий, нужно пользоваться командой: sudo renice -10 PID

> `PID`- номер процесса.

> Команда `renice` изменяет приоритет запущенных процессов.

Чтобы сменить время на начало эпохи `Unix`, нужно: sudo date -s O

> Вместо '0' может быть любое значение в секундах, начиная с эпохи `Unix`

Всё получилось, в связи с тем, что у нас есть права суперпользователя.

Система не ограничивает попытки.

Задание 20.

Убедитесь в том, что пользователю разрешен запуск указанных утилит. Объясните, почему пользователь не может запустить утилиты с некоторыми «критичными» параметрами? Где, по вашему мнению, расположен механизм контроля за ходом запуска (в ядре операционной системы, в командной оболочке, в самой утилите?). Ответ обоснуйте.

Опять-таки приведу пример с `renice`, который пользователь может запускать, но с определенным параметрами выдает ошибку.

renice 5 PID

> `PID`- номер процесса.

> Команда `renice` изменяет приоритет запущенных процессов.

В итоге почему так происходит? Происходит в целях безопасности, чтобы пользователь просто так систему не навернул.

Где же в итоге тогда защита? На каком слое в ОС? Тут первичным фильтром выступает сама оболочка и программа.

Они предоставляют дополнительные уровни проверки, но это зачастую бывает недостаточно, поэтому ядро выступает главным

контроллером.

Ядро операционной системы является ключевым компонентом в контроле за ходом запуска и выполнения команд,

поскольку именно оно имеет доступ ко всем ресурсам системы и контролирует права доступа на самом низком уровне.

Командная оболочка и отдельные программы могут предоставлять дополнительные уровни проверки, но они действуют в рамках

правил и ограничений, установленных ядром. Это обеспечивает, что даже если внешний уровень (например, оболочка или приложение)

подвергнется компрометации, низкоуровневый контроль защиты, предоставляемый ядром, останется в силе.

Задание 21.

С правами пользователя скопируйте в свой рабочий каталог один из исполняемых файлов с параметром `SUID` каталога `/bin` (исполняемые файлы выделены цветом и символом \*, а параметр `SUID` отмечен символом «s» в правах владельца на исполнение). Как изменились права доступа к файлу после его копирования?

> Бит `SUID` (Set User ID) — это специальный бит в Unix-подобных операционных системах,

> который позволяет исполняемым файлам запускаться с правами владельца файла, а не с правами пользователя,

> который запустил файл.

> Это может быть полезно для выполнения программ, которые требуют повышенных привилегий для выполнения определенных операций.

Как найти файл, где есть SUID? Воспользуйтесь командой ниже: ls /bin | grep '^...s'

Я же лично буду использовать для копирования команду `ping`. Пример команды для копирования представлена ниже: cp /bin/ping ~/my\_directory/

Что же происходит когда мы копируем в домашний каталог? В таком случае сбрасывается `SUID`.

Сделано в целях безопасности.

Задание 22.

Из второй консоли с правами пользователя скопируйте в свой домашний каталог утилиту, которую разрешено запускать только администратору (например, `chattr`). Копирование производите с параметрами, гарантирующими переход копии во владение пользователю. Убедитесь и покажите, что пользователь имеет на скопированный файл все необходимые права.

Перейдем во вторую консоль, для этого используем сочетание клавиш:

CTRL + ALT + F2

Теперь скопируем `chattr` с правами пользователя, для этого воспользуйтесь командой ниже: cp /usr/bin/chattr ~/chattr\_copy

> Если не пропускает, то используйте ещё `sudo` перед командой

Теперь назначим права, для этого воспользуйтесь командами ниже:

```bash

sudo chown $USER:$USER ~/chattr\_copy

chmod +x ~/chattr\_copy

```

Проверьте права доступа, вбив команду ниже: ls -l ~/chattr\_copy

Попробуем воспользоваться, для этого выполните набор команд, который представлен ниже:

```bash

touch ~/test\_file

~/chattr\_copy +i ~/test\_file

```

Вывод: не все утилиты будут функционировать корректно, если они предполагают взаимодействие с системными файлами или

требуют глобальных изменений в системе, что выходит за рамки прав обычного пользователя.

Задание 23.

Настроить на запуск однократно некоторую задачу в определенное время. Вы также должны наметить другую задачу, которая стартовала бы каждые десять минут (между 8:00 и 17:00). Задачи выбрать самостоятельно.

В `Linux` есть две утилиты, которые позволяют запускать задачи на конкретное время.

- `at` - для однократных задач, запланированных на конкретное время. Задача запускается один раз. То же самое, что и таймер.

- `cron` - для периодических задач. То есть задача запускается каждый раз в определенный период.

Давайте создадим скрипты, которые можно будет потом использовать для запуска.

Для однократной задачи:

```bash

#!/bin/bash

echo "One-time script executed at $(date)" > result.txt

```

Для периодической задачи:

```bash

#!/bin/bash

echo "Periodic script executed at $(date)" > result.txt

```

> Перед запуском каждого скрипта установите ему права на запуск, используя команду `chmod +x <name>`, где `name` - это название `sh` скрипта.

Теперь для установки однократной задачи используйте пример ниже:

at 12:00 <<< "[path/to/script]"

> `path/to/script` - это абсолютный путь к скрипту.

Теперь для установки периодической задачи будем использовать команды ниже: crontab -e

В конце файла добавьте строку, как показано ниже: \*/10 8-17 \* \* \* [path/to\_script]

> Это путь к скрипту, который нужно вставить.

> `cron` и `at` на `Astra Linux` 1.8 не работают нормально, они не могут открывать приложения, выводить результат в консоль.

> Методом проб и ошибок нашли, что они нормально могут только записывать в `txt` файл.

Задание 24.

Создать напоминание, например, о встрече с Х в 12:00, сегодня. Войдите в систему как `root` и введите следующие команды: `at noon`; <Нажмите Enter > `echo "Time for meet with Х."` <Нажмите Enter > <После завершения нажмите ctrl-D>. Проверьте очередь заданий, используя команду `atq`.

> Выполняйте последовательно команды, которые я описал ниже.

1. Заходим под основной учетной записью, то есть под администратором в учетную запись.

2. Открываем терминал, используя комбинацию `CTRL + ALT + F1`

3. Вбиваем команду `at noon`

4. Теперь вбиваем команду `echo "Time for meet with X."`

5. Нажимаем комбинацию клавиш `CTRL + D`

6. Проверяем очередь, вбивая в терминал команду: `atq`

Задание 25.

Настройте получение информации о статусе системы каждые десять минут.

Для начала, нам нужно зайти, как суперпользователь. Для этого вбейте в терминале команду ниже: su root

Теперь откроем планировщик задач в терминале, для этого воспользуйтесь командой, которая представлена ниже: crontab -e

Укажите строку, которая представлена ниже: \*/10 8-17 \* \* \* /usr/bin/free >> /root/free.txt

> Данная команда выводит информацию о доступной и использованной памяти,

> а потом перенаправляет ее вывод в файл `/root/free.txt`

После этого нажмите `CTRL + D`

Результат можно увидеть теперь в файле, для этого в терминале вбейте команду, которая представлена ниже: cat /root/free.txt

Задание 26.

Выполните задачи: убедиться, что каталог, где сохраняются задания at, пуст; проверить время и дату в терминале; запланировать создание файла в корневом каталоге через две минуты;

Произведем настройку задания с использованием `at`

> Убедитесь, что каталог, где сохраняются задания `at`, пуст.

> Это можно проверить командой `atq`.

> Если есть задания, их можно удалить с помощью `atrm` <номер задания>.

Теперь проверьте текущее время и дату в терминале. Вы можете использовать команду ниже: date

Зачем мы проверяли дату и время? Неизвестно. Ведь можно, не зная текущее время, поставить на выполнение скрипт: echo "touch /root/testfile.txt" | at now + 2 minutes

> Выше представлен пример команды, которая запланирует создание файла через 2 минуты.

Теперь посмотрите наличие того, что у Вас добавлена задача в очередь. Для этого используйте команду, которая представлена ниже: atq

> Проверьте каталог, где собираются задания в очереди на выполнение.

> Обычно это `/var/spool/at` или `/var/spool/cron/atjobs`, в зависимости от вашей системы.

> Вы должны увидеть новый файл, который представляет задание.

Контрольные вопросы по Astra Linux

1. Имеются ли различия в приоритете процессов, выполняемых от имени администратора и пользователя?

Да, в Astra Linux (как и в других Unix-подобных системах) процессы, выполняемые от имени администратора (root), могут иметь более высокие приоритеты доступа к системным ресурсам по сравнению с процессами, запущенными обычным пользователем. Это связано с тем, что администратору необходимо обеспечить бесперебойную работу критически важных системных процессов.

2. Как изменяется относительный приоритет процесса?

Относительный приоритет процесса можно изменить с помощью команды `nice` и `renice`. Команда `nice` задает начальный приоритет для нового процесса, а `renice` изменяет приоритет уже запущенного процесса. Чем ниже значение nice (от -20 до 19), тем выше приоритет процесса.

3. Почему в списке PATH администратора отсутствует текущий каталог (.)?

Текущий каталог (.) отсутствует в PATH администратора для повышения безопасности. Это предотвращает случайный запуск вредоносных программ из текущего каталога, что может привести к компрометации системы.

4. Почему в списке PATH пользователя отсутствует каталог /sbin?

Каталог `/sbin` содержит системные утилиты, которые обычно используются администратором для управления системой. Обычным пользователям не требуется доступ к этим утилитам, поэтому `/sbin` не включен в их PATH.

5. Имеет ли пользователь возможность изменить порядок проверки каталогов для администратора?

Нет, обычный пользователь не может изменить порядок проверки каталогов в PATH администратора. Это связано с ограничениями прав доступа: только администратор может изменять системные настройки, включая PATH.

6. Где расположен механизм контроля за ходом запуска утилит (в ядре операционной системы, в командной оболочке, в самой утилите?)

Механизм контроля за ходом запуска утилит расположен в \*\*командной оболочке\*\*. Именно оболочка интерпретирует команды, ищет исполняемые файлы в каталогах, указанных в PATH, и запускает их.

7. Покажите, какие основные три процесса наиболее потребляют ресурсы на вашем компьютере?

Для просмотра процессов, потребляющих наибольшее количество ресурсов, можно использовать команду `top` или `htop`. В верхней части вывода будут отображены процессы, потребляющие больше всего CPU и памяти. Пример: top

8. Покажите, присутствуют ли на вашей машине процессы-зомби?

Процессы-зомби можно найти с помощью команды `top` или `ps`. В `top` они обозначаются как "Z" в колонке состояния. Пример: ps aux | grep 'Z'

9. Назначение Cron и Anacron.

- Cron используется для планирования периодических задач, которые должны выполняться в определенное время (например, ежедневно, еженедельно).

- Anacron предназначен для выполнения задач, которые должны запускаться с определенной периодичностью, но не требуют точного времени запуска (например, на машинах, которые не работают 24/7).

10. Crontab и at применение.

- Crontab используется для создания, редактирования и управления расписанием выполнения задач.

- At позволяет запустить задачу однократно в указанное время.

11. С помощью какой команды пользователь может составить расписание для запуска периодических заданий?

Для составления расписания используется команда `crontab -e`. Она открывает редактор для редактирования файла crontab пользователя.

12. Какой командой можно увидеть активные таймеры?

Активные таймеры можно увидеть с помощью команды `systemctl list-timers`. Она покажет все запланированные таймеры systemd, включая те, которые связаны с cron и anacron.

Пример:

systemctl list-timers

Лабораторная работа 4

Управление пользователями и правами

Цель работы – Научится администрировать учетные записи пользователей: создавать, удалять менять политики доступа. Изучить на практике дискреционные полномочия. Научится работать с правами доступа и расширенными списками ACL на файлы и директории.

Ход работы:

1. Просмотрите в файле /etc/passwd поля с информацией о пользователях вашей системы.

a) Какой символ используется для разделения полей в /etc/passwd?

b) Сколько полей используется для описания каждого пользователя?

c) Сколько пользователей в вашей системе?

|  |
| --- |
| Для выполнения задания используйте команду, которая представлена ниже:  cat /etc/passwd  а) Какой символ используется для разделения полей в /etc/passwd  Используется символ :.  б) Сколько полей используется для описания каждого пользователя?  Используется 7 полей. Например, root:x:0:0:root:/root:/bin/bash.  Что за нотация для описания пользователей в данном файле?  c) Сколько пользователей в вашей системе?  Чтобы узнать количество пользователей в системе, используйте команду, которая представлена ниже:  wc -l /etc/passwd  wc -l подсчитывает количество строк в файле /etc/passwd. |

2. Сколько различных входных оболочек используется в вашей системе?

|  |
| --- |
| Входная оболочка (или интерактивная оболочка) — это программа, которая предоставляет пользователю интерфейс для взаимодействия с операционной системой через командную строку. Для просмотра различных входных оболочек можете использовать команду ниже:  cut -d ":" -f 7 /etc/passwd | sort | uniq | wc -l  Более подробное объяснение про данную команду  Если попросят вывести все оболочки, то используйте команду: cut -d ":" -f 7 /etc/passwd |

3. Второе поле в /etc/passwd хранит пароли пользователей в закодированной форме. Если поле пароля содержит букву х, то ваша система использует теневые пароли и хранит закодированные пароли в другом месте.

Применяются ли в вашей системе теневые пароли?

|  |
| --- |
| Для проверки наличия технологии теневых паролей, можно использовать команду ниже:  cut -d ":" -f 2 /etc/passwd | grep "x" | wc -l  Если у Вас вывелось не 0, а любое другое положительное число, то у Вас есть теневые пароли, а значит и включена данная технология.  Что делает данная команда?  cut -d ":" -f 2 /etc/passwd  cut: Команда, используемая для извлечения определенных полей из строк текста.  d ":": Указывает, что разделителем полей является двоеточие (:). В файле /etc/passwd поля разделены именно этим символом.  f 2: Указывает, что нужно извлечь 2-е поле из каждой строки. В файле /etc/passwd это поле соответствует хешу пароля пользователя (или x, если хеш хранится в другом месте, например, в файле /etc/shadow).  /etc/passwd: Это файл, из которого мы извлекаем данные. Таким образом, эта часть команды извлекает 2-е поле (хеш пароля) для каждого пользователя из файла /etc/passwd.  | grep "x"  |: Оператор конвейера, который передает вывод предыдущей команды (результат cut) в качестве ввода для следующей команды (grep).  grep "x": Эта команда ищет строки, содержащие символ x. В контексте файла /etc/passwd, если в 2-м поле стоит x, это означает, что хеш пароля хранится в другом месте (обычно в файле /etc/shadow).  Таким образом, результатом выполнения всей команды будет список пользователей, у которых в файле /etc/passwd в поле хеша пароля стоит x, что указывает на то, что их пароли хранятся в файле /etc/shadow.  Теневые пароли по умолчанию включены в Astra Linux SE Смоленск |

4. Добавьте трех новых пользователей с соответствующими домашними директориями: student7, student8, student9. Задайте пароли для каждого из них.

|  |
| --- |
| Создаем пользователя student7:  sudo useradd -m student7  Создаем пользователя student8:  sudo useradd -m student8  Создаем пользователя student9:  sudo useradd -m student9  Задаем пароль для student7:  sudo passwd student7  Задаем пароль для student8:  sudo passwd student8  Задаем пароль для student9:  sudo passwd student9  Если у Вас вылетело предупреждение. Система предупреждает, но не запрещает использовать данный пароль. Просто вбейте его ещё раз. Я, например, использовал пароль 123. |

5. Создайте группу course и добавьте в нее всех трех пользователей.

|  |
| --- |
| Создаем группу, используя команду ниже:  sudo groupadd course  Теперь добавляю пользоватля student7:  sudo usermod -aG course student7  Теперь добавляю пользоватля student8:  sudo usermod -aG course student8  Теперь добавляю пользоватля student9:  sudo usermod -aG course student9  usermod -aG - добавляет пользователя в указанную группу (или группы). Сразу всех пользователей через 1 команду нельзя добавить, то есть такая запись sudo usermod -aG course student7 student8 student9 не сработает.  Теперь сделаем проверку. Например, проверим к какой группе относится student 7, для этого используйте команду ниже:  groups student7  Данная команда позволяет узнать к какой группе относится пользователь. |

6. Для пользователя student7 выставите ограничение: срок действия пароля 5 месяцев и предупреждение об окончании срока действия пароля 7 дней.

|  |
| --- |
| Задаем время действия пароля, используя команду ниже:  sudo chage -M 150 student7  -M 150: Эта опция устанавливает максимальный срок действия пароля в 150 дней. Это означает, что пользователь student7 должен будет изменить свой пароль не реже чем раз в 150 дней. Если пользователь не изменит пароль в течение этого времени, он не сможет войти в систему до тех пор, пока не изменит пароль.  sudo chage -W 7 student7  -W 7: Эта опция устанавливает период предупреждения о необходимости смены пароля. В данном случае, если срок действия пароля истекает, пользователь student7 будет предупрежден за 7 дней до истечения срока действия пароля. Это означает, что за 7 дней до того, как пароль станет недействительным, пользователь получит уведомление о том, что ему нужно изменить пароль. |

7. Заблокируйте пользователя student8. Проверьте, что блокировка

подействовала.

|  |
| --- |
| Для блокировки пользователя student8 используйте команду ниже:  sudo usermod -L student8  Теперь распишу 2 возможных сценария проверки, что пользователь заблокирован.  Вариант 1: проверка через /etc/shadow  Здесь идея в том, чтобы проверить по метасимволам о состоянии пользователя  sudo grep "^student8:" /etc/shadow  Если строчка начинается так: student8:! - то пользователь заблокирован.  Вариант 2: попробовать зайти на пользователя через терминал (CTRL + ALT + F2)  Здесь Вас в терминале попросит ввести логин и пароль. После того, как вы введете данные, то у вас выведется в терминале Password Blocked.  В терминале - приложение Konsole - не разрешает переключать пользователей через команду sudo su - username. |

8. Войдите в систему под пользователем student9. Создайте два новых файла file1 и file2 и две новых директории dir1 и dir2.

|  |
| --- |
| Откройте терминал через комбинацию клавиш (CTRL + ALT + F2), у вас попросят ввести логин и пароль, здесь как раз вводим данные для student9.  Теперь создадим файл file1:  touch file1  Создадим файл file2:  touch file 2  Создадим директорию dir1:  mkdir dir1  Создадим директорию dir2:  mkdir dir 2  Теперь остается проверить тот факт, что файлы и директории созданы. Для этого используйте команду, которая представлена ниже:  ls -l |

9. Войдите в систему под пользователем root. Сделайте file1 исполняемым. Запускаться файл должен от имени владельца и группы файла. Установите в качестве владельца файла file1 пользователя student7 и группу course.

|  |
| --- |
| Так у Вас 2 варианта, как можно переключиться на root:  Вариант 1: через терминал, который открывается через кобминацию (CTRL + ALT + F<number>), где number принимает значения от 1 до 6. Там вам нужно будет вбить дальше только логин и пароль. После этого sudo su Вариант 2: через терминал, которое открывается через приложение Konsole. Здесь дальше вам надо будет ввести комбинацию sudo su.  Задаём исполнябщий файл, для этого используем команду ниже:  sudo chmod +x /home/student9/file1  Задаём права запуска для нашего file1, команды представлены ниже:  В начале задаем исполнение от имени владельца файла, используя команду ниже:  sudo chmod u+s /home/student9/file1  Теперь задаем от имени группы, используя команду ниже:  sudo chmod g+s /home/student9/file1  Теперь устанавливаем владельца файла:  chown student7:course /home/student9/file1  Для проверки того, что все применилось можно использовать команду, которая представлена ниже:  ls -l /home/student9/file1 |

10. Войдите в систему под пользователем student7. Попробуйте перейти в директорию пользователя student9 и сделать запись в файле file1.

|  |
| --- |
| Чтобы войти под пользователем student7 откройте терминал через комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6.  После того, как вы ввели свои данные, используйте команду, которая представлена ниже:  cd /home/student9  Note  Если вы все сделали правильно до этого, то вас не пустит перейти в данную директорию. Даже с использоваем sudo у вас не получится, так как вы сейчас находитесь под аккаунтом обычного пользователя, а не root. |

11. Войдите в систему под пользователем root. Разблокируйте пользователя student8. Проверьте, что блокировка снята.

|  |
| --- |
| Чтобы восстановить пользователя, нам нужно задать ему пароль. Для этого используйте команду, которая представлена ниже:  sudo passwd student8  Для проверки того, что блокировка снята есть 2 способа, которые я изложу ниже:  Вариант 1 - посмотреть его существование в /etc/shadow, здесь используем команду, которая представлена ниже:  sudo grep "^student8:" /etc/shadow  Вариант 2 - попробовать войти на аккаунт student8 через терминал, который открывается через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6. Здесь вам нужно будет ввести логин и пароль. |

12. Управление учетными записями пользователей. Создайте в ОС Linux двух пользователей (user1 и user2) и задайте их пароли. Зарегистрируйтесь в первой консоли как userl.

|  |
| --- |
| Для создания user1 используйте команду, которая представлена ниже:  sudo useradd -m user1  Для создания user2 используйте команду, которая представлена ниже:  sudo useradd -m user2  Задаем пароль для user1, для этого используем команду, которая представлена ниже:  sudo passwd user1  Задаем пароль для user2, для этого используем команду, которая представлена ниже:  sudo passwd user2  Теперь вам нужно обязательно открыть терминал, который появляется при нажатии комбинации (CTRL + ALT + F<number>), где number - это число от 1 до 6. В открывшимся окне введите данные пользователя user1. После удачной аутентификации у вас появится командная строка для user1. |

13. С помощью Ctrl+Alt+F2 (Alt+F2) откройте второй текстовый терминал и зарегистрируйтесь как user2.

|  |
| --- |
| Открываем терминал, используя комбинацию CTRL + ALT + F2. Введите логин и пароль.  Note  Если вы уже в этом окне были зарегистрированы под другим пользователем, то используйте команду sudo su user2, чтобы перейти под аккаунт user2. |

14. Аналогично откройте третий текстовый терминал и зарегистрируйтесь в нем с правами суперпользователя.

|  |
| --- |
| Открываем третий терминал, используя комбинацию CTRL + ALT + F3. В нем введите данные суперпользователя.  Note  Суперпользователь - это самый первый пользователь, которого вы создавали, когда устанавливали Astra Linux. |

15. Нажатием Ctrl+Alt-Fl (Alt-Fl) вернитесь в первую консоль. Теперь, переключая консоль, вы можете работать с объектами операционной системы от имени двух разных пользователей и администратора системы. Основная часть задания выполняется с правами обычного пользователя. Переходите в третью консоль и используйте права root только при выполнении соответствующих пунктов задания.

|  |
| --- |
|  |

16. С правами userl попробуйте войти в каталог /root. Объясните результат. С помощью команды ls -la / просмотрите список основных каталогов и укажите, каких прав доступа вам недостает для входа в каждый из каталогов.

|  |
| --- |
| Заходим из-под user1 в терминале, который открывается через комбинацию (CTRL + ALT + F<number>). Если у Вас уже было занято другим пользователем, то используйте комнаду, которая представлена ниже:  sudo su user1  После того, как вы удачно аутентифицировались, то попробуйте перейти в root. Используйте команду, которая представлена ниже:  cd /root  Note  Если у вас до этого было выполнено все правильно, то вас не пропустит.  Теперь вводим команду, которую попросили в условии. Представлю её здесь для вашего удобства:  ls -la /  После того, как вы используете данную команду, то у вас будет что-то похожее на это:  drwxr-xr-x 2 root root 4096 Oct 26 10:00 bin  drwxr-xr-x 3 root root 4096 Oct 26 10:00 boot  drwxr-xr-x 20 root root 3260 Oct 26 10:00 dev  drwxr-xr-x 74 root root 4096 Oct 26 10:00 etc  drwxr-xr-x 3 root root 4096 Oct 26 10:00 home  Note  Расскаху, что за символы в первой колонке. Объяснения символов написаны слева направо, поэтому есть два раза r-x.  d: Указывает, что это директория.  rwx: Права для пользователя (в данном случае, root).  r-x: Права для группы (в данном случае, группа root).  r-x Права для всех остальных пользователей. |

17. Переключитесь в консоль администратора и создайте два новых временных каталога mkdir -m 777 /home/temp1 и mkdir -m 1777 /home/temp2. Проверьте права доступа к каталогам /home/user 1 и /home/user2: они должны быть установлены в 755. Вернитесь в консоль user1.

|  |
| --- |
| Открываем терминал, который называется Konsole, через него входим за root. Для этого используйте команду:  sudo su  Important  Представленные команды ниже у меня не работают в терминале, который открывается через комбинацию (CTRL + ALT + F<number>).  Note  Если вы введете без имени пользователя после su, то Linux умолчанию переключается на root.  Создадим теперь временные каталог temp1:  sudo mkdir -m 777 /home/temp1  Создадим теперь временный каталог temp2:  sudo mkdir -m 1777 /home/temp2  Теперь проверяем права директорий других пользователей.  Для user1 используйте команду, которая представлена ниже:  ls -ld /home/user1  У меня, например, вывелось такое: drwx------ 4 user1 user1 4096 фев 13 18:31 /home/user1.  Что тут вывелось?  Для user2 используйте команду, которая представлена ниже:  ls -ld /home/user2  Если права не установлены в 755, то это надо исправлять.  Задаем права доступа 755 для user1:  sudo chmod 755 /home/user1  Задаем права доступа 755 для user2:  sudo chmod 755 /home/user2 |

18. Пользуясь командой mkdir, создайте в домашнем каталоге пользователя /home/userl четыре каталога с именами: qul, qu2, qu3, qu4. При создании каталогов объявите следующие права доступа к ним: (qul - 777, qu2 - 404, qu3 - 1333, qu4 - 505. Пример: cd; mkdir -m 777 qu1). С помощью команды ls /home/userl убедитесь в том, что каталоги созданы. Какие из предоставленных прав кажутся Вам лишенными смысла? Почему?

|  |
| --- |
| Заходим за пользователя user1 в терминале, который открывается через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6. Теперь заходим за пользователя user1. Если вы до этого находились за другим пользователем, то перейдите за user1 используя команду, которая представлена ниже:  sudo su user1  Создаем директорию qu1, используя команду ниже:  mkdir -m 777 qu1  Создаем директорию qu2, используя команду ниже:  mkdir -m 404 qu2  Создаем директорию qu3, используя команду ниже:  mkdir -m 1333 qu3  Создаем директорию qu4, используя команду ниже:  mkdir -m 505 qu4  Проверяем теперь, что директории созданы:  ls -l /home/user1  У меня такое вот вывело:  qu1 (777): drwxrwxrwx  Note  Владелец: Чтение, запись, выполнение.  Группа: Чтение, запись, выполнение.  Группа: Чтение, запись, выполнение.  Комментарий: Дает полный доступ к каталогу всем пользователям.  qu2 (404): dr--r--r--  Note  Владелец: Чтение.  Группа: Чтение.  Остальные: Чтение.  Комментарий: Каталог доступен только для чтения. Владелец не может в нем создавать и удалять файлы, что весьма странно.  qu3 (1333): d-wxrwxrwx  Note  Владелец: Запись, выполнение.  Группа: Чтение, запись, выполнение.  Остальные: Чтение, запись, выполнение.  Комментарий: Владелец не может просматривать содержимое директории. Это странно, но это не мешает никому другому, включая владельца, модифицировать содержимое.  qu4 (505): dr-xr-xr-x  Note  Владелец: Чтение, выполнение.  Группа: Чтение, выполнение.  Остальные: Чтение, выполнение.  Комментарий: Директория доступна только для чтения и выполнения.  Каталоги с правами, кажущимися лишенными смысла, и почему:  qu2 (404): Эти права доступа кажутся наиболее странными и бессмысленными. Владелец каталога имеет только право на чтение, но не имеет прав на запись и выполнение. Это означает, что владелец каталога не может создавать новые файлы или подкаталоги, удалять существующие файлы или изменять права доступа к ним. Практически, это делает каталог бесполезным для владельца, так как он не может в нем ничего менять. Обычно, владельцу директории нужно как минимум право записи, чтобы иметь возможность управлять файлами внутри.  qu3 (1333): Владелец каталога имеет права на запись и выполнение, но не имеет права на чтение. Это означает, что владелец каталога может создавать новые файлы или подкаталоги, удалять существующие файлы или изменять права доступа к ним, но не может просматривать список файлов и подкаталогов внутри каталога. Хотя это и менее интуитивно, чем с каталогом qu2, можно представить себе сценарии, где это может иметь смысл (например, специальный каталог для обмена файлами, где пользователь должен положить файл, но не имеет права видеть, что там уже лежит). Но, безусловно, это нестандартная конфигурация. |

19. Задайте права доступа к файлам "по умолчанию". Для этого установите umask 022.

Поясните, какие права к вновь создаваемым файлам и каталогам будут предоставляться пользователю, членам его группы и остальным.

|  |
| --- |
| Открываем терминал, который Konsole и вводим команду, которая представлена ниже:  umask 022  Note  После ввода данной команды в терминал у Вас ничего не выведет, это вполне нормально.  Что вообще делает данная команда?  0 - никакие права не удаляются у пользователя.  2 - удаляется право на запись (w) у группы.  2 - удаляется право на запись (w) у остальных пользователей.  Права доступа по умолчанию:  Для файлов права по умолчанию - 666 (rw-rw-rw-)  Для каталогов права по умолчанию - 777 (rwxrwxrwx) |

20. В каждом из каталогов создайте по три текстовых файла с именами81(jan, feb, mar), (apr, may, jun), (jul, aug, sep), (oct, nov, dec). В каждый файлзапишите календарь на определенный месяц текущего года. Например,команда cal 1 2021 > jan создает в текущем каталоге файл jan и записывает внего календарь на январь 2021 года. Не забывайте, что использованиеотносительного (короткого) имени файла требует, чтобы вы находились внужном каталоге. В противном случае следует указывать полный путь ксоздаваемому файлу. Для навигации по каталогам используйте команды cd иpwd. В каком случае создание файлов не удалось? Почему?

|  |
| --- |
| Important  После активации даже других репозиториев в synaptic у меня не получилось скачать cal  В каталоге qu1 создаем (jan, feb, mar), испльзуя команды ниже:  cd /home/user1/qu1  date > jan  date > feb  date > mar  В каталоге qu2 создаем (apr, may, jun), используя команду ниже:  cd /home/user1/qu2  date > apr  date > may  date > jun  В каталоге qu3 создаем (jul, aug, sep), используя команду ниже:  cd /home/user1/qu3  date > jul  date > aug  date > sep  В каталоге qu4 создаем (oct, nov, dec), используя команду ниже:  cd /home/user1/qu4  date > oct  date > nov  date > dec  Important  И если вы сделали все правильно, то при попытке создать файлы в qu2 и qu4 вам откажут в доступе. Так надо, так как в предыдущих заданиях на директорию qu2 и qu4 были заданы права 404, 505. В случае qu3 можно записать файл, но нельзя просмотреть. |

21. С помощью команды chmod измените нужные права доступа в "недоступные" каталоги qu2, qu4 и создайте там указанные файлы. После этого верните каталогам прежние права доступа.

|  |
| --- |
| Меняем права к директории qu2, используя команду ниже:  sudo chmod 777 /home/user1/qu2  Меняем права к диретории qu4, используя команду ниже:  sudo chmod 777 /home/student9/qu4  Создаем файлы в нужных директориях теперь:  date > /home/user1/qu2/apr  date > /home/user1/qu2/may  date > /home/user1/qu2/jun  date > /home/user1/qu4/oct  date > /home/user1/qu4/nov  date > /home/user1/qu4/dec  Меняем права на прежние:  sudo chmod 404 /home/user1/qu2  sudo chmod 505 /home/user1/qu4  Note  Вместо user1 у вас может быть любой пользователь, за которого вы создали директории и файлы. |

22. С помощью команд cd и ls войдите в каждый из созданных каталогов и просмотрите список созданных файлов. Для просмотра каталога необходимо последовательно ввести две команды: cd и ls. При просмотре используйте два режима: ls без аргументов и ls -l. В каких случаях не удалось войти в каталог? В каких случаях не удалось посмотреть список файлов? Почему?

|  |
| --- |
| Сначала попробуем с директорией qu1:  cd /home/user1/qu1  ls /home/user1/qu1  ls -l /home/user1/qu1  Теперь попробуем для директории qu2:  cd /home/user1/qu2  ls /home/user1/qu2  ls -l /home/user1/qu2  Теперь попробуем для директории qu3:  cd /home/user1/qu3  ls /home/user1/qu3  ls -l /home/user1/qu3  Теперь попробуем для директории qu4:  cd /home/user1/qu4  ls /home/user1/qu4  ls -l /home/user1/qu4 |

23. Прочитайте содержимое одного из файлов в "темном" каталоге (например, cd /home/user1/qu3; cat aug). Сделайте выводы.

|  |
| --- |
| Считываем содержимое файла:  sudo cat /home/user1/qu3/aug  Important  Если вы сделали все правильно, то вам откажут в доступе при просмотре директории, но при просмотре файла все будет видно.  Вывод: разные права могут по-разному влиять на взаимодействие с файлами. В данном случае права доступа позволяли на просмотр содержимого директории, но не на чтение этих же файлов. |

24. Перейдите во 2-ю консоль и с правами пользователя user2 войдите в каталог /home/user1/qul. Создайте в каталоге /home/user2 новый файл quart1 путем конкатенации нескольких имеющихся (cat jan feb mar >/home/user2/quartl). С помощью команды fi le определите тип созданного файла. Попробуйте вывести его на экран командой cat. Что представляет собой данный файл?

|  |
| --- |
| Заходим во второй терминал, используя комбинацию (CTRL + ALT + F<number>), где number - это номер от 1 до 6. там переключитесь на пользователя user2.  За нового пользователя переходим в /home/user1/qu1  Note  Вместо user1 может быть абсолютно другой пользователь, за которого вы до этого создали директории qu1 и т.п.  Создаем новый файл, как указано в методичке. Команду представлю ниже:  cat jan feb mar > /home/user2/quart1  Выводы:  Тип файла: Файл /home/user2/quart1 является текстовым файлом, содержащим конкатенацию содержимого файлов jan, feb и mar.  Содержимое файла: Содержимое файла представляет собой последовательность календарей за январь, февраль и март.  Права доступа: Тот факт, что пользователь user2 смог прочитать файлы jan, feb и mar из каталога /home/user1/qu1, подтверждает, что права доступа к этому каталогу позволяют любому пользователю читать файлы в нем. Возможность создать файл /home/user2/quart1 в домашнем каталоге пользователя user1 подтверждает, что у пользователя user1 есть права на запись в свой домашний каталог.  Note  В моем случае не совсем календарь, потому что команда cal не работает.  Вместо пользователей user1, user2 могут быть пользователи, которые вам удобны. |

25. С помощью команды chmod установите права доступа 077 на созданный файл quart1. Вновь попробуйте прочесть его. Ответьте, почему владельцу файла запрещается доступ, если файл доступен для всех? Что необходимо сделать, чтобы вернуть владельцу права на доступ?

|  |
| --- |
| Открываем терминал через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6. Для выполнения команды используйте команду ниже:  chmod 077 quart1  Что обозначают цифры в команде?  Первая цифра 0: это права для владельца. В данном случае она равна 0, что означает, что специальные права не установлены.  Вторая цифра 7: это права для группы. 7 в восьмеричном формате означает, что группа имеет все права: чтение (4) + запись (2) + исполнение (1) = 7.  Третья цифра 7: это права для других пользователей.  Выводы: Не получится прочитать его по тем причинам, потому что мы поставили 0 для владельца файла в команде chmod. Чтобы вернуть владельцу права на доступ, надо поставить 7 вместо 0. |

26. Установите для файла quatrl права на доступ 4700. Кому и какие права вы при этом предоставили? Как воспользоваться этими правами? Какие из предоставленных прав не имеют смысла?

|  |
| --- |
| Задаём новые права. Для этого используйте команду, которую я представил ниже:  chmod 4700 /home/user2/quart1  Что за права доступа?  Разбор прав доступа 4700: Восьмеричное представление прав доступа 4700 состоит из четырех цифр:  4: Это бит SUID (Set User ID).  7: Права для владельца (чтение, запись, выполнение).  0: Права для группы (нет прав).  0: Права для остальных (нет прав).  SUID: Бит SUID (Set User ID) имеет эффект только для исполняемых файлов (программ). Когда исполняемый файл с установленным битом SUID запускается, процесс, созданный из этого файла, получает права владельца файла, а не пользователя, который запустил файл.  Note  Вместо пользователя user2 может быть абсолютно другой пользователь, который удобен вам. |

27. Перейдите в консоль администратора и передайте право владения на файлы may и aug пользователю user2 (команда chown). Поочередно из консолей userl и user2 проверьте, как изменились права владения файлами после его передачи. Может ли пользователь user2 воспользоваться предоставленными правами?

|  |
| --- |
| Important  Чтобы задать нового владельца для таких файлов нужно зайти за root в терминале, который открывается через комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Попробуем поменять владельца. В моем случае изначально был владелец этих файлов user1, нам нужно, чтобы user2 стал владельцем. Для этого используем команду, которая представлена ниже:  Меняем владельца may, используя команду ниже:  chown user2 /home/user1/qu2/may  Меняем владельца aug, используя команду ниже:  chown user2 /home/user1/qu3/aug  Теперь проверяем выданные права, используя команду, которая представлена ниже:  ls -l  Note  Если всё было выполнено правильно, то вам откажут в доступе. Почему? Изначально на на эти файлы заданы права 404 и 505 соответственно, которые позволяют создавать файлы, но не считывать.  У вас могут абсолютно другие пользователи. Здесь я представил пользователей, которые я использую. |

28. С правами пользователя userl из каталогов /home/temp1 и /home/temp2 с по мощью команды ln создайте две "жесткие" ссылки на файл dec с именами dec\_h1 и dec\_h2 (пример: ln /home/user1/qu4/dec /home/templ/dec\_hl). Чем созданные ссылки отличаются от исходного файла? На сколько байт уменьшилось дисковое пространство после создания этих ссылок?

|  |
| --- |
| Important  Зайдите в терминал, используя комбинацию (CTRL + ALF + F<number>), где number - это число от 1 до 6. Если вы были за другим пользователем, то вам нужно ввести команду exit, после чего вводите свой логин и пароль.  Теперь создаем жесткие ссылки за user1, используя команды, которые представлены ниже:  ln /home/user1/dec /home/temp1/dec\_h1  ln /home/user1/dec /home/temp2/dec\_h2  Теперь проверяем эти файлы:  ls -l /home/user1/qu4/dec  ls -l /home/temp1/dec\_h1  ls -l /home/temp2/dec\_h2  Чем созданные ссылки отличаются от исходного файла?  Жесткие ссылки - это не просто “ярлыки” или “указатели” на файл. Жесткая ссылка — это другое имя для того же самого файла. Все жесткие ссылки (включая исходное имя файла) указывают на один и тот же inode на диске.  На сколько байт уменьшилось дисковое пространство после создания этих ссылок?  Дисковое пространство не уменьшилось. Создание жестких ссылок не приводит к уменьшению используемого дискового пространства. Жесткие ссылки — это просто дополнительные указатели на существующие данные на диске. Они добавляют записи в каталоги, но не дублируют сами данные. Жесткая ссылка занимает немного места в таблице каталогов (inode) для хранения имени файла и указателя на inode. Это место очень мало по сравнению с объемом, который занимает сам файл. |

29. С помощью команды ln -s создайте из каталогов /home/temp1 и /home/temp2 две символические ссылки на файл dec с именами dec\_sl и dec\_s2. Чем отличаются созданные ссылки от исходного файла? Попытайтесь прочитать содержимое файлов символических ссылок. Что они собой представляют?

|  |
| --- |
| Important  Я пользовался терминалом, который находится в приложении Konsole.  Создаём символические ссылки, используя команду ниже:  Сначала dec\_s1:  ln -s /home/user1/qu4/dec /home/temp1/dec\_s1  Потом уже на dec\_s2:  ln -s /home/user1/qu4/dec /home/temp2/dec\_s2  Note  Вместо user1 у вас может быть абсолютно другой пользователь. Главное выбирайте того пользователя, под котормым создали файлы dec, mar и т.п.  Проверяем теперь ссылки, используя команды ниже:  В начале на dec\_s1:  readlink /home/temp1/dec\_s1  Теперь на dec\_s2:  readlink /home/temp2/dec\_s2  Чем отличаются созданные ссылки от исходного файла?  Символические ссылки (также называемые “мягкими ссылками”) - это специальные типы файлов, которые содержат текстовое представлен ие пути к другому файлу или каталогу. В отличие от жестких ссылок, символические ссылки не указывают непосредственно на inode файла, а указывают на путь к нему.  Note  Если простыми словами, символические ссылки - это ярлык. |

30. С правами пользователя user2 с помощью команды ср создайте в каталогах /home/temp1 и /home/temp2 по одной копии файла dec с другим именем (dec\_copyl). Чем отличаются исходный файл и его копия (обратите внимание на то, кто является владельцем исходного файла и его копии)? Чем отличаются права доступа на эти файлы?

|  |
| --- |
| Important  Откройте терминал через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6. Если вы авторизированы за другого пользователя, то вбейте в терминале команду exit. После этого введите данные от user2, которые вы задали.  Теперь делаем копии файлов dec:  cp /home/user1/qu4/dec /home/temp1/dec\_copy1  cp /home/user1/qu4/dec /home/temp2/dec\_copy2  Теперь проверяем оригинальный файл:  ls -l /home/student9/qu4/dec  А теперь проверяем копию файла:  ls -l /home/temp1/dec\_copy1  Если вы сделали всё правильно, то владельцы файлов будут различаться. Можно сделать вывод, что если доступ позволяет создавать копию файла, то копия, которая была создана новым другим пользователем, будет принадлежать ему. В данном случае владелец оригинала user1, а копии user2.  Note  Вместо user1 у вас может быть абсолютно другой, которого вы задали. |

31.Вернитесь в консоль userl. С помощью команды rm удалите файл dec. Что произошло с "жесткими" и символическими ссылками на данный файл? Что произошло с его копиями? Что нужно сделать для того, чтобы файл перестал существовать (на логическом уровне)?

|  |
| --- |
| Important  Открываем консоль через сочетание (CTRL + ALT + F<number>), где number - это число от 1 до 6. Если вы находились в сессии за другого пользователя, то введите exit для выхода. После этого вводите данные от > user1.  Удаляем исходный файл в /home/user1/qu4/dec, используя команду ниже:  rm /home/student9/qu4/dec  Теперь ответим на вопросы  Что стало с жёсткими ссылками? Ничего, они также ссылаются на файл. Проверяем, используя команду ниже:  cat /home/temp1/dec\_h1  Note  Если было всё сделанно правильно, то вам выведет содержимое файла.  Что стало с мягкими ссылками? Они стали битыми, так как они пытаються сослаться на файл, которого нет. Проверим, используя команду ниже:  cat /home/temp1/dec\_s1  Note  Если было всё сделанно правильно, то вам сообщат, что такого файла нет.  Что стало с копиями? Ничего, это новые файлы, созданные другими.  Что нужно сделать, чтобы удалить файл на логическом уровне? Если удалить ВСЕ жёсткие ссылки, то тода файл удалится на логическом уровне. |

32. С правами userl удалите файлы из каталогов /home/temp1 и /home/temp2. Какие файлы не удалось удалить? Почему? Попробуйте удалить 83 оставшиеся файлы правами пользователя user2. Объясните результат.

|  |
| --- |
| Important  Откройте терминал, используя комбинаацию (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Теперь пробуем удалить /home/temp1, для этого используйте команду, которая представлена ниже:  rm /home/temp1  Теперь пробуем удалить файл /home/temp2, для этого используйте команду, которая представлена ниже:  rm /home/temp2  Important  Вы не сможете удалить файлы user2, находясь за user1. |

33. Попробуйте удалить любой из каталогов qul, qu2, qu3, qu4 с помощью команды rmdir (не удаляя предварительно из них файлов). Объясните результат.

|  |
| --- |
| Important  Откройте терминал, используя комбинацию (CTRL + ALT + F>number>), где number - это число от 1 до 6. Советую здесь войти за user2. Для выхода из прошлой сессии используйте команду exit.  Теперь попробуем удалить qu1, для этого используйте команду, которая представлена ниже:  rmdir /home/user1/qu1  Note  Команда не будет выполнена, потому что в данном каталоге находяться файлы.  Теперь попробуем удалить qu2, для этого используйте команду, которая представлена ниже:  rmdir /home/user1/qu2  Теперь попробуем удалить qu3, для этого используйте команду, которая представлена ниже:  rmdir /home/user1/qu3  Теперь попробуем удалить qu4, для этого используйте команду, которая представлена ниже:  rmdir /home/user1/qu4  Note  Вместо user1 у вас может быть абсолютно другой пользователь. |

34. Войдите в консоль администратора и с правами root, пользуясь командой chattr, заблокируйте файл feb от любых изменений. Установите параметр запрета любых операций, кроме добавления данных для файла mar. Вернитесь в консоль userl. С помощью команды lsattr -1 проверьте наличие дополнительных атрибутов у файлов.

|  |
| --- |
| Important  Откройте консоль, используя комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6. Если вы до этого были в пользовательской сессии, то вам следует использовать команду exit. Вы можете войти в главную учетную запись, которую создали в начале, а потом перейти в root, используя команду sudo su.  После того, как удачно зашли за root, меняем атрибуты файлов mar и feb:  Сначала заблокируем файл feb от любых изменений:  chattr +i /home/user1/qu1/feb  Теперь запретим все операции, исключая добавления, в файл mar:  chattr +a /home/user1/qu1/mar  Что вообще делает данные команда?  Проверяем атрибуты, используя команду ниже:  lsattr /home/user1/qu1/feb  Note  У меня выглядит вот так: ----i--------e-- /home/user1/qu1/feb  lsattr /home/user1/qu1/mar  Note  У меня выглядит вот так: -----a-------e-- /home/user1/qu1/mar |

35. С правами пользователя userl добавьте одну строку finish в конец файлов feb и mar (воспользуйтесь для этого командой echo fi nish >> fi le\_name). Убедитесь в успешном завершении операции, объясните результат.

|  |
| --- |
| Important  Откройте терминал, используя комбинацию клавиш (CTRL + ALT + F<number>), где number - это данные от 1 до 6. Теперь попробуйте войти за пользователя user1. Если вы находитесь в другой сессии, то вам нужно > выйти, используя команду exit.  Теперь добавляем finish в файл feb:  echo "finish" >> /home/user1/qu1/feb  Note  Файл feb: поскольку для файла feb установлен атрибут i (immutable), который запрещает любые изменения, команда echo "finish" >> /home/user1/qu1/feb завершится с ошибкой “Permission denied” (Отказано в доступе). Никто, даже владелец файла, не может изменить его, пока установлен атрибут i.  Теперь добавляем finish в файл mar:  echo "finish" >> /home/user1/qu1/mar  Note  Для файла mar установлен атрибут a (append only), который разрешает только добавление данных в конец файла. Команда echo "finish" >> /home/user1/qu1/mar должна выполниться успешно. Строка “finish” будет добавлена в конец файла mar. |

36. C правами пользователя userl с помощью команды rm -rf последовательно удалите ранее созданные каталоги qu2, qu3, qu4 вместе с файлами. Объясните результат.

|  |
| --- |
| Important  Откройте терминал с помощью комбинации клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6. Если вы сейчас находитесь уже в сессии за другого пользователя, то нужно выйти из текущей с помощью команды exit. После этого вы можете войти за user1.  Теперь удаляем qu2:  rm -rf qu2  Теперь удаляем qu3:  rm -rf qu3  Теперь удаляем qu4:  rm -rf qu4  Note  В результате у вас должно отказать в доступе при попытке удалить qu2 и qu3 А вот qu4 вы сможете удалить. |

37. С помощью команды md5sum вычислите и запишите контрольную сумму для одного из файлов в каталоге /home/user1/qul. Добавьте один символ в этот файл с помощью команды echo (например, echo a >> /home/userl/qul/jan). Вновь вычислите контрольную сумму файла и сравните два результата.

|  |
| --- |
| Important  Откройте терминал через приложение Konsole.  Выполняем действия, сказанные в методичке:  md5sum /home/user1/qu1/jan > jan.md5  Проверяем, ЧТО файл не пустой, используя команду ниже:  cat jan.md5  Добавляем символ, используя команду ниже:  echo a >> /home/user1/qu1/jan  Теперь проверяем контрольную сумму.  Сначала выполните команду ниже:  md5sum /home/user1/qu1/jan > jan\_modified.md5  Теперь просмотрим файл. Используйте команду ниже:  cat jan\_modified.md5  Note  Если вы сделали все правильно, то контрольные суммы должны отличаться. |

38. С помощью команды find с правами администратора найдите в корневом каталоге файлы:

- имеющие атрибуты SUID (fi nd / -type f -perm -4000);

- файлы, которые разрешено модифицировать всем (find / -type f - perm - 2);

- файлы, не имеющие владельца (find / -nouser);

- объясните, какой интерес могут представлять для администратора указанные категории файлов?

|  |
| --- |
| Important  Заходим за админа через терминал, который открывается комбинацией (CTRL + ALT + F<number>), где number - это число от 1 до 6. Если вы до этого были в другой сессии, то попробуйте перейти в root, используя команду sudo su.  Теперь произведем поиск файлов с атрибутом SUID. Для этого используйте команду, которая представлена ниже:  find / -type f -perm -4000  Для поиска файлов, разрешенных для модификации всем, используйте команду, которая представлена ниже:  find / -type f -perm -222  Теперь произведем поиск файлов без владельца. Для этого используйте команду, которая представлена ниже:  find / -nouser  Объяснение интереса для администратора  Файлы с атрибутом SUID:  Риск безопасности: Файлы с SUID выполняются с правами владельца файла, а не пользователя, запустившего файл. Это может быть очень опасно, если владелец файла — root. Любой пользователь, запустивший SUID-программу, принадлежащую root, получает временные права root, что может быть использовано для выполнения несанкционированных действий. Администратор должен регулярно проверять список SUID-файлов, чтобы убедиться, что все они необходимы и настроены правильно. Неправильно сконфигурированный SUID-файл может быть использован злоумышленником для повышения своих привилегий в системе.  Пример: Часто встречающиеся SUID-файлы включают passwd, su и sudo. Они необходимы для работы системы, но требуют особого внимания.  Файлы, разрешенные для модификации всем:  Риск повреждения данных: Если файл доступен для записи всем пользователям, любой пользователь (или даже вредоносная программа) может изменить его содержимое. Это может привести к по вреждению данных, нарушению работы системы или даже к компрометации безопасности.  Неправильная конфигурация: Обычно нет необходимости предоставлять права на запись для всех пользователей. Такие права доступа часто являются результатом ошибки конфигурации.  Пример: Файлы конфигурации, скрипты и другие важные файлы не должны быть доступны для записи всем пользователям.  Файлы без владельца:  Проблемы с управлением: Если файл не имеет владельца, его сложно правильно администрировать. Непонятно, кто отвечает за этот файл, и кто должен устанавливать права доступа.  Риск безопасности: Файлы без владельца могут представлять риск безопасности, так как их сложно контролировать и защищать.  Причины появления: Файлы без владельца могут появиться в результате удаления пользователя, которому принадлежал файл, без предварительного изменения владельца файлов этого пользователя.  Пример: Файлы во временных каталогах (например, /tmp) могут остаться без владельца, если процесс, создавший файл, завершился некорректно.  Действия администратора:  Обнаружив такие файлы, администратор должен предпринять следующие действия:  SUID-файлы: Проверить необходимость SUID-атрибута. Если он не нужен, его следует убрать. Если он необходим, убедиться, что программа безопасна и не имеет уязвимостей. Файлы, доступные для записи всем: Изменить права доступа, чтобы ограничить возможность записи только для владельца и, возможно, группы.  Файлы без владельца: Назначить владельца файлу (обычно пользователю, который будет отвечать за его обслуживание) или удалить файл, если он больше не нужен. |

39. Зарегистрируйтесь в системе в консольном режиме с правами root.Используя команду cat с правами root, просмотрите содержимое файлов/etc/passwd и /etc/shadow.

Задание.Вам необходимо создать учетные записи и определить правадоступа для десяти (10) сотрудников: w\_gromov, n\_kalinina, e\_ivanova,r\_klinova, b\_rebrov, k\_beglov, i\_frolov, d\_lavrov, m\_kruglov, t\_uporov,работающих в одном подразделении и занятых созданием и редактированиемтекстовых документов различного уровня конфиденциальности.

Разграничение доступа к информации должно быть произведено наосновании следующих требований:

- допуск к секретным сведениям имеют четыре пользователя: w\_gromov,n\_kalinina, b\_rebrov, k\_beglov;

- три пользователя: n\_kalinina, b\_rebrov, k\_beglov работают надсозданием секретных документов, каждый по своему профилю. Их домашниекаталоги и файлы должны быть полностью недоступными как друг для друга,так и для всех остальных, исключая w\_gromov;

- три пользователя: i\_frolov, d\_lavrov, e\_ivanova имеют допуск к конфиденциальной информациии работают над документами с соответствующим грифом.Они имеют право читать файлы с конфиденциальной информацией, созданные своими коллегами, без права ихмодификации;

- все секретоносители имеют право знакомиться с конфиденциальными файлами

- три пользователя: r\_klinova, m\_kruglov, t\_uporov могут работать толькос открытой информацией. Их файлы должны быть доступны для чтениякаждому сотруднику подразделения (без права модификации);

- w\_gromov является редактором подразделения и имеет право читать имодифицироватьфайлывсехсотрудниковивсехуровнейконфиденциальности. Завершенные документы копируются пользователемw\_gromov в его домашний каталог, который должен быть недоступен для всехостальных сотрудников подразделения.

Укажите в отчете,какие коллизии вы усматриваете в сформулированных требованиях? Как реализовать указанные требования таким образом, чтобы пользователи не могли по своему усмотрению изменять установленный порядок?

|  |
| --- |
| Important  Я пользовался терминалом, которое открывается через приложение Konsole.  Создадим учетную запись w\_gromov, используя команду ниже:  sudo useradd -u 510 -d /home/w\_gromov -m -p gromov510 w\_gromov  Что вообще делает данная команда?  Команда sudo useradd -u 510 -d /home/w\_gromov -m -p gromov510 w\_gromov выполняет следующие действия:  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как добавление нового пользователя.  useradd: Это команда для создания нового пользователя в системе.  -u 510: Указывает UID (идентификатор пользователя) нового пользователя. В данном случае UID будет 510.  -d /home/w\_gromov: Указывает домашний каталог для нового пользователя. В данном случае домашний каталог будет /home/w\_gromov.  -m: Создает домашний каталог, если он не существует. Это означает, что будет создан каталог /home/w\_gromov.  -p gromov510: Указывает пароль для нового пользователя в зашифрованном виде. Однако, если пароль не зашифрован, это может привести к проблемам с безопасностью. Обычно для установки пароля рекомендуется использовать команду passwd после создания пользователя.  w\_gromov: Это имя нового пользователя, который будет создан.  Таким образом, данная команда создает нового пользователя с именем w\_gromov, UID 510, домашним каталогом /home/w\_gromov, и устанавливает (или пытается установить) пароль gromov510.  Important  В дальнейших командах фигурирует дата, вам нужно будет поменять дату на момент сдачи. Для чего? Читайте в пояснении ниже.  Не пугайтесь WARNING при создании пользователя, все вполне нормально дальше будет работать.  Теперь создадим пользователя n\_kalinina, используя команду ниже:  sudo useradd -u 508 -d /home/n\_kalinina -m -p kalinina508 -e 2024-12-31 n\_kalinina  Что делает данная команда?  Теперь создадим пользователя e\_ivanova, используя команду ниже:  sudo useradd -u 505 -d /home/e\_ivanova -m -p parolparol -e 2024-09-31 e\_ivanova  Теперь создадим пользователя r\_klinova, используя команду ниже:  sudo useradd -u 509 -d /home/r\_klinova -m -p parolparol -e 2024-06-31 r\_klinova  Теперь создадим пользователя b\_rebrov, используя команду ниже:  sudo useradd -u 503 -d /home/b\_rebrov -m -p rebrov503 -e 2024-07-31 b\_rebrov  Теперь создадим пользователя k\_beglov, используя команду ниже:  sudo useradd -u 507 -d /home/k\_beglov -m -p beglov507 -e 2024-08-20 k\_beglov  Теперь создадим пользователя i\_frolov, используя команду ниже:  sudo useradd -u 501 -d /home/i\_frolov -m -p frolov501 -e 2024-12-10 i\_frolov  Теперь создадим пользователя d\_lavrov, используя команду ниже:  sudo useradd -u 504 -d /home/d\_lavrov -m -p lavrov504 -e 2024-12-31 d\_lavrov  Теперь создадим пользователя m\_kruglov, используя команду ниже:  sudo useradd -u 502 -d /home/m\_kruglov -m -p kruglov502 -e 2024-12-31 m\_kruglov  Теперь создадим пользователя t\_uporov, используя команду ниже:  sudo useradd -u 506 -d /home/t\_uporov -m -p uporov506 -e 2024-12-31 t\_uporov  Теперь создаём группы секретности для пользователей с допуском к секретным сведениям:  groupadd secret  Теперь создаём группы секретности для пользователей с допуском к конфиденциальным сведениям:  groupadd confidential  Теперь создаем группы секретности для пользователей, работающих только с открытой информацией:  groupadd open  Добавляем пользователей в группу secret:  usermod -aG secret w\_gromov  usermod -aG secret n\_kalinina  usermod -aG secret b\_rebrov  usermod -aG secret k\_beglov  Добавляем пользователей в группу confidential:  usermod -aG confidential i\_frolov  usermod -aG confidential d\_lavrov  usermod -aG confidential e\_ivanova  Добавляем пользователей в группу open:  usermod -aG open r\_klinova  usermod -aG open m\_kruglov  usermod -aG open t\_uporov  Настройка прав n\_kalinina, b\_rebrov, k\_beglov:  chmod 700 /home/n\_kalinina  chmod 700 /home/b\_rebrov  chmod 700 /home/k\_beglov  Теперь в задании, где есть данных 3 лица i\_frolov, d\_lavrov, e\_ivanova выполните команды, которые представлены ниже:  Создаем папку confidential:  mkdir /home/confidential  Ставим права у группы теперь:  chown root:confidential /home/confidential  Ставим права теперь на файл:  chmod 770 /home/confidential  Теперь в задании, где есть 3 лица r\_klinova, m\_kruglov, t\_uporov:  mkdir /home/open  chown root:open /home/open  chmod 755 /home/open  chmod g+s /home/open  Note  Его - w\_gromov - домашний каталог должен быть недоступен для всех остальных:  chmod 700 /home/w\_gromov  Настройка прав доступа к файлам:  Секретные файлы: файлы, создаваемые n\_kalinina, b\_rebrov и k\_beglov, должны быть доступны только им самим и w\_gromov. Права на файлы, создаваемые в их домашних каталогах, будут определяться umask. Чтобы обеспечить максимальную защиту, можно изменить umask для этих пользователей в их .bashrc файлах:  echo "umask 077" >> /home/n\_kalinina/.bashrc  echo "umask 077" >> /home/b\_rebrov/.bashrc  echo "umask 077" >> /home/k\_beglov/.bashrc  Конфиденциальные файлы: Пользователи i\_frolov, d\_lavrov и e\_ivanova должны создавать свои файлы в /home/confidential.  [!IMPORTNAT] Пользователь - владелец файла будет задавать права доступа.  Открытые файлы: Пользователи r\_klinova, m\_kruglov и t\_uporov должны создавать свои файлы в /home/open. Пользователь владелец файла будет задавать права доступа.  Настройка прав доступа для w\_gromov: w\_gromov должен иметь возможность читать и модифицировать файлы всех сотрудников и всех уровней конфиденциальности. Самый простой способ реализовать это - добавить пользователя w\_gromov в группу sudo. |

40. С помощью команды groupadd создайте четыре пользовательских группы: alfa, beta, nabla, sigma. Формат команды groupadd -g GID group\_name. Идентификатор группы GID можно назначать произвольно, начиная с номера 100 (например, groupadd -g 101 alfa).

|  |
| --- |
| Создаем группу alfa, используя команду ниже:  sudo groupadd -g 101 alfa  Создаем группу beta, используя команду ниже:  sudo groupadd -g 102 beta  Создаем группу nabla, используя команду ниже:  sudo groupadd -g 103 nabla  Создаем группу sigma, используя команду ниже:  sudo groupadd -g 104 sigma  Что делает данная команда?  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как добавление новой группы.  groupadd: Это команда для создания новой группы в системе.  -g 104: Указывает GID (идентификатор группы) для новой группы. В данном случае GID будет 104. Это число должно быть уникальным в системе.  sigma: Это имя новой группы, которая будет создана. |

41. Создайте учетные записи для вышеуказанных десяти новыхпользователей.Регистрационные данные (кроме паролей и групп) сведены в таблицу 1.Пароли назначайте произвольно, длиной не менее 8 символов, не забываяфиксировать их в отчете. Для пользователей e\_ivanova, r\_klinova задайтеодинаковые пароли. Распределите сотрудников по группам таким образом,чтобы удовлетворить вышеперечисленным требованиям. Изобразите в отчетесхему, поясняющую разграничение доступа сотрудников подразделения ккомпьютерной информации.

|  |
| --- |
| Important  Я пользовался терминалом, которое открывается через приложение Konsole.  Создадим учетную запись w\_gromov, используя команду ниже:  sudo useradd -u 510 -d /home/w\_gromov -m -p gromov510 w\_gromov  Что вообще делает данная команда?  Команда sudo useradd -u 510 -d /home/w\_gromov -m -p gromov510 w\_gromov выполняет следующие действия:  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как добавление нового пользователя.  useradd: Это команда для создания нового пользователя в системе.  -u 510: Указывает UID (идентификатор пользователя) нового пользователя. В данном случае UID будет 510.  -d /home/w\_gromov: Указывает домашний каталог для нового пользователя. В данном случае домашний каталог будет /home/w\_gromov.  -m: Создает домашний каталог, если он не существует. Это означает, что будет создан каталог /home/w\_gromov.  -p gromov510: Указывает пароль для нового пользователя в зашифрованном виде. Однако, если пароль не зашифрован, это может привести к проблемам с безопасностью. Обычно для установки пароля рекомендуется использовать команду passwd после создания пользователя.  w\_gromov: Это имя нового пользователя, который будет создан.  Таким образом, данная команда создает нового пользователя с именем w\_gromov, UID 510, домашним каталогом /home/w\_gromov, и устанавливает (или пытается установить) пароль gromov510.  Important  В дальнейших командах фигурирует дата, вам нужно будет поменять дату на момент сдачи. Для чего? Читайте в пояснении ниже.  Не пугайтесь WARNING при создании пользователя, все вполне нормально дальше будет работать.  Теперь создадим пользователя n\_kalinina, используя команду ниже:  sudo useradd -u 508 -d /home/n\_kalinina -m -p kalinina508 -e 2024-12-31 n\_kalinina  Что делает данная команда?  Давайте разберем команду sudo useradd -u 508 -d /home/n\_kalinina -m -p kalinina508 -e 2024-12-31 n\_kalinina по частям:  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как добавление нового пользователя.  useradd: Это команда для создания нового пользователя в системе.  -u 508: Указывает UID (идентификатор пользователя) нового пользователя. В данном случае UID будет 508.  -d /home/n\_kalinina: Указывает домашний каталог для нового пользователя. В данном случае домашний каталог будет /home/n\_kalinina.  -m: Создает домашний каталог, если он не существует. Это означает, что будет создан каталог /home/n\_kalinina.  -p kalinina508: Указывает пароль для нового пользователя в зашифрованном виде. Однако, как и в предыдущем примере, если пароль не зашифрован, это может привести к проблемам с безопасностью. Обычно для установки пароля рекомендуется использовать команду passwd после создания пользователя.  -e 2024-12-31: Указывает дату истечения срока действия учетной записи пользователя. В данном случае учетная запись пользователя n\_kalinina будет недоступна после 31 декабря 2024 года.  n\_kalinina: Это имя нового пользователя, который будет создан.  Таким образом, данная команда создает нового пользователя с именем n\_kalinina, UID 508, домашним каталогом /home/n\_kalinina, устанавливает (или пытается установить) пароль kalinina508, и задает дату истечения учетной записи на 31 декабря 2024 года.  Теперь создадим пользователя e\_ivanova, используя команду ниже:  sudo useradd -u 505 -d /home/e\_ivanova -m -p parolparol -e 2024-09-31 e\_ivanova  Теперь создадим пользователя r\_klinova, используя команду ниже:  sudo useradd -u 509 -d /home/r\_klinova -m -p parolparol -e 2024-06-31 r\_klinova  Теперь создадим пользователя b\_rebrov, используя команду ниже:  sudo useradd -u 503 -d /home/b\_rebrov -m -p rebrov503 -e 2024-07-31 b\_rebrov  Теперь создадим пользователя k\_beglov, используя команду ниже:  sudo useradd -u 507 -d /home/k\_beglov -m -p beglov507 -e 2024-08-20 k\_beglov  Теперь создадим пользователя i\_frolov, используя команду ниже:  sudo useradd -u 501 -d /home/i\_frolov -m -p frolov501 -e 2024-12-10 i\_frolov  Теперь создадим пользователя d\_lavrov, используя команду ниже:  sudo useradd -u 504 -d /home/d\_lavrov -m -p lavrov504 -e 2024-12-31 d\_lavrov  Теперь создадим пользователя m\_kruglov, используя команду ниже:  sudo useradd -u 502 -d /home/m\_kruglov -m -p kruglov502 -e 2024-12-31 m\_kruglov  Теперь создадим пользователя t\_uporov, используя команду ниже:  sudo useradd -u 506 -d /home/t\_uporov -m -p uporov506 -e 2024-12-31 t\_uporov |

42. Пять первых пользователей (w\_gromov, n\_kalinina, e\_ivanova,r\_klinova, b\_rebrov) зарегистрируйте с помощью команды useradd. Синтаксис команды:useradd - u UID - g group\_name - d dir\_home - m – p password -edate\_del\_user user\_name.Например, useradd -u 501 -g sigma -d/home/n\_kalinina -p v5g7K2S4 -e 2011- 01-07 n\_kalinina. Параметр -mобеспечивает создание домашнего каталога пользователя, если он ещене существует.Прочие параметры команды можно не указывать. Помните, имяпользователя не должно начинаться с цифры и содержать заглавных и русскихбукв, символов типа

\*#%л .... Идентификаторы пользователей UID назначаются, начиная с 500. Дата удаления учетной записи пользователя вводится в формате ГГГГ-ММ-ДД.

|  |
| --- |
| Important  Я пользовался терминалом, которое открывается через приложение Konsole.  Создадим учетную запись w\_gromov, используя команду ниже:  sudo useradd -u 510 -d /home/w\_gromov -m -p gromov510 w\_gromov  Что вообще делает данная команда?  Команда sudo useradd -u 510 -d /home/w\_gromov -m -p gromov510 w\_gromov выполняет следующие действия:  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как добавление нового пользователя.  useradd: Это команда для создания нового пользователя в системе.  -u 510: Указывает UID (идентификатор пользователя) нового пользователя. В данном случае UID будет 510.  -d /home/w\_gromov: Указывает домашний каталог для нового пользователя. В данном случае домашний каталог будет /home/w\_gromov.  -m: Создает домашний каталог, если он не существует. Это означает, что будет создан каталог /home/w\_gromov.  -p gromov510: Указывает пароль для нового пользователя в зашифрованном виде. Однако, если пароль не зашифрован, это может привести к проблемам с безопасностью. Обычно для установки пароля рекомендуется использовать команду passwd после создания пользователя.  w\_gromov: Это имя нового пользователя, который будет создан.  Таким образом, данная команда создает нового пользователя с именем w\_gromov, UID 510, домашним каталогом /home/w\_gromov, и устанавливает (или пытается установить) пароль gromov510.  Important  В дальнейших командах фигурирует дата, вам нужно будет поменять дату на момент сдачи. Для чего? Читайте в пояснении ниже.  Не пугайтесь WARNING при создании пользователя, все вполне нормально дальше будет работать.  Теперь создадим пользователя n\_kalinina, используя команду ниже:  sudo useradd -u 508 -d /home/n\_kalinina -m -p kalinina508 -e 2024-12-31 n\_kalinina  Что делает данная команда?  Давайте разберем команду sudo useradd -u 508 -d /home/n\_kalinina -m -p kalinina508 -e 2024-12-31 n\_kalinina по частям:  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как добавление нового пользователя.  useradd: Это команда для создания нового пользователя в системе.  -u 508: Указывает UID (идентификатор пользователя) нового пользователя. В данном случае UID будет 508.  -d /home/n\_kalinina: Указывает домашний каталог для нового пользователя. В данном случае домашний каталог будет /home/n\_kalinina.  -m: Создает домашний каталог, если он не существует. Это означает, что будет создан каталог /home/n\_kalinina.  -p kalinina508: Указывает пароль для нового пользователя в зашифрованном виде. Однако, как и в предыдущем примере, если пароль не зашифрован, это может привести к проблемам с безопасностью. Обычно для установки пароля рекомендуется использовать команду passwd после создания пользователя.  -e 2024-12-31: Указывает дату истечения срока действия учетной записи пользователя. В данном случае учетная запись пользователя n\_kalinina будет недоступна после 31 декабря 2024 года.  n\_kalinina: Это имя нового пользователя, который будет создан.  Таким образом, данная команда создает нового пользователя с именем n\_kalinina, UID 508, домашним каталогом /home/n\_kalinina, устанавливает (или пытается установить) пароль kalinina508, и задает дату истечения учетной записи на 31 декабря 2024 года.  Теперь создадим пользователя e\_ivanova, используя команду ниже:  sudo useradd -u 505 -d /home/e\_ivanova -m -p parolparol -e 2024-09-31 e\_ivanova  Теперь создадим пользователя r\_klinova, используя команду ниже:  sudo useradd -u 509 -d /home/r\_klinova -m -p parolparol -e 2024-06-31 r\_klinova  Теперь создадим пользователя b\_rebrov, используя команду ниже:  sudo useradd -u 503 -d /home/b\_rebrov -m -p rebrov503 -e 2024-07-31 b\_rebrov  Теперь создадим пользователя k\_beglov, используя команду ниже:  sudo useradd -u 507 -d /home/k\_beglov -m -p beglov507 -e 2024-08-20 k\_beglov  Теперь создадим пользователя i\_frolov, используя команду ниже:  sudo useradd -u 501 -d /home/i\_frolov -m -p frolov501 -e 2024-12-10 i\_frolov  Теперь создадим пользователя d\_lavrov, используя команду ниже:  sudo useradd -u 504 -d /home/d\_lavrov -m -p lavrov504 -e 2024-12-31 d\_lavrov  Теперь создадим пользователя m\_kruglov, используя команду ниже:  sudo useradd -u 502 -d /home/m\_kruglov -m -p kruglov502 -e 2024-12-31 m\_kruglov  Теперь создадим пользователя t\_uporov, используя команду ниже:  sudo useradd -u 506 -d /home/t\_uporov -m -p uporov506 -e 2024-12-31 t\_uporov |

43. Пять последних пользователей зарегистрируйте с помощью командного файла adduser, которая запрашивает значения в интерактивном режиме. При вводе данных ориентируйтесь на подсказки системы [в квадратных скобках]. Все параметры, кроме имени пользователя, его идентификатора, имени группы, пароля и домашнего каталога можно игнорировать. Для ввода параметра по умолчанию вводить Enter.

Переключаясь во вторую консоль, отслеживайте изменения, происходящие в файле /etc/passwd по мере ввода новых учетных записей.

|  |
| --- |
| Important  Откройте терминал, используя приложение: Konsole.  Попробуйте вводить команды, параллельно смотря во 2 вкладке на файл: /etc/passwd.  sudo adduser k\_beglov  sudo adduser i\_frolov  sudo adduser d\_lavrov  sudo adduser m\_kruglov  sudo adduser t\_uporov  Теперь для просмотра каждый раз используйте cat. |

44. Посмотрите с правами пользователя файл /etc/shadow. Повторите попытку просмотра с консоли суперпользователя. Почему поля, отведенные для хэшированных паролей у пользователей e\_ivanova и r\_klinova различаются?

|  |
| --- |
| Important  Откройте терминал через комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6. Если вы находитесь в другой сессии, то попробуйте выйти, используя команду exit. После этого сможете войти в другую сессию за другого пользователя.  Теперь попробуйте посмотреть файл /etc/shadow за обычного пользователя, используя команду ниже:  sudo less /etc/shadow  Теперь попробуйте перейти за root, используя команду ниже:  sudo su  Теперь попробуйте посмотреть файл /etc/shadow. Самая первая команда в файле.  Note  На счет почему разные хэши мне неизвестно. Скорее всего проблема в том, что хэш высчитывается из всех параметров, а не только из пароля. Опять-таки все возможно. |

45. Из первой консоли с помощью команды su измените права администратора на права пользователя w\_gromov. Почему система не запрашивает пароль? С помощью команды exit верните себе права администратора. Был ли запрошен пароль? (В различных дистрибутивах Linux возврат полномочий администратора организован различным образом).

|  |
| --- |
| Important  Откройте терминал, используя комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Вы по заданию изначально должны были быть в root. Если вы были из-под root, то просто введите команду, которая представлена ниже:  su w\_gromov  После этого вбейте команду:  exit  Note  У меня пароль не запросили после того, как exit. |

46. Запустите оболочку Midnight Commander в режиме редактирования(F4) файла паролей /etc/passwd и удалите в учетной записи пользователяn\_kalinina символ признака пароля (между первым и вторым двоеточием),включая пробел. Сохраните изменения в файле, завершите сеанс в MidnightCommander, с помощью Ctrl+Alt+F2(Alt+F2) откройте второй текстовый терминал и зарегистрируйтесьпользователем n\_kalinina, но теперь с «пустым» паролем. Сделайте выводотносительно опасности предоставления прав на запись в этот файл.Завершите сеанс для пользователя n\_kalinina с помощью команды exit.

|  |
| --- |
| Откройте терминал через приложение Konsole. Нам нужно открыть Midnight Commander, для этого используем команду в терминале, которая представлена ниже:  mc  В Midnight Commander перейдите к файлу /etc/passwd. Вам на несколько уровней нужно подняться, там будет etc директория. Файл passwd найдите по алфавитному возрастанию.  После того, как вы нашли файл и выбрали его, Нажмите F4 (Edit) для редактирования файла.  Найдите строку, соответствующую пользователю n\_kalinina. Она будет выглядеть примерно так, как представлено ниже:  n\_kalinina:x:1002:1002::/home/n\_kalinina:/bin/bash  Удалите символ x (или любой другой символ, представляющий пароль) между первым и вторым двоеточием, включая пробел, если он есть. Строка должна выглядеть так:  n\_kalinina::1002:1002::/home/n\_kalinina:/bin/bash  Удалите символ x (или любой другой символ, представляющий пароль) между первым и вторым двоеточием, включая пробел, если он есть. Строка должна выглядеть так:  n\_kalinina::1002:1002::/home/n\_kalinina:/bin/bash  Теперь перейдем к регистрации пользователя n\_kalinina в другом терминале:  Нажмите Ctrl+Alt+F2 (или Alt+F2 в некоторых системах) для переключения во второй текстовый терминал. В терминале введите имя пользователя n\_kalinina.  Нажмите Enter.  Important  Система не должна запросить пароль. Если вы правильно удалили символ пароля в /etc/passwd, вход должен быть выполнен без пароля. |

47. Пользователь d\_lavrov уволен за дисциплинарный проступок. С помощью команды userdel -r user\_name удалите его учетную запись вместе с домашним каталогом. В реальных условиях необходимо вначале скопировать в другую директорию файлы пользователя, представляющие ценность для организации.

|  |
| --- |
| Important  Откройте терминал через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Вам нужно перейти за root. Для этого войдите под пользователя, которого изначально создали при установке Астры. Теперь используйте команду:  sudo su  Теперь мы можем удалить учетную запись:  sudo userdel -r d\_lavrov  Что вообще делает данная команда?  Команда sudo userdel -r d\_lavrov выполняет следующие действия:  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как удаление пользователя.  userdel: Это команда для удаления пользователя из системы.  -r: Этот параметр указывает, что необходимо удалить не только учетную запись пользователя, но и его домашний каталог и все файлы, принадлежащие этому пользователю. Это означает, что все данные, хранящиеся в домашнем каталоге пользователя, будут также удалены.  d\_lavrov: Это имя пользователя, который будет удален из системы.  Таким образом, команда sudo userdel -r d\_lavrov удаляет пользователя с именем d\_lavrov и все его файлы, включая домашний каталог, из системы. Будьте осторожны при использовании этой команды, так как восстановить удаленные данные будет невозможно без резервной копии. |

48. Зарегистрируйте вместо уволенного пользователя нового сотрудника f\_mironov с предоставлением ему аналогичных прав (пароль должен быть новым!).

|  |
| --- |
| Important  Откройте терминал через комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Вам нужно перейти за root, для этого используйте команду:  sudo su  Регистрация нового сотрудника f\_mironov:  sudo useradd -m f\_mironov  Теперь ставим пароль на пользователя:  sudo passwd f\_mironov |

49. Пользователь r\_klinova убыла в командировку сроком на две недели. Заблокируйте ее учетную запись, для чего с правами администратора войдите в режим редактирования файла паролей и вставьте во второе поле (между первым и вторым двоеточием) любой символ, который не разрешено использовать для пароля. Попытайтесь зарегистрироваться во второй консоли с правами r\_klinova и убедитесь в том, что для этого пользователя система не доступна.

|  |
| --- |
| Important  Откройте терминал через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Теперь можете перейти в root, используя команду, которая представлена ниже:  sudo su  Теперь есть 2 варианта по блокировке:  Для перманентного бана используйте команду, которая представлена ниже:  sudo usermod -L r\_klinova  Если хотите заблокировать временно, то вам нужно править файл /etc/shadow. Вам нужно для учетной записи r\_klinova можно вставить символ \* в начало строки пароля в файле /etc/shadow. |

50. Зарегистрируйтесь во второй консоли с правами пользователя k\_beglov, вызовите команду passwd и измените свой пароль. В качестве нового пароля введите qwerty.

|  |
| --- |
| Important  Откройте терминал, используя комбинацию клавиш (CTRL + ALT + F<number>), где number от 1 до 6. Если вы были в текущей сессии, то вам нужно выйти, используя команду exit.  Зайдите в консоль с правами пользователя k\_beglov и выполните passwd. После этого он предложит вам ввести новый пароль. |

51. Перейдите в консоль администратора и назначьте пользователю k\_beglov новый пароль zxcvbnm. Затем с помощью команды chage (change aging – изменить информацию об устаревании) установите для этого пользователя минимальное время действия паролей, равное 5 дням. С какой целью устанавливается минимальный срок действия пароля?

|  |
| --- |
| mportant  Откройте терминал, используя сочетание клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6. Если вы были не в сессии администратора, то вам нужно перейти, используя команду exit. Теперь вам нужно перейти за администратора.  Теперь поставим новый пароль на k\_beglov, для этого используйте команду, которая представлена ниже:  sudo passwd k\_beglov  Теперь задайте новый пароль: zxcvbnm  Установка минмального срока пароля:  sudo chage -m 5 k\_beglov  Что делает данная команда?  Команда sudo chage -m 5 k\_beglov выполняет следующие действия:  sudo: Запускает команду с правами суперпользователя (root). Это необходимо для выполнения операций, требующих повышенных привилегий, таких как изменение параметров учетной записи пользователя.  chage: Это команда для изменения параметров управления сроком действия пароля пользователя.  -m 5: Этот параметр устанавливает минимальный срок действия пароля в 5 дней. Это означает, что пользователь k\_beglov не сможет изменить свой пароль на более новый, чем через 5 дней после последнего изменения пароля. Если пользователь попытается изменить пароль до истечения этого срока, система не позволит ему это сделать.  k\_beglov: Это имя пользователя, для которого устанавливается минимальный срок действия пароля.  Таким образом, команда sudo chage -m 5 k\_beglov устанавливает минимальный срок действия пароля для пользователя k\_beglov на 5 дней, что ограничивает его возможность менять пароль чаще, чем раз в 5 дней. |

52. Просмотрите электронную справку по файлу /etc/sudoers. Отредактируйте его таким образом, чтобы предоставить следующим пользователям дополнительные права за счет использования команды sudo

-пользователю e\_ivanova - право монтировать файловые системы,

-пользователю b\_rebrov - право изменения владельца файлов. Ответьте, чем отличается предоставление прав пользователям с помощью sudo от использования эффективных идентификаторов SUID?

|  |
| --- |
| Important  Для выполнения данного задания я пользовался терминалом, которое открывается через приложение Konsole.  Для редактирования файла /etc/sudoers и предоставления дополнительных прав пользователям, вам нужно использовать команду visudo, которая обеспечивает безопасное редактирование этого файла и проверяет его на наличие синтаксических ошибок перед сохранением.  Шаги для редактирования файла /etc/sudoers:  Откройте терминал и выполните команду:  sudo visudo  Добавьте следующие строки в конец файла, чтобы предоставить необходимые права:  e\_ivanova ALL=(ALL) NOPASSWD: /bin/mount, /bin/umount  b\_rebrov ALL=(ALL) NOPASSWD: /bin/chown  Note  Первая строка позволяет пользователю e\_ivanova монтировать и размонтировать файловые системы без запроса пароля. Вторая строка позволяет пользователю b\_rebrov изменять владельца файлов без запроса пароля.  Различия между предоставлением прав с помощью sudo и использованием эффективных идентификаторов SUID:  Безопасность:  sudo: Позволяет временно предоставлять права на выполнение определенных команд с правами другого пользователя (обычно root). Это позволяет контролировать, какие команды могут выполняться, и ведет журнал использования.  SUID: Устанавливает бит SUID на исполняемом файле, что позволяет пользователю запускать этот файл с правами владельца файла (обычно root). Это может быть менее безопасно, так как любой пользователь может запустить этот файл с повышенными привилегиями, что может привести к уязвимостям.  Контроль:  sudo: Предоставляет более тонкий контроль над тем, какие команды могут выполняться с повышенными привилегиями. Можно настроить права для отдельных пользователей или групп.  SUID: Менее гибкий, так как права предоставляются на уровне файла, и нет возможности ограничить, какие действия может выполнять пользователь с этими правами.  Журналирование:  sudo: Ведет журнал всех команд, выполненных с использованием sudo, что позволяет отслеживать действия пользователей.  SUID: Не предоставляет возможности журналирования, так как выполнение происходит напрямую через исполняемый файл.  Таким образом, использование sudo является более безопасным и контролируемым способом предоставления повышенных привилегий пользователям по сравнению с использованием SUID. |

53. Из второй консоли с правами пользователя f\_mironov создайте файл cal 2021 >/home/f\_mironov/cal2021. С помощью команды su переключите консоль на пользователя b\_rebrov и с помощью временно предоставленных ему привилегий передайте права на созданный f\_mironov файл другому владельцу n\_kalinina. Каким еще путем можно предоставить подобные права пользователям, не передавая им "опасных" полномочий администратора?

|  |
| --- |
| Important  Откройте консоль через комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6. Теперь вам нужно войти под пользователем f\_mironov. Если вы были до этого в другой сессии, то введите exit.  Так как у меня не получилось скачать cal, у меня будет чуточку другая команда для добавления в файл.  echo "cal 2021" > /home/f\_mironov/cal2021  Теперь сделаем переключение на пользователя b\_rebrov. Простая команда su b\_rebrov нам не поможет, здесь вам нужно выйти, используя exit, а потом ввести данные от b\_rebrov.  После того, как вошли за пользователя, выполните команду, которая представлена ниже:  sudo -u b\_rebrov chown n\_kalinina /home/f\_mironov/cal2021  Для предоставления прав без полномочий администратора можно использовать настройку sudoers для конкретных команд |

54. Просмотрите с правами администратора системные журналы в каталоге /var/log и убедитесь, что система зафиксировала факты присвоения полномочий администратора.

|  |
| --- |
| Important  Для выполнения данного задания я пользовался терминалом, которое открывается через приложение Konsole.  Теперь выполните команду, которая представлена ниже:  sudo less /var/log/auth.log |

55. Отключитесь от всех терминалов и переключитесь на 1-ый терминал:<CTRL-ALT-F1>. Войдите в систему как обычный пользователь (не root).Получите информацию о данном логине, представьте преподавателю.Получите информацию обо всех параллельных логинах на локальнойрабочейстанции(должентолькобытьодинпользователь,зарегистрированный в системе).Переключитесь в виртуальный терминал 2: <CTRL-ALT-F2>Войдите с данного терминала как пользователь studentПолучите информацию о данном логине, прдставьтепреподавателю.Получите информацию обо всех параллельных логинах на локальной рабочейстанции.Находясь в системе, под пользователем student посмотрите маску.Создайте пару файлов и директорий, не изменяя прав доступа к ним.Измените вашу маску на более безопасную, а затем создайте новый файли новуюДиректорию. Как изменились права доступа у новых файлов?

|  |
| --- |
| Для выполнения данного задания я пользовался терминалом, который открывается через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Нажимаем CTRL + ALT + F1. Теперь Войдите под любую сессию, исключая root. Я, например, зайду под своего основного пользователя c3equalz. Теперь, чтобы получить информацию о логине, используйте команду, которая представлена ниже:  whoami  Чтобы просмотреть информацию о всех пользователях, можно использовать команду, которая представлена ниже:  w  Note  Команда показывает список всех пользователей, которые в данный момент вошли в систему, а также информацию о том, когда и откуда они вошли.  Теперь войдите под другого пользователя, повторив все телодвижения, представленные выше. Только теперь вам остается посмотреть на маску. Для этого используйте команду, которая представлена ниже:  umask  Теперь попробуем создать файл и директорию. Для этого используйте команду, которая представлена ниже:  touch file1  mkdir dir1  Теперь попробуем поменять маску. Пример команды представляю ниже:  umask 077  После того, как поменяли права, используйте команды для создания файлов и директорий.  touch file2  mkdir dir2  В данном случае, после изменения маски на 077, новые файлы и каталоги будут создаваться с более строгими правами доступа, что повышает безопасность, ограничивая доступ к ним для других пользователей. |

56. Для выполнения этого задания, Вы должны находится в системе под пользователем root. Создайте общую директорию для всех пользователей /var/ftp/pub. Все пользователи должны иметь возможность записи в директорию, но удалять файлы из директории пользователь может только в том случае, если файл принадлежит ему.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал с приложения Konsole.  Чтобы перейти в root, используйте команду, которую я представил ниже:  sudo su  Теперь создадим общую директорию, используя команду, которая представлена ниже:  mkdir -p /var/ftp/pub  Теперь изменим права доступа к директории, чтобы все пользователи могли в ней записывать:  chmod 777 /var/ftp/pub  Теперь установим sticky bit. Это делается с той целью, чтобы пользователь, который создал файл, мог удалять файл и никто другой.  chmod +t /var/ftp/pub |

57. Создайте новый файл file2 в вашей рабочей директории. Посмотрите ACL для файла file2. Совпадают ли права доступа с установленной маской? Измените права доступа на чтение, запись и выполнение для группы файла file2. Посмотрите права на file2 с помощью команды ls –l а также посмотрите ACL для этого файла.

|  |
| --- |
| Important  Для данного задания я пользовался терминалом, который открывается через приложение Konsole.  Создадим file2, для этого используйте данную команду:  touch ~/file2  Теперь исползуйте данную команду для просмотра списка acl:  getfacl ~/file2  Теперь измените права доступа на чтение, запись и выполнение для группы:  chmod g+rwx ~/file2  Теперь сделаем просмотр прав, используя команды ниже:  ls -l ~/file2  getfacl ~/file2 |

58. Установите маску для файла file2 - только чтение. Посмотрите права на file2 с помощью команды ls –l а также посмотрите ACL для этого файла.

|  |
| --- |
| Important  Для данного задания я пользовался терминалом, которое открывается через приложение Konsole.  Для установки прав только на чтение для файла file2 с использованием ACL, используйте команду, которая представлена ниже:  setfacl -m m::r ~/file2  Для просмотра прав используйте команды, которая представлена ниже:  ls -l ~/file2  getfacl ~/file2 |

59. Если группа group1 не существует в вашей системе, создайте эту группу с ID равным 101. Добавьте в ACL группу group1 для файла file2. Установите только права на чтение и выполнение для данной группы.

|  |
| --- |
| Important  Для выполнения данного задания я пользовался терминалом, которое открывается через приложение Konsole.  Добавление группы group1 и настройка ACL:  groupadd -g 101 group1  Добавьте в ACL группу group1 для файла file2 с правами на чтение и выполнение, используя команду ниже:  setfacl -m g:group1:rx ~/file2 |

60. Добавьте в ACL пользователя user10 для файла file2. Добавьте для этого пользователя доступ по исполнению файла.

|  |
| --- |
| Important  Для данного задания я пользовался терминалом, которое открывается через приложение Konsole.  Перейдите в root, используя команду, которая представлена ниже:  sudo su  Добавим пользователя user10 в ACL. Для этого используйте команду, которая представлена ниже:  useradd user10  Добавим в ACL пользователя user10 для файла file2 с правом на исполнение. Для этого используйте команду, которая представлена ниже:  setfacl -m u:user10:x ~/file2 |

Лабораторная работа №5

Файловая система ОС Astra Linux Special Edition. LVM. Swap

Цель работы - Научится работать с символическими и жесткими

ссылками, добавлять новые диски в систему и обслуживать их (разбивать

диски на разделы, создавать нужную файловую систему (ФС), изменять

параметры файловой системы). Научится создавать и обслуживать разделы

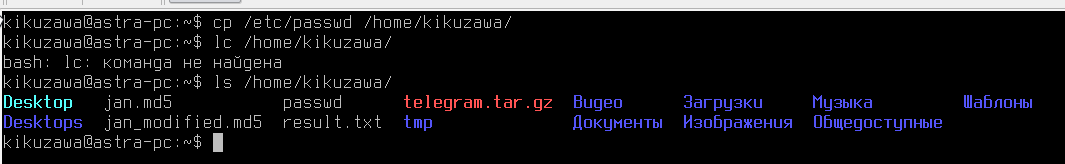
LVM. Настройка swap.

Ход работы:

Задание 1. Символические и жесткие ссылки

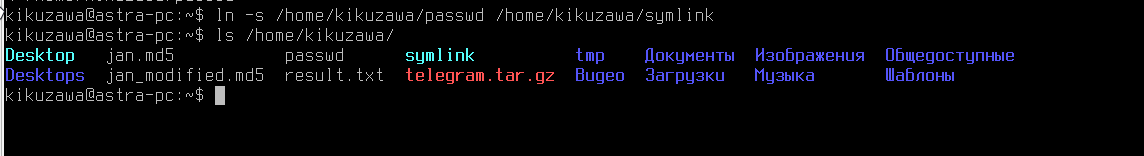
1. Скопируйте файл passwd из каталога /etc в домашнюю директорию пользователя student

|  |
| --- |
| Для выполнения задания используйте команду ниже:  cp /etc/passwd /home/student/ |



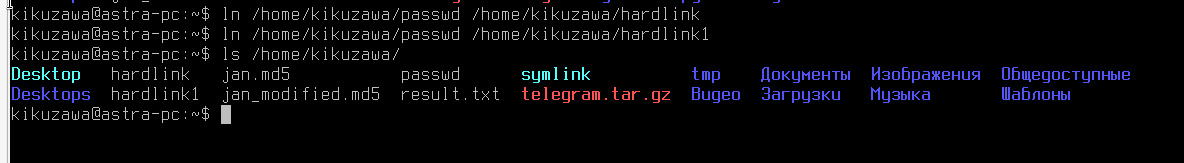
2.Создайте символическую ссылку symlink на скопированный файл passwd

|  |
| --- |
| Для решения данной задачи используйте команду, которая представлена ниже:  ln -s /home/student/passwd /home/student/symlink  Important  Вместо student укажите имя вашего пользователя.  Вот что делает команда:   * ln — это команда для создания ссылок. * -s — это опция, которая указывает, что вы хотите создать символическую ссылку. * /home/student/passwd — это путь к исходному файлу, на который вы создаете ссылку. * /home/student/symlink — это путь, по которому будет создана символическая ссылка.   Если забыли что такое символичные ссылки.  Символическая ссылка - symlink — это специальный тип файла в файловой системе, который указывает на другой файл или директорию. Она действует как указатель, позволяя вам обращаться к целевому файлу или директории, используя альтернативное имя или путь. Вот несколько ключевых моментов о символических ссылках:   * Указатель на файл: Символическая ссылка содержит путь к целевому файлу или директории. Когда вы обращаетесь к символической ссылке, операционная система перенаправляет вас к оригинальному файлу. * Отличие от жесткой ссылки: В отличие от жесткой ссылки, которая ссылается на тот же inode (физическое представление файла на диске), символическая ссылка может указывать на файл или директорию, находящиеся в другом месте файловой системы. Если оригинальный файл удален, символическая ссылка становится "висячей" (broken link) и не будет работать. * Удобство: Символические ссылки полезны для создания удобных путей к файлам, упрощения доступа к часто используемым ресурсам или организации структуры каталогов. |



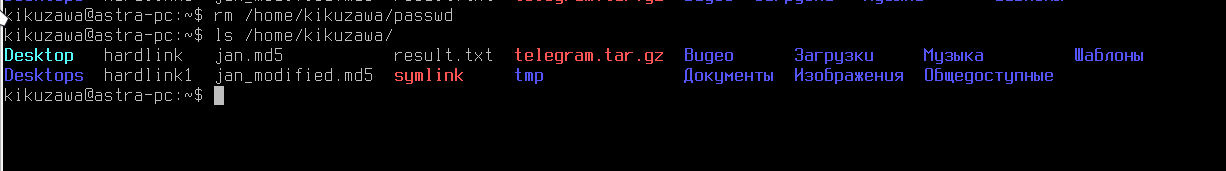
3.Создайте две жестких ссылки hardlink и hardlink1 на скопированный файл passwd. Проверьте что ссылки работают.

|  |
| --- |
| Для решения, поставленной задачи, используйте команды, которые представлены ниже:  ln /home/student/passwd /home/student/hardlink  ln /home/student/passwd /home/student/hardlink1  Note  Вместо student может быть имя любого пользователя.  Можно проверить существование жесткой ссылки, используя команды ниже:  cat /home/student/hardlink  cat /home/student/hardlink1  Если забыли что такое жесткие ссылки.  Жесткая ссылка — это другой тип ссылки на файл в файловой системе, который указывает на тот же inode, что и оригинальный файл. Это означает, что жесткая ссылка и оригинальный файл фактически являются разными именами для одного и того же файла на диске. Вот несколько ключевых моментов о жестких ссылках:   * Общий inode: Жесткая ссылка ссылается на тот же inode, что и оригинальный файл. Это означает, что изменения, внесенные в файл через одну ссылку, будут видны через другую ссылку, поскольку они указывают на одно и то же физическое представление данных. * Отличие от жесткой ссылки: В отличие от жесткой ссылки, которая ссылается на тот же inode (физическое представление файла на диске), символическая ссылка может указывать на файл или директорию, находящиеся в другом месте файловой системы. Если оригинальный файл удален, символическая ссылка становится "висячей" (broken link) и не будет работать. * Удобство: Символические ссылки полезны для создания удобных путей к файлам, упрощения доступа к часто используемым ресурсам или организации структуры каталогов. |



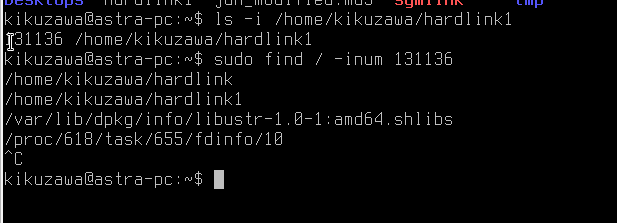
4.Удалите оригинал /home/student/passwd. Что изменилось, опишите.

|  |
| --- |
| rm /home/student/passwd  После удаления оригинального файла passwd все ссылки (как символическая, так и жесткие) продолжают работать, поскольку они ссылались на inode, который оставался в системе. Однако сам файл был удален, так что любые операции, которые требуют его содержимого, будут проваливаться. |



5.Посмотрите номер inode оставшихся жестких ссылок. Как найти все жесткие ссылки, если они находятся в разных директориях, и вы не знаете в каких. Покажите это на примере ваших жестких ссылок.

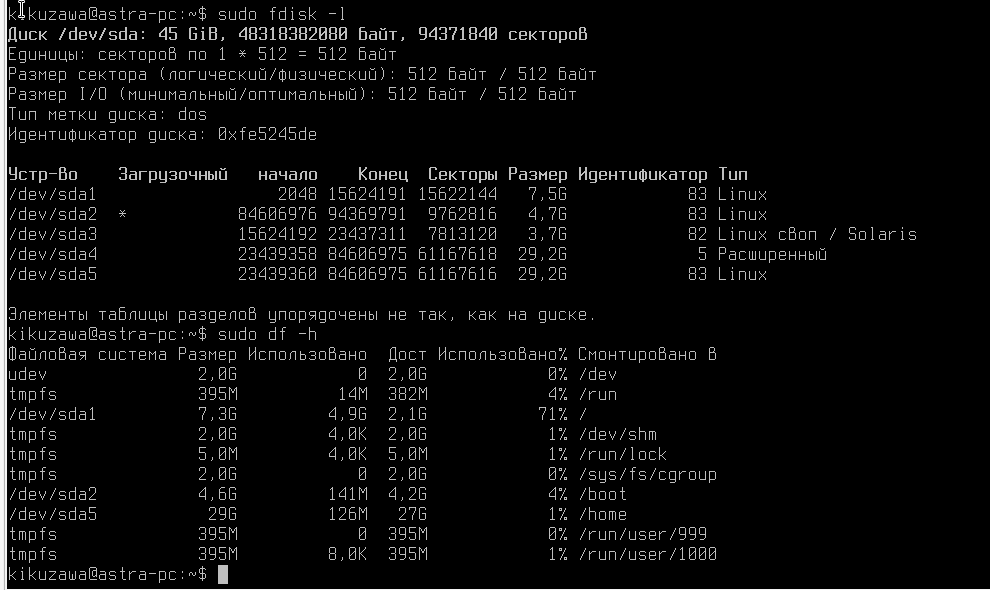
|  |
| --- |
| Для просмотра номера inode оставшихся жестких ссылок, можете воспользоваться командой, которая представлена ниже:  ls -i ~/hardlink1  Теперь по выведенному номеру от прошлой команды произведем поиск:  sudo find / -inum <number>  Note  number - это номер, который вам вывела 1 команда. |



Задание 2. Работа с жесткими дисками

1. Используйте fdisk -l, чтобы посмотреть информации о дисках и разделах на вашем компьютере. Какие из ваших дисков в системе имеют разметку? Описать. Посмотрите свободное место на этих разделах с помощью команды df

|  |
| --- |
| Команда fdisk -l используется для отображения информации о дисках и разделах на вашем компьютере. Она показывает список всех доступных дисков и их разделов, а также информацию о размере, типе и состоянии каждого раздела.  Для просмотра всех в терминале вбейте команду, которая представлена ниже:  sudo fdisk -l  Note  Команда может потребовать прав суперпользователя, поэтому добавьте sudo в начале.  Давайте рассмотрим что выводит данная команда. Тут есть некоторые параметры, которые могут быть неочевидны:   * Disk: Имя устройства и его размер. * Device: Имя раздела (например, /dev/sda1). * Boot: Указывает, является ли раздел загрузочным (обычно помечен звездочкой \*). * Start/End: Начальный и конечный сектора раздела. * Sectors: Общее количество секторов в разделе. * Size: Размер раздела. * Id: Идентификатор типа файловой системы. * Type: Тип раздела (например, Linux, NTFS и т.д.).   Теперь перейдем для проверки свободного места на всех диска. Для этого воспользуйтесь командой ниже:  sudo df -h  Note  Опция -h выводит информацию в удобочитаемом формате (например, в гигабайтах и мегабайтах). |

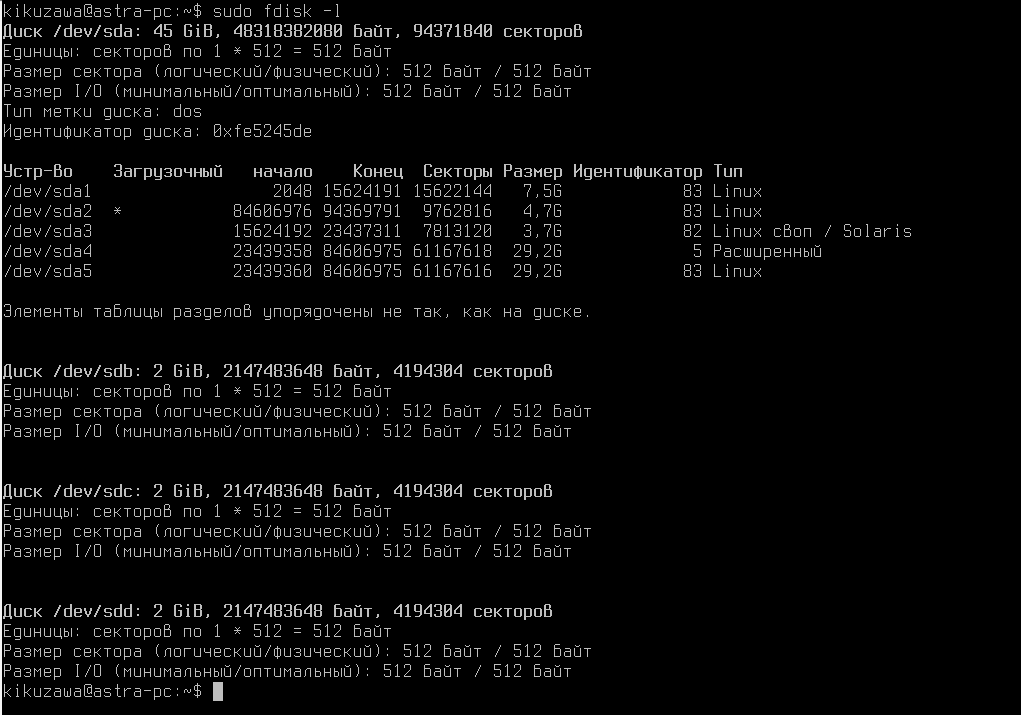


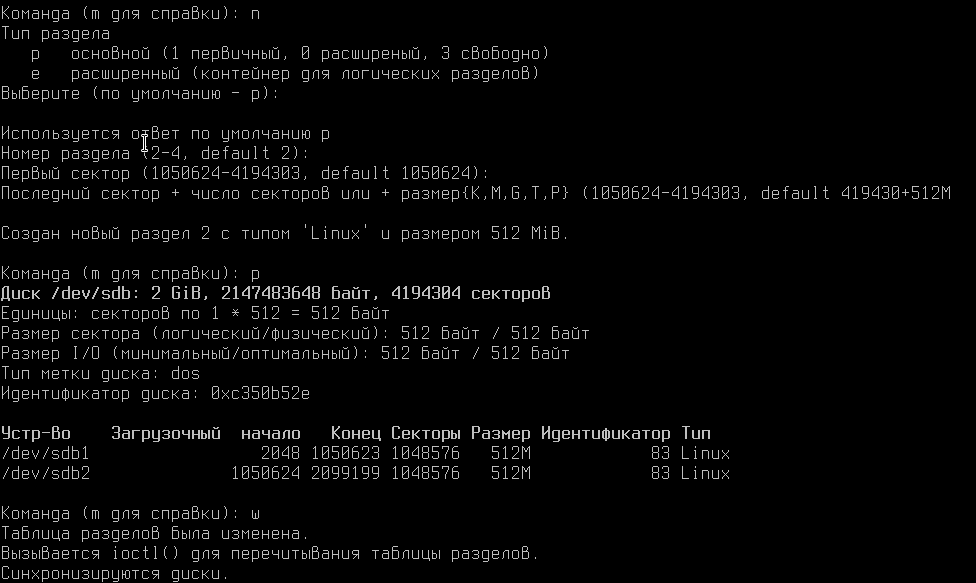
2.Добавьте 2 новых жестких диска в в виртуальную машину ( SCSI и IDE). Для добавления новых дисков виртуальную машину нужно выключить. После добавления новых дисков загрузите Astra Linux. Далее проверьте, что новые диски появились в системе.

Например, один из наших новых дисков определился в системе как /dev/sdc.

Используя команду fdisk, создайте два новых раздела (/dev/sdc1 и /dev/sdc2) на данном диске, размером 512 M. Перезагрузитесь, чтобы удостовериться, что вы корректно изменили разделы на жестком диске.







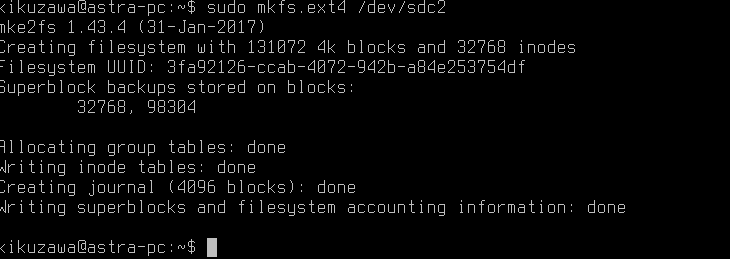
3.Используя команду mke2fs или команду mkfs.ext2, создайте новуюфайловую систему ext2 на новом логическом разделе /dev/sdc1.

|  |
| --- |
| sudo mkfs.ext2 /dev/sdc1  Note  Это команда для создания файловой системы. mkfs расшифровывается как "make filesystem" (создать файловую систему). ext2 указывает, что вы хотите создать файловую систему типа ext2. Ext2 — это одна из старейших и наиболее распространенных файловых систем в Linux. |



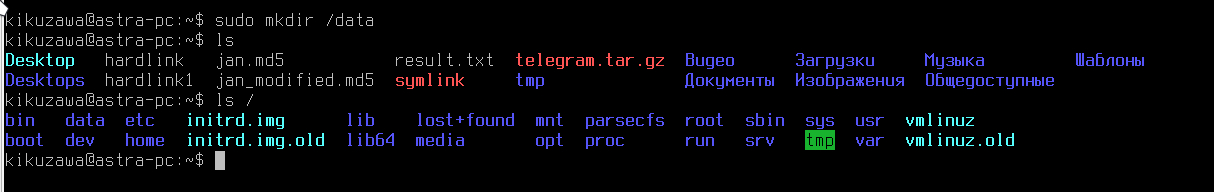
4.На разделе /dev/sdc2 создайте файловую систему ext4

|  |
| --- |
| sudo mkfs.ext4 /dev/sdc2  Note  mkfs.ext4 - это команда для создания файловой системы. mkfs расшифровывается как "make filesystem" (создать файловую систему). ext4 указывает, что вы хотите создать файловую систему типа ext4. Ext4 — это более современная версия файловой системы ext3, которая предлагает улучшенные характеристики, такие как более высокая производительность, поддержка больших файлов и улучшенная надежность. |



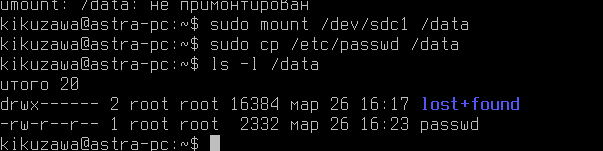
5.Создайте директорию /data, в которую вы будете монтировать новый логический том /dev/sdc2.

|  |
| --- |
| Для создания директории, можете воспользоваться командой, которая представлена ниже:  sudo mkdir /data |



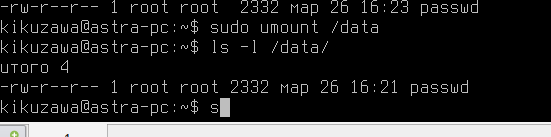
6.Используйте команду mount, чтобы смонтировать новый логический том в директорию /data. Скопируйте /etc/passwd в директорию /data и проверьте, что копирование было успешно.

|  |
| --- |
| Покажу ниже пример использования.  Для начала покажу, как смонтировать диск /dev/sdс1 на директорию /data  sudo mount /dev/sdс1 /data  После этого копируем /etc/passwd в /data. Команда представлена ниже:  sudo cp /etc/passwd /data  Теперь сделайте проверку:  ls -l /data |



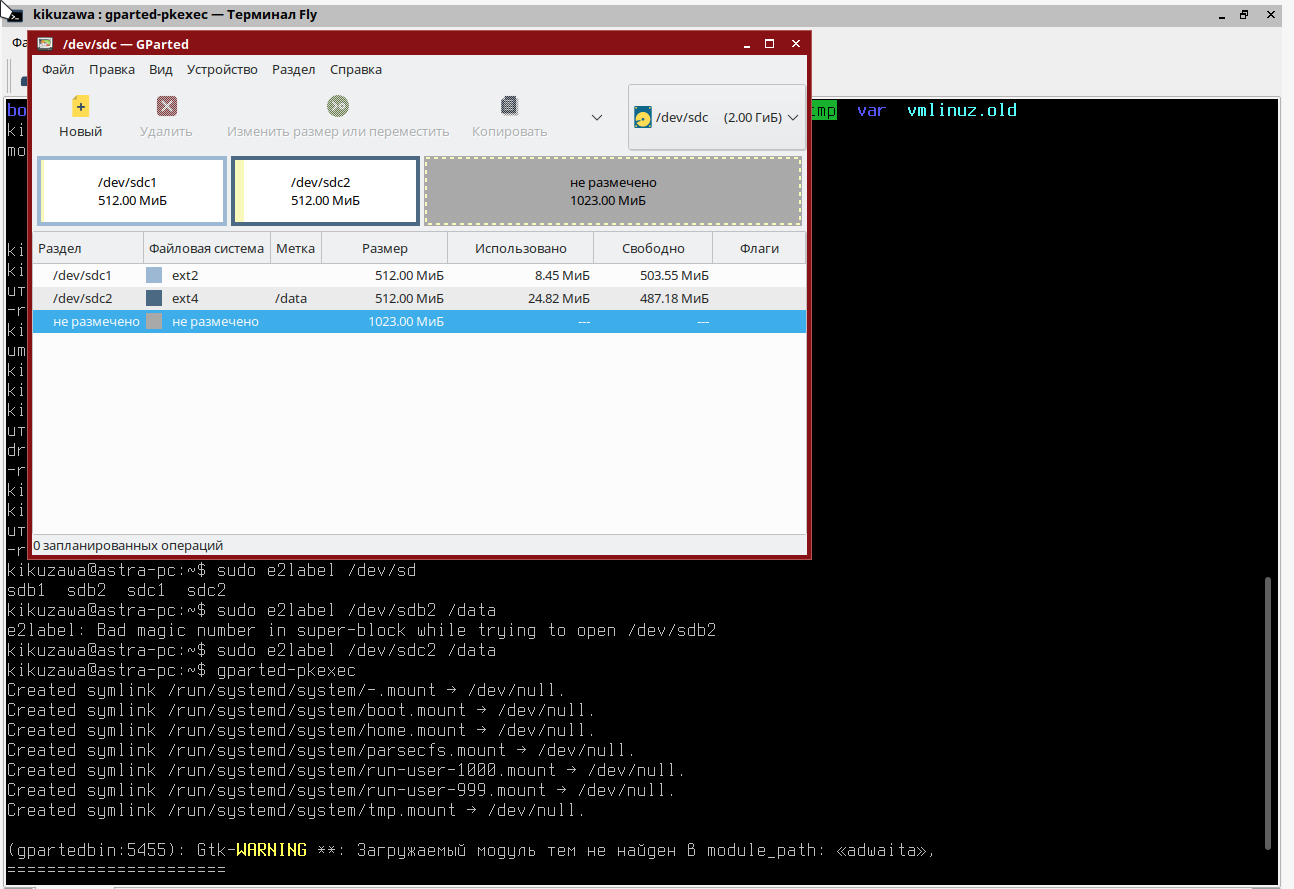
7.Затем размонтируйте директорию. Еще раз проверьте содержимое каталога /data.

|  |
| --- |
| Теперь попробуем размонтировать директорию. Для этого используйте команду, которая представлена ниже:  sudo umount /data  Теперь нам нужно проверить, что принадлежит ли диску:  ls -l /data |



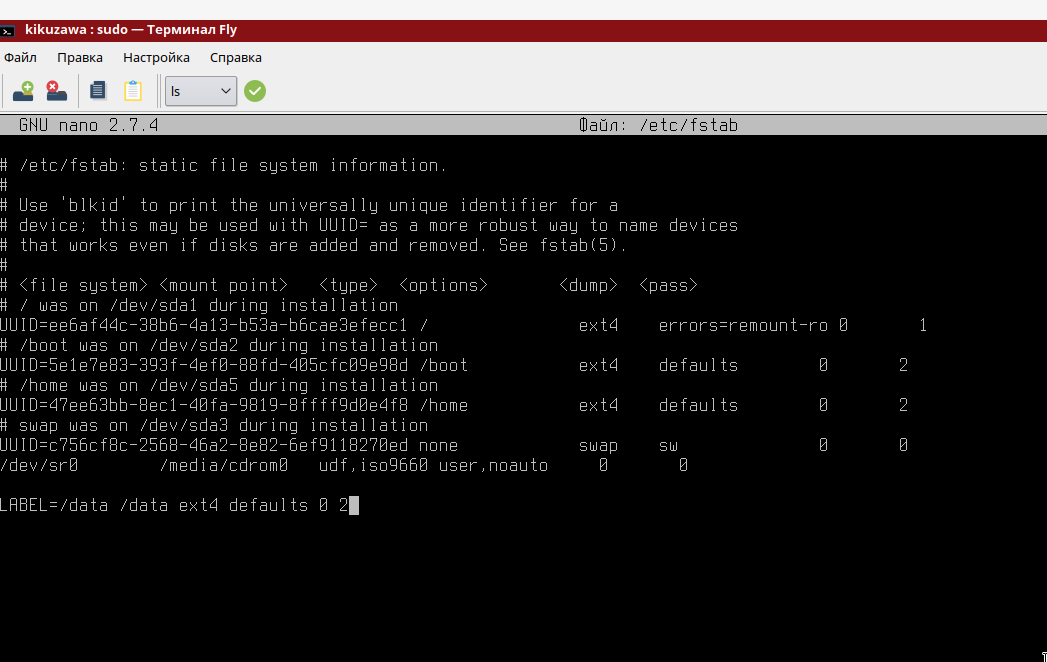
8.Добавьте метку /data к новому разделу с помощью команды e2label.

|  |
| --- |
| Для выполнения задания, используйте команду ниже:  sudo e2label /dev/sdс2 /data  Посмотреть наличие метки можете в приложении gparted. |



9.Отредактируйте файл /etc/fstab так, чтобы новый раздел монтировался при загрузке системы. Проверьте, что вы правильно прописали данную строку в файл fstab

|  |
| --- |
| Для начала откроем файл, который мы собираемся редактировать:  sudo nano /etc/fstab  Теперь добавьте строку в конце для монтирования раздела автоматически при загрузке:  LABEL=/data /data ext4 defaults 0 2 |

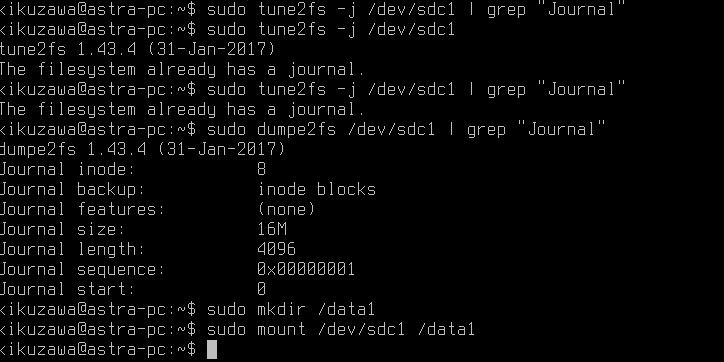


10.Перезагрузите систему и убедитесь, что новый раздел монтируется автоматически.

|  |
| --- |
| Для перезагрузки системы используйте команду ниже:  sudo reboot  Для просмотра разделов используйте команду ниже:  ls -l /data |

11.Посмотрите свойства файловой системы для раздела /dev/sdc1. Включено ли журналирование данной файловой системы? Если нет, то включите журналирование для раздела /dev/sdc1. Создайте для данного раздела точку монтирования /data1 и смонтируйте туда этот слайс.

|  |
| --- |
| Как же включить журналирование? Для этого воспользуйтесь командой, которая представлена ниже:  sudo tune2fs -j /dev/sdс1 | grep "Journal"  Note  Команда sudo tune2fs -j /dev/sdс1 | grep "Journal" пытается включить журнал для файловой системы на разделе /dev/sdс1 и затем выводит информацию о журнале, если такая информация присутствует в выводе команды. Если журнал был успешно добавлен, вы увидите соответствующую строку в выводе.  Более подробное описание команды   * sudo: Эта команда позволяет выполнять другие команды с правами суперпользователя (root). Это необходимо, так как tune2fs требует повышенных привилегий для изменения параметров файловой системы. * tune2fs -j /dev/sdb1: tune2fs — это утилита для настройки параметров файловой системы ext2, ext3 и ext4. Опция -j указывает на то, что вы хотите включить журнал для файловой системы на указанном разделе. Если файловая система уже является ext3 или ext4, то эта команда добавит журнал, если он еще не был включен. В данном случае команда применяется к файловой системе на разделе /dev/sdb1. * | (пайп): Этот символ используется для передачи вывода одной команды в качестве ввода для другой команды. В данном случае вывод tune2fs передается в команду grep. * grep "Journal": grep — это утилита для поиска строк, соответствующих заданному шаблону. В данном случае она ищет строки, содержащие слово "Journal" в выводе команды tune2fs. Это может быть полезно для проверки, была ли успешно включена функция журнала.   Теперь посмотрим есть ли журналирование на раздел. Для этого используйте команду, которая представлена ниже:  sudo dumpe2fs /dev/sdс1 | grep "Journal"  Note  Команда sudo dumpe2fs /dev/sdb1 | grep "Journal" выводит информацию о журнале файловой системы на разделе /dev/sdb1, если таковой имеется. Это может помочь вам узнать, включен ли журнал и какие параметры он имеет.  Более подробное описание команды   * sudo: Эта команда позволяет выполнять другие команды с правами суперпользователя (root). Это необходимо, так как dumpe2fs требует повышенных привилегий для доступа к информации о файловой системе. * dumpe2fs /dev/sdb1: dumpe2fs — это утилита, которая выводит информацию о файловой системе ext2, ext3 или ext4, находящейся на указанном разделе. В данном случае, она анализирует файловую систему на разделе /dev/sdb1. Эта команда выводит множество деталей о файловой системе, включая информацию о размере, количестве блоков, состоянии, метаданных и других параметрах. * | (пайп): Этот символ используется для передачи вывода одной команды в качестве ввода для другой команды. В данном случае вывод dumpe2fs передается в команду grep. * grep "Journal": grep — это утилита для поиска строк, соответствующих заданному шаблону. В данном случае она ищет строки, содержащие слово "Journal" в выводе команды dumpe2fs. Это может быть полезно для получения информации о журнале файловой системы, если он включен. Журнал позволяет отслеживать изменения и восстанавливать файловую систему в случае сбоя.   Попробуем создать теперь точку монтирования и смонинтировать туда слайс. Для этого используйте команду, которая представлена ниже:  sudo mkdir /data1  sudo mount /dev/sdb1 /data1 |



12.Перейдите в раздел /data1 и попробуйте размонтировать его. Почему вы не можете размонтировать данный раздел?

|  |
| --- |
| Для выполнения задания воспользуйтесь командой ниже:  sudo umount /data1  Important  Размонтировать его не получится, так как он занят. |

13.Посмотрите, кто из пользователей, и какими процессами занял раздел /data1. Завершите все процессы на разделе /data1

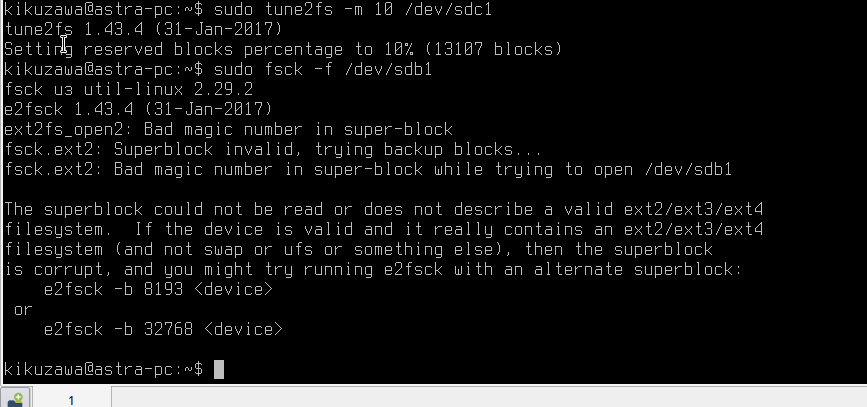
|  |
| --- |
| Посмотреть кто из пользователей занял раздел можно, используя команду ниже:  sudo lsof /data1  Более подробное описание по команде   * sudo: Эта команда позволяет выполнять другие команды с правами суперпользователя (root). Это может быть необходимо, так как некоторые процессы могут быть недоступны для обычного пользователя, и для получения полной информации может потребоваться повышенные привилегии. * lsof: List Open Files — это утилита, которая отображает список открытых файлов и процессов, которые их используют. В Linux и Unix все является файлом, включая устройства, каталоги и сокеты, поэтому lsof может быть полезен для диагностики и мониторинга системы. * /data1: Это путь к каталогу или файлу, для которого вы хотите получить информацию о открытых файлах. В данном случае команда будет искать все открытые файлы и процессы, которые используют файлы в каталоге /data1.   Как можно убить процесс? Для этого есть 2 варианта. Ниже опишу каждый.  Первый вариант - это использовать команду, которая представлена ниже:  sudo kill -9 PID  Note  PID - это уникальный идентификатор процесса.  Второй вариант - это использовать команду, которая представлена ниже:  sudo fuser -ck /data1  Более подробное описание по команде   * sudo: Эта команда позволяет выполнять другие команды с правами суперпользователя (root). Это необходимо, так как fuser может требовать повышенных привилегий для завершения процессов, которые используют указанный ресурс. * fuser: Это утилита, которая показывает идентификаторы процессов (PID), использующих указанные файлы или сокеты. Она может также использоваться для завершения этих процессов. * -c: Этот параметр указывает fuser обрабатывать все файлы в указанном каталоге и его подкаталогах. То есть, если вы укажете каталог, fuser будет искать процессы, использующие файлы не только в этом каталоге, но и во всех его подкаталогах. * -k: Этот параметр указывает fuser завершить все процессы, которые используют указанные файлы или каталоги. Это может быть полезно, если вы хотите освободить ресурсы, занятые определенными процессами. * /data1: Это путь к каталогу, для которого вы хотите найти и завершить процессы, использующие его. |

14.Попробуйте размонтировать раздел /data1 снова. Что произошло?

|  |
| --- |
| Для выполнения задания используйте команду ниже:  sudo umount /data1  Important  Теперь все работает хорошо, так как мы удалили все процессы и данные с данного раздела. |

15.Увеличьте резервируемое место (minfree) файловой системой до 10% на разделе /dev/sdc1. Осуществите проверку файловой системы для раздела /dev/sdc1

|  |
| --- |
| Как увеличить резервируемое место файловой системы на 10%? Для этого используйте команду, которая представлена ниже:  sudo tune2fs -m 10 /dev/sdc1  Note  Раздел вы можете указать свой. Необязательно, что у вас точно такой же будет.  Теперь как осуществить проверку? Для этого вы можете 2 разных команды, обе представлю ниже:  Первый вариант через fsck:  sudo fsck -f /dev/sdb1  Второй вариант через e2fsck:  sudo e2fsck /dev/sdb1 |



Задание 3. LVM

Для данного раздела нужно установить пакет lvm2 (если он у вас не

установлен).

1.Создайте три новых раздела на диске по 512 М. При необходимости

добавьте в систему новый диск (если вы работаете на виртуальной машине).

Предположим, что в нашем случае мы добавили новый диск и он был

распознан системой как /dev/sda (соответственно, новые разделы будут

/dev/sda1, /dev/sda2 и /dev/sda3). Покажите и опишите свой диск и разделы.

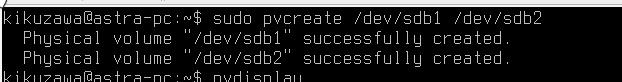
Разделы на диске должны иметь тип LVM\

|  |
| --- |
| Как создать новые разделы на определенном диске? Для этого в примере используйте команду ниже:  sudo fdisk /dev/sdd  Note  Вместо /dev/sdd может быть любой диск, который удобен вам.  Теперь на данном диске создайте разделы, приписав просто рядом цифры.  Создайте три раздела /dev/sda1, /dev/sda2, /dev/sda3 размером 512M каждый и установите их тип как "8e" (Linux LVM)  Note  Установить тип, там же только ввести вместо n - t |

2.LVM строится на основе разделов жёсткого диска и/или целых

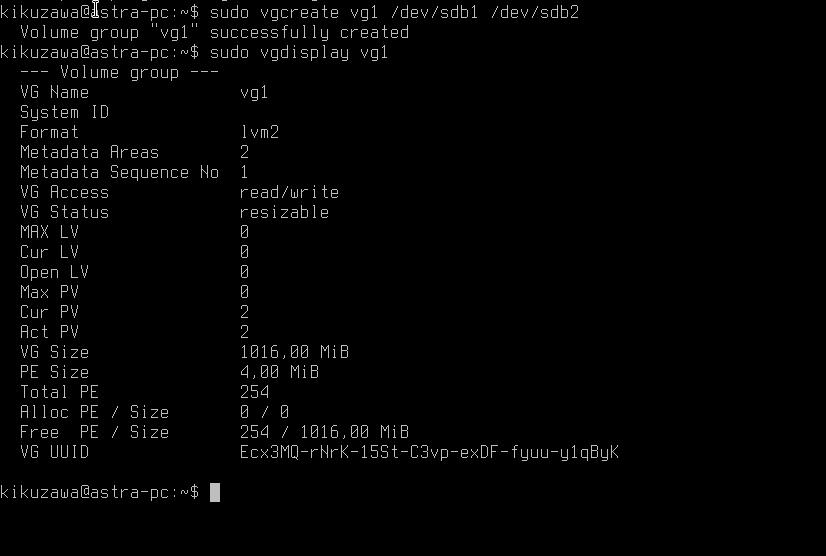
жёстких дисков. Поэтому на первых двух из созданных нами разделов (/dev/sda1, /dev/sda2) создайте физический том (physical volume). Проверьте, что физические тома созданы корректно.

|  |
| --- |
| Как создать физический том?  sudo pvcreate /dev/sda1 /dev/sda2  Note  Если вы хотите создать физический том на неразмеченном пространстве, вам нужно сначала создать раздел на диске с помощью fdisk или parted, а затем использовать pvcreate на этом разделе.  Чтобы проверить, что все прошло успешно, нужно использовать ниже команду:  pvdisplay |



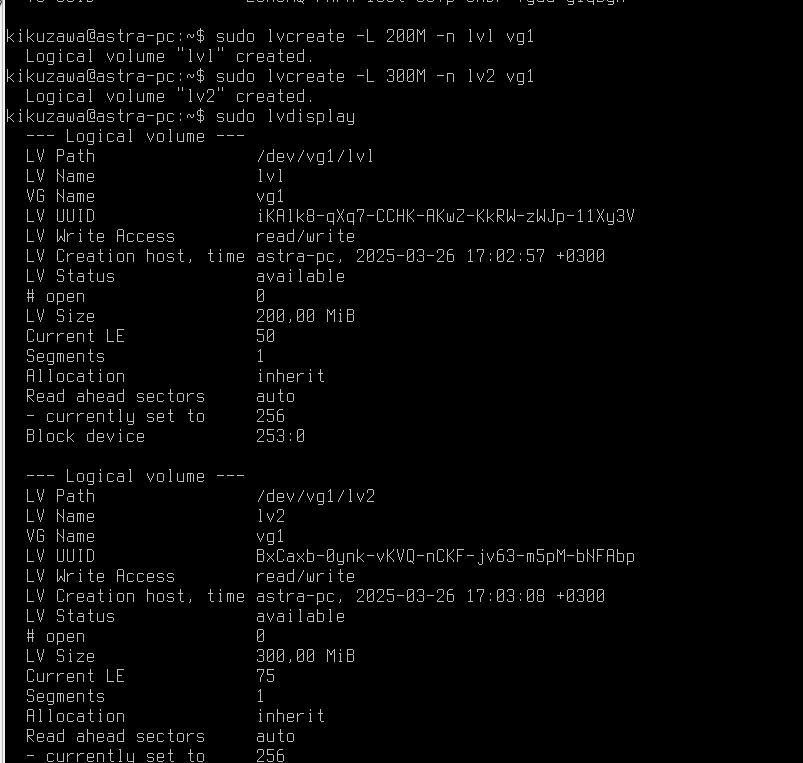
3.На первых двух физических томах (/dev/sda1 и /dev/sda2) создаём группу томов, которая будет называться, например, vg1. Проверьте, что группа vg1 создана корректно. Групп можно создать несколько, каждая со своим набором томов. Но обычно это не требуется.

|  |
| --- |
| Как создать группу томов? Для этого используйте команду, которая представлена ниже:  sudo vgcreate vg1 /dev/sda1 /dev/sda2  Note  vg1 - это название группы, которую мы хотим создать.  Important  Названия физических томов могут быть абсолютно другие. В команде приведен лишь пример, который соответствует условию.  Теперь проверим существование группы. Используйте команду ниже:  sudo vgdisplay vg1 |



4.В группе томов создайте логический том lv1 размером 200 Мб и lv2 размером 300 Мб. Проверьте, что том создан корректно.

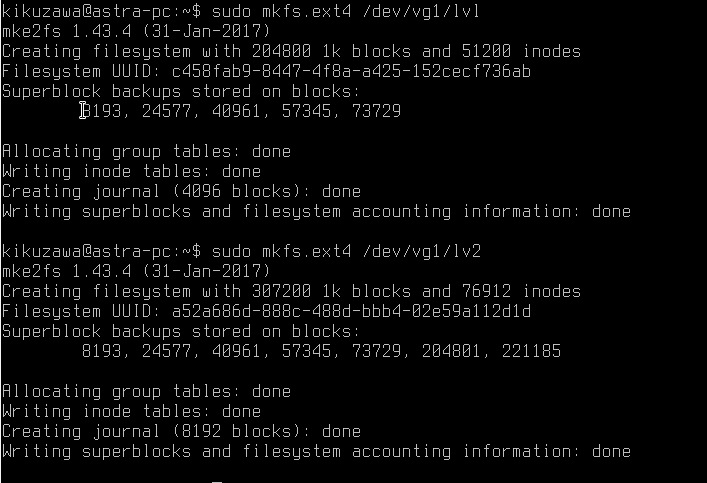
|  |
| --- |
| Создадим логический том lv1 в группе vg1 с размером 200 МБ, используя команду ниже:  sudo lvcreate -L 200M -n lv1 vg1  Теперь создадим логический том lv2 в группе vg1 с размером 300 МБ, используя команду ниже:  sudo lvcreate -L 300M -n lv2 vg1  Проверим, что томы созданы корректно, используя команду ниже:  sudo lvdisplay |



5.Теперь у вас есть блочные устройства /dev/vg1/lv1 и /dev/vg1/lv2 . Создайте на них файловую систему: на lv1 – ext4 и на lv2 – ext3.

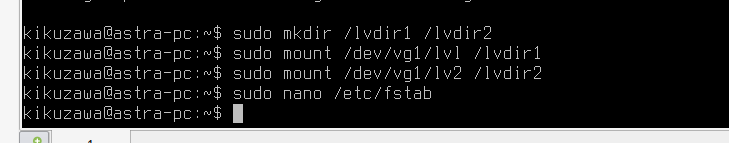
Примечание. Удаление LVM (или отдельных его частей, например, логических томов или групп томов) происходит в обратном порядке – сначала нужно отмонтировать разделы, затем удалить логические тома (lvremove), после этого можно удалить группы томов (vgremove) и ненужные физические тома (pvremove). На данном шаге удалять ничего не нужно!

|  |
| --- |
| Note  Удаление LVM (или отдельных его частей, например, логических томов или групп томов) происходит в обратном порядке - сначала нужно отмонтировать разделы, затем удалить логические тома (lvremove), после этого можно удалить группы томов (vgremove) и ненужные физические тома (pvremove). На данном шаге удалять ничего не нужно!  Создать файловые системы на блочных устройствах можно, используя команды ниже:  Для начала создадим на /dev/vg1/lv1:  sudo mkfs.ext4 /dev/vg1/lv1  Теперь создадим на /dev/vg1/lv2:  sudo mkfs.ext3 /dev/vg1/lv2 |



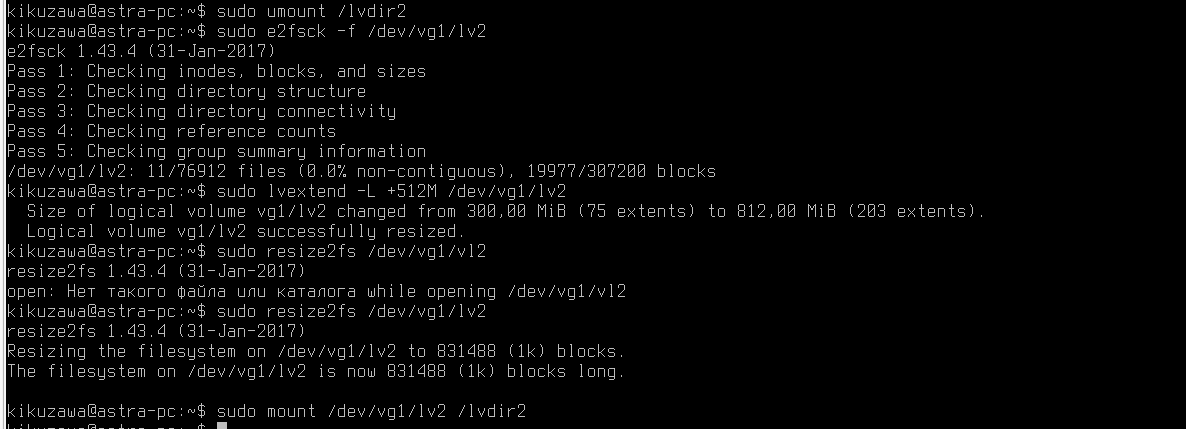
6.Смонтируйте созданные логические тома lv1 и lv2 в директории /lvdir1 и /lvdir2 (предварительно их создав). Посмотрите информацию по смонтированным томам, опишите. Выполните настройки для автоматического монтирования данных томов во время запуска системы. Для этого внесите изменения в файл /etc/fstab. Проверьте корректность правок в файле /etc/fstab без перезагрузки

|  |
| --- |
| Как монтировать логические тома и настроить автоматическое монтирование в /etc/fstab?  Для начала создадим директории, к которым будем прикреплять логические тома. Для этого используйте команду ниже:  sudo mkdir /lvdir1 /lvdir2  Теперь монтируем оба тома, используя нижестоящую команду:  sudo mount /dev/vg1/lv1 /lvdir1  sudo mount /dev/vg1/lv2 /lvdir2  Остается добавить записи в /etc/fstab для автоматического монтирования. Откроем /etc/fstab, для этого используем команду ниже:  sudo nano /etc/fstab  Теперь добавляем строки, которые прикреплены ниже:  /dev/vg1/lv1 /lvdir1 ext4 defaults 0 0  /dev/vg1/lv2 /lvdir2 ext3 defaults 0 0 |



7.Чтобы добавить раздел /dev/sda3 в группу томов, создайте физический том для этого раздела. Далее добавьте его в группу.

|  |
| --- |
| Нам нужно в начале отмонтировать раздел. Ниже команда отмонтирует раздел /lvdir2, чтобы избежать возможных ошибок во время проверки файловой системы и изменения размера тома.  sudo umount /lvdir2  Note  Отмонтирование обязательно, так как файловая система не должна быть занята при изменении размера.  Теперь проверим файловую систему, проведем исправление ошибок тома /dev/vg1/lv2. Используйте команду ниже:  sudo e2fsck -f /dev/vg1/lv2  Note  -f (force) принудительно выполняет проверку даже если файловая система кажется чистой. e2fsck работает с файловыми системами типа ext2/ext3/ext4.  Теперь произведем расширение логического тома. Команда ниже увеличивает размер логического тома /dev/vg1/lv2 на **512 МБ**  sudo lvextend -L +512M /dev/vg1/lv2  Note  -L +512M означает увеличение текущего размера на указанное значение. Без указания + размер тома будет установлен строго на заданное значение.  Теперь изменим размер файловой системы, теперь нам нужно использовать команду ниже:  sudo resize2fs /dev/vg1/lv2  Important  Эта команда безопасна для использования даже если файловая система уже занимает весь том.  Теперь обратно монтируем логический том в точку монтирования /lvdir2. Команда ниже решает это:  sudo mount /dev/vg1/lv2 /lvdir2 |

у

8.Увеличьте размер существующего тома lv2 за счет физического тома,

добавленного в группу. Для этого размонтируйте том lv2 и проверьте его на

наличие ошибок. Увеличьте lv2 на 512M. После увеличения выполните

проверку файловой системы на наличие ошибок. Подмонтируйте измененный

том и проверьте, изменился ли его размер.

|  |
| --- |
| sudo pvmove /dev/sdd2  sudo vgreduce vg1 /dev/sdd2  sudo pvremove /dev/sdd2 |

9.Чтобы убрать из работающей группы томов раздел /dev/sda2 сначала

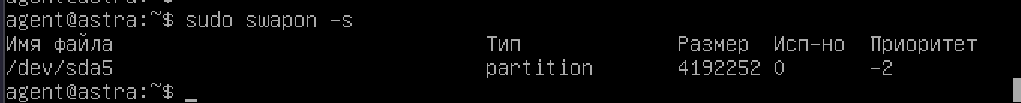
перенесите все данные с него на другие диски, затем удалите его из группы

томов, после этого удалите физический том. (прошлый вопрос)

Задание 4. Swap

1.Посмотрите текущие параметры swap-а в системе swapon –s

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Посмотрите текущие параметры swap-а в системе, используя команды ниже:  sudo swapon –s |



2.На одном из дисков (например, /dev/sdc) выделите отдельный

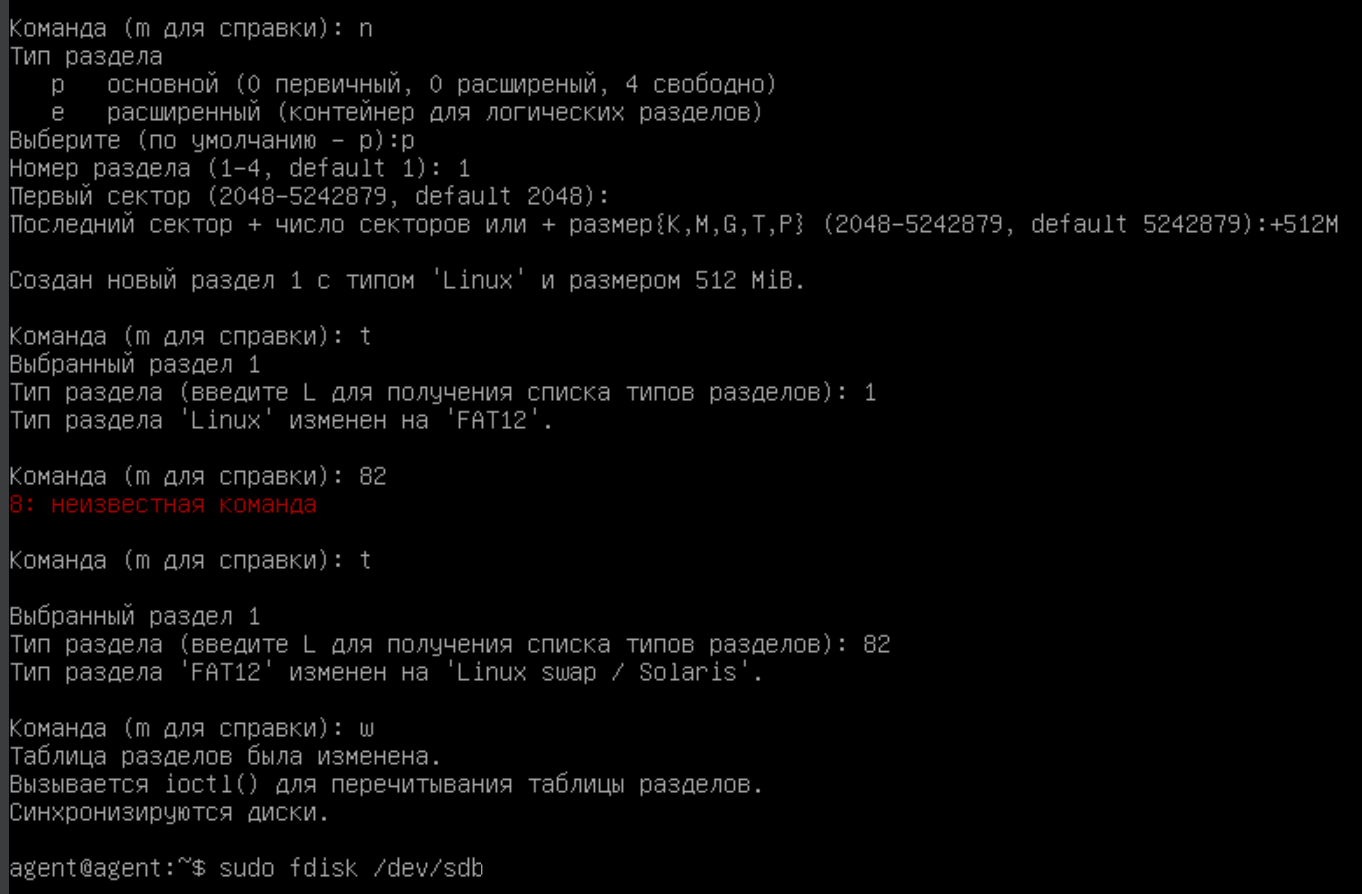
раздел, например, /dev/sdc3 (использовать под swap). Размер раздела можно

задать произвольно. Не забудьте изменить id раздела (Linux swap). В подменю

команды fdisk: n – новый раздел; w-сохранение разбиения на диск; t – id

раздела (для swap ставим 82).

|  |
| --- |
| Important  Для выполнения задания я использовал терминал через приложение Konsole. Выполняю на sdb, который добавил раньше.  sudo fdisk /dev/sdс  Создайте новый раздел (например, /dev/sdc3), установите тип раздела как 82 (Linux swap). Сохраните изменения и выйдите из fdisk. |



3. Создайте swap из нового раздела командой mkswap, подключите

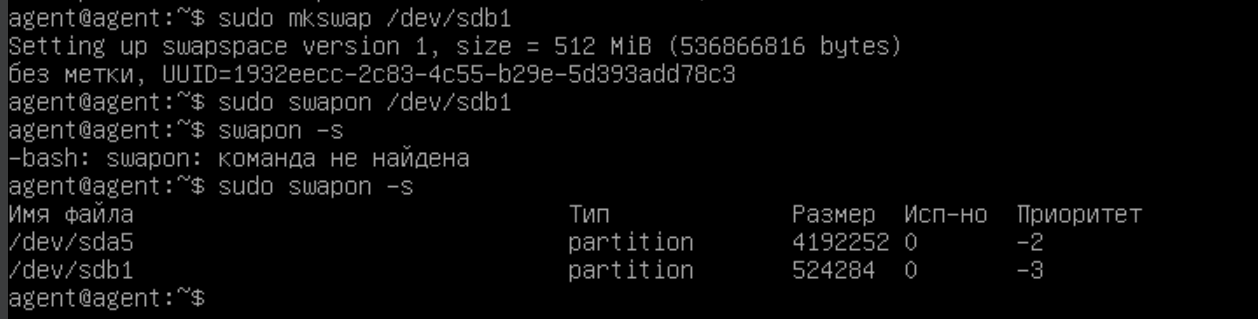
созданный swap-раздел, проверьте, что swap-раздел был добавлен к основному

swap.

Примечание. Если на диске нет места под создание новых разделов,

можно создать файл для использования его в кчестве swap.

|  |
| --- |
| Important  Для выполнения данного задания я использовал консоль, которая открывается через приложение Konsole  Теперь создаем swap:  sudo mkswap /dev/sdс3  sudo swapon /dev/sdс3  Проверка, что у нас добавилось все нормально:  sudo swapon -s |



4. Создайте файл определенного размера, например, 500M

dd if=/dev/zero of=/swapfile bs=1M count=500

|  |
| --- |
| Important  Для выполнения задания я использовал терминал, который открывается через приложение Konsole.  Чтобы создать файл определенного размера, используйте команду, которая представлена ниже:  dd if=/dev/zero of=/swapfile bs=1M count=500 |

5. Создайте swap из нового файла командой mkswap. Подключите

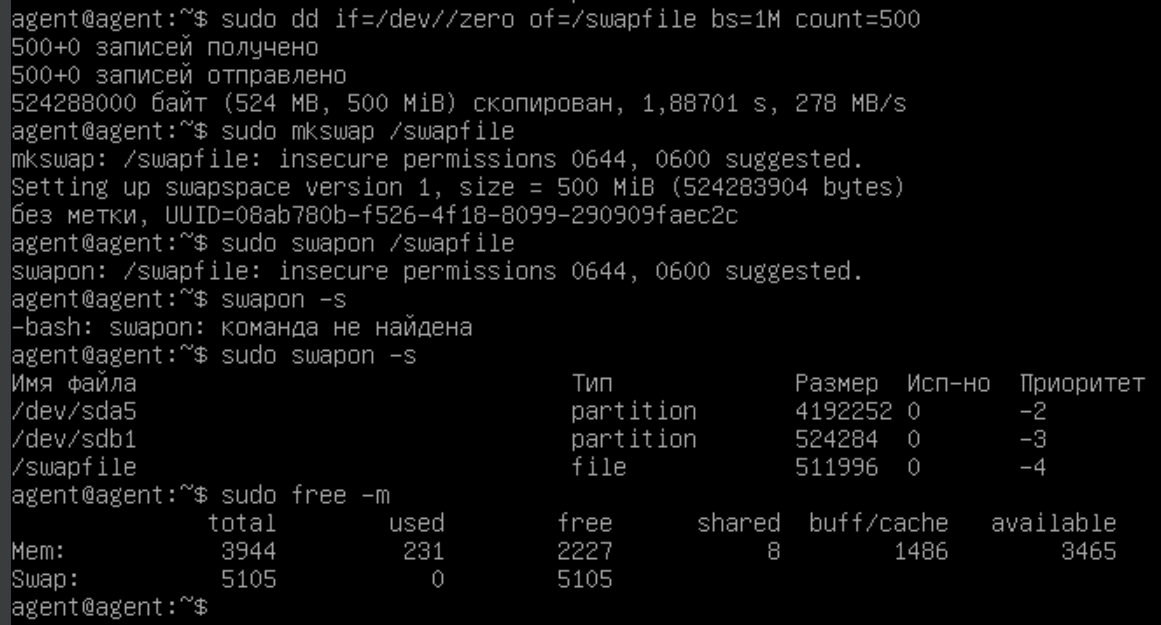
созданный swap-файл.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через терминал Konsole.  Создаем /swapfile, используя команду, которая представлена ниже:  sudo mkswap /swapfile  sudo swapon /swapfile  Проверка, что swap-файл был добавлен:  sudo swapon -s |

6. В выводе команды top или команды free должно появиться

упоминание, что свопинга в системе прибавилось. Проверьте это.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Теперь выполните данную команду:  free -h  Important  В выводе команды top или команды free должно появиться упоминание, что свопинга в системе прибавилось. Проверьте это. |



7. Отключие файл подкачки swapoff /swapfile

|  |
| --- |
| Important  Для выполнения данного задания я использовал Konsole.  Теперь для удаления файла подкачки используйте команду, которая представлена ниже:  sudo swapoff /swapfile  Проверить можно, используя команду:  sudo swapon -s |



8. Чтобы не подключать swap-файл или swap-раздел каждый раз,

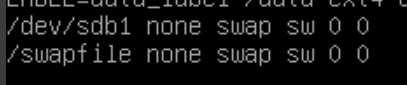
добавьте соответствующую запись в /etc/fstab:

# vi /etc/fstab

/dev/sdc3 none swap sw 0 0

/swapfile none swap sw 0 0

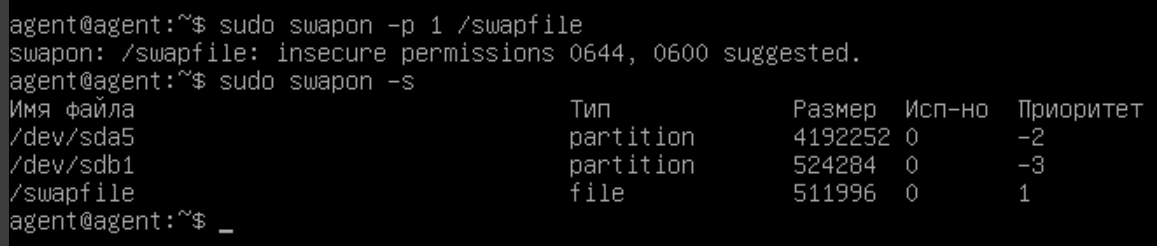
|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через терминал Konsole.  Выполните команду ниже для изменения файла:  sudo nano /etc/fstab  Теперь добавим эти строки в файл:  /dev/sdd3 none swap sw 0 0  /swapfile none swap sw 0 0 |



9. Установите, наивысший приоритет (p1) для файла подкачки

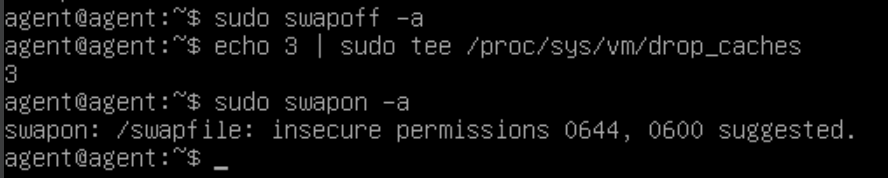
командой swapon

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через терминал Konsole.  Для выполнения задания я использовал команду, которая представлена ниже:  sudo swapon -p 1 /swapfile |



10. Произведите очистку swap-пространства на вашем компьютере

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал Konsole.  sudo swapoff -a  sudo swapon -a |



11. Измените параметр swappiness временно (до перезагрузки

системы):

echo 50 > /proc/sys/vm/swappiness

Также измените значение по умолчанию, для этого необходимо

изменить параметр

vm.swappiness в файле /etc/sysctl.conf

vm.swappiness=50

Следует отметить, что при больших значениях система потеряет в

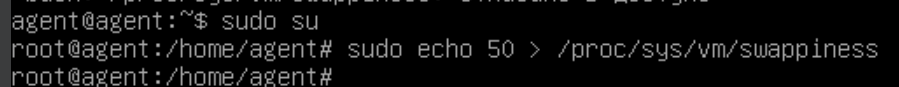
отзывчивости (будет вытеснять память, с которой работают приложения, в

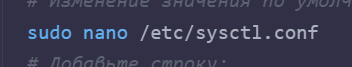
своп, хотя оперативной памяти ещё много). При малых значениях система

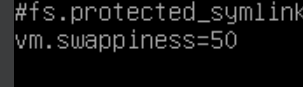
работает отзывчивей, но когда оперативная память заканчивается, система

начинает активно свопиться и притормаживать.

|  |
| --- |
| Important  Для выполнения задания я использовал терминал, который открывается через Kosnole.  Измените параметр swappiness временно (до перезагрузки системы):  echo 50 > /proc/sys/vm/swappiness  Также измените значение по умолчанию, для этого необходимо изменить параметр vm.swappiness в файле /etc/sysctl.conf, используя команду ниже:  Открываем конфиг:  sudo nano /etc/sysctl.conf  Меняем параметр:  vm.swappiness=50  Следует отметить, что при больших значениях система потеряет в отзывчивости (будет вытеснять память, с которой работают приложения, в своп, хотя оперативной памяти ещё много). При малых значениях система работает отзывчивей, но когда оперативная память заканчивается, система начинает активно свопиться и притормаживать.  echo 50 | sudo tee /proc/sys/vm/swappiness  Теперь установим параметр.  sudo sysctl -w vm.swappiness=50 |



****



12. Также можно попробовать увеличить\уменьшить объём потребляемой системой памяти за счёт изменения размеров дискового кеша.Уровень выделяемой под кеш памяти хранится в /proc/sys/vm/vfs\_cache\_pressure. Значение по умолчанию: 100.

Чтобы использовать меньше памяти под дисковые кеши (не

желательно), поставьте значение 50. Если, наоборот, хочется больше

отзывчивости системы, увеличьте размер кеша:

echo 1000 > /proc/sys/vm/vfs\_cache\_pressure

Измените параметры до полного удовлетворения. Для того, чтобы

настройки стали постоянными, занесите нужный параметр в файл

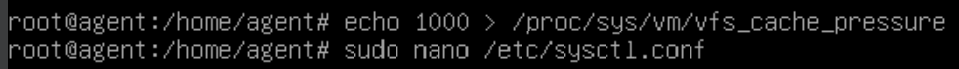
/etc/sysctl.conf

# vi /etc/sysctl.conf

vm.vfs\_cache\_pressure = 1000

Привести скриншот и пояснить работу данного пункта.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал Konsole.  Теперь используем команду для просмотра файла:  sudo nano /etc/sysctl.conf  Теперь ставим данный параметр в файле:  vm.vfs\_cache\_pressure = 1000  echo 1000 | sudo tee /proc/sys/vm/vfs\_cache\_pressure  sudo sysctl -w vm.vfs\_cache\_pressure=1000  Чтобы сделать эти настройки постоянными, добавьте соответствующие строки в файл /etc/sysctl.conf:  vm.swappiness=50  vm.vfs\_cache\_pressure=1000  После внесения изменений перезагрузите систему или выполните команду  sudo sysctl -p |



Лабораторная работа №6

Шифрование дисков LUKS

Цель работы – научится выполнять шифрование разделов/дисков,

проводить мониторинг жестких дисков.

1

Проверка работоспособности жесткого диска

1. Проверить общее состояние диска с помощью smartctl.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал через приложение Konsole.  В Astra Linux по умолчанию нет приложения для просмотра состояния. Скачайте приложение, используя команду ниже:  sudo apt install smartmontools  После установки сервис мониторинга smartd запускается автоматически. Проверить его состояние можно командой:  systemctl status smartd  После того, как сервис запущен, давайте посмотрим на какой-нибудь диск. Например, чтобы посмотреть состояние диска /dev/sda используйте команду, которая представлена ниже:  sudo smartctl -i /dev/sda  Note  Без sudo данная команда не заработает. На астре будет написано, что такой команды нет ради безопасности.  Если хотите поcмотреть какие диски есть, то используйте команду, которая представлена ниже:  sudo smartctl --scan |

2. Посмотреть дополнительную информацию по диску с помощью smartctl.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через терминал Konsole.  В Astra Linux по умолчанию нет приложения для просмотра состояния. Скачайте приложение, используя команду ниже:  sudo apt install smartmontools  После установки сервис мониторинга smartd запускается автоматически. Проверить его состояние можно командой:  systemctl status smartd  Например, для просмотра дополнительной информации по диску /dev/sdb, используйте команду, которая представлена ниже:  sudo smartctl --all /dev/sdb  Note  Все диски в системе вы можете просмотреть, используя команду sudo fdisk -l. |

3. Выполнить расширенный тест диска с помощью smartctl.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал через приложение Konsole.  В Astra Linux по умолчанию нет приложения для просмотра состояния. Скачайте приложение, используя команду ниже:  sudo apt install smartmontools  После установки сервис мониторинга smartd запускается автоматически. Проверить его состояние можно командой:  systemctl status smartd  После того, как заработал сервис, начнем выполнение задания. Например, я проведу расширенный тест для диска /dev/sdb, используя команду, которая представлена ниже:  sudo smartctl -a --test=long /dev/sdb  Note  Для просмотра всех дисков, которые есть в системе, используйте команду sudo fdisk -l. |

4. Распечатать журналы ошибок диска с помощью smartctl.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал через приложение Konsole.  В Astra Linux по умолчанию нет приложения для просмотра состояния. Скачайте приложение, используя команду ниже:  sudo apt install smartmontools  После установки сервис мониторинга smartd запускается автоматически. Проверить его состояние можно командой:  systemctl status smartd  После того, как у вас заработал сервис, используйте команду, которая представлена ниже. Я здесь делал на примере диска /dev/sdb:  sudo smartctl -l error /dev/sdb  Note  Для просмотра всех дисков в системе sudo fdisk -l. |

5. Посмотреть информацию о диске с помощью утилиты hdparm.

|  |
| --- |
| Для выполнения задания я пользовался приложением Konsole.  Пример команды, которая выполняет задание:  hdparm -i /dev/sda  Note  Вместо /dev/sda может быть абсолютно другой диск.  Important  На версии 1.8 Astra Linux плохо отображалось у меня. В терминале, который открывается через CTRL + ALT + F1 вообще ничего не отображется. Если открывать в Konsole, то пишет ошибку считывания. |

6. Посмотреть текущие настройки для различных флагов диска с

помощью утилиты hdparm.

|  |
| --- |
| Important  Для выполнения задания я пользовался терминалом из приложения Konsole.  Выполните команду, которая представлена ниже:  sudo hdparm -i /dev/sda  Теперь по некоторым источникам было сказано, что надо смотреть на dma, pio. Типо это будет результат задания.  Note  У меня ничего не отображалось, выдавало ошибку считывания.  Скриншот в прошлом задании |

**2**

**Шифрование диска**

1.Установите cryptsetup-luks

|  |
| --- |
| Important  Для выполнения задания я пользовался терминалом Konsole.  На момент 16.02.2025 данная команда актуальна:  sudo apt install cryptsetup  Important  На момент версии 1.8 пакет уже называется по-другому. Сейчас это не cryptsetup-luks, а просто cryptsetup. Если хотите посмотреть как пакет сейчас называется, то вам нужно войти в synaptic и там искать что-нибудь подобное по описанию. |

2. Создайте новый раздел на диске (можно использовать весь диск)

|  |
| --- |
| Important  Для выполнения задания я пользовался терминалом, который открывается через приложение Konsole. Подключите диск или внешний SSD для выполнения данного задания. Вам нужно обязательно примонтировать!  Note  В моем случае внешний SSD назывался /dev/sdb, буду выполнять задание относительно него. Если вы хотите посмотреть какие у вас диски есть, то можете использовать команду sudo parted -l.  Откройте диск хранения, который вы собираетесь разделить, выполнив следующую команду:  sudo parted /dev/sdb  Important  Всегда указывайте запоминающее устройство. Если вы не укажете имя диска, он будет выбран случайным образом.  Теперь я создам таблицу разделов gpt, используя команду ниже:  mklabel gpt  Теперь для проверки того, что таблица была нормально построена используйте команду, которая представлена ниже:  print  Давайте создадим новый раздел размером 1854 Мбайт, используя файловую систему ext4. Назначенное начало диска должно быть 1 МБ, а конец диска - 1855 МБ.  mkpart primary ext4 1MB 1855MB  Для сохранения используйте команду quit. Результаты наших работ можете просмотреть, используя команду, которая представлена ниже:  sudo parted -l |

3. Отформатируйте раздел (диск) LUKS, например /dev/sdc1.

|  |
| --- |
| Important  Для выполнения задания я использовал терминал, который открывается через приложение Konsole. Вам нужно преждевременно подключить диск или флешку для выполнения задания.  В начале выбираем раздел, который хо тим форматировать. Для этого посмотрите какие есть разделы, используя команду ниже:  sudo fdisk -l  После того, как мы увидели все разделы можем попробовать форматировать диск под LUKS, используя команду ниже:  sudo cryptsetup luksFormat /dev/sda  После этого введите: YES  Для ключевой фразы я использовал пароль: 1234  Note  Если cryptsetup жалуется, что не может отформатировать диск под LUKS,то удалите все разделы на диске, используя gparted. После удаления советую перезагрузиться. |

4. Подключите зашифрованный диск

|  |
| --- |
| Important  Для выполнения задания я пользовался терминалом, которое открывается через приложение Konsole.  Чтобы узнать какие диски и разделы у вас есть, нужно использовать команду, представленную ниже:  sudo fdisk -l  Для подключения к диску я использовал команду, которая представлена ниже:  sudo cryptsetup luksOpen /dev/sdb4 disk1  Note  Вместо /dev/sdb4 может быть абсолютно другой раздел. В прошлом задании вы как раз шифровали диск, поэтому смотрите все действия оттуда, если не шифровали диск.  Что делает данная команда?  Команда sudo cryptsetup luksOpen /dev/sdb4 disk1 выполняет следующие действия:   * sudo: Эта часть команды позволяет выполнять команду с правами суперпользователя (root). Это необходимо, так как работа с зашифрованными дисками требует повышенных привилегий. * cryptsetup: Это утилита для управления зашифрованными дисками, использующая LUKS (Linux Unified Key Setup). * luksOpen: Это подкоманда cryptsetup, которая открывает зашифрованный LUKS-том. Она расшифровывает содержимое зашифрованного раздела и делает его доступным для использования. * /dev/sdb4: Это путь к зашифрованному разделу на диске. В данном случае это четвертый раздел на втором диске (sdb). * disk1: Это имя, под которым будет доступен расшифрованный том. После выполнения команды, зашифрованный раздел будет доступен в /dev/mapper/disk1.   Таким образом, команда открывает зашифрованный раздел /dev/sdb4, позволяя пользователю получить доступ к его содержимому через /dev/mapper/disk1. После выполнения этой команды, пользователю будет предложено ввести пароль для расшифровки раздела.  После этого вам остается ввести парольную фразу, которую вы задавали при шифровании диска. |

5. Создайте файловую систему на подключенном диске

|  |
| --- |
| Important   * Для выполнения задания я использовал терминал, который открывается через приложение Konsole. * Перед тем, как создавать файловую систему на диске, вам нужно подключить диск, сделать mount, выполнить 4 задание   Для создания файловой системы на данном диске можете воспользоваться командой, которая представлена ниже:  sudo mkfs.ext4 /dev/mapper/disk1 |

6. Cоздайте директорию для монтирования зашифрованного раздела и

смонтируйте зашифрованный раздел в нее

|  |
| --- |
| Important  Для выполнения данного задания я пользовался терминалом, которое открывается через приложение Konsole. Предпологается, что Вы выполнили прошлые задания с данного блока.  Создаем директорию, используя команду ниже:  sudo mkdir /mnt/disk1  Теперь монтируем, используя команду ниже:  sudo mount /dev/mapper/disk1 /mnt/disk1 |

7. Просмотрите список используемых ключей. Сколько свободных

слотов для ключей присутствует?

|  |
| --- |
| Для выполнения задания я использовал я использовал терминал, который открывается через приложение Konsole. Ожидается, что до этого вы выполнили прошлые задания.  Для просмотра списка используемых ключей используйте команду, которая представлена ниже:  sudo cryptsetup luksDump /dev/sdb4  Далее, чтобы узнать количество, у Вас будет параметр Keyslots. Вот там вы глазками уже смотрите. Представлю на фото ниже какой у меня результат. |

8. Добавьте ключевую фразу к слоту

|  |
| --- |
| Important  Для выполнения данного задания я пользовался терминалом, которое открывается через приложение Konsole. Предполагается, что до этого вы выполнили прошлые задания.  Теперь добавим ключевую фразу к слоту, используя команду, которая представлена ниже:  sudo cryptsetup luksAddKey /dev/sdb4  Note  Вместо /dev/sdb4 может быть абсолютно другой раздел или даже диск.  Далее вас попросят ввести ключевую фразу, я лично для удобства использовал 1234. |

9. Добавьте ключевой файл

|  |
| --- |
| Important  Для выполнения данного задания я пользовался терминалом, который открывается через приложение Konsole. Предпологается, что вы выполнили прошлые задания.  Для своего удобства осталю команду, которая создает файл размером 5 килобайт с случайными данными из if:  sudo dd if=/dev/urandom of=/keyfile1 bs=1024 count=4  Теперь добавим ключевой файл, используя команду ниже:  sudo cryptsetup luksAddKey /dev/sdb4 /keyfile1  Note  Вместо /dev/sdb4 может быть абсолютно другой раздел или даже диск. |

10. Разблокируйте зашифрованный раздел диска при помощи ключевого

файла.

|  |
| --- |
| Important  Для выполнения данного задания я пользовался терминалом, который открывается через Konsole. Предполагается, что до этого вы выполнили прошлые задания.  Посмотрите какой вы там раздел сделали LUKS, используя команду ниже:  sudo fdisk -l  Для выполнения данного задания выполните команду, которая представлена ниже:  sudo cryptsetup luksOpen /dev/sdb4 disk --key-file /keyfile1  Note  Если у вас вылетела ошибка по типу: "Невозможно использовать устройство /dev/sda, которое используется (отображено или примонтировано)", то советую переподключить устройство. Просто вытащите и вставьте диске обратно.  Теперь удалите, используя команду:  sudo rm /keyfile1 |

11. Удалите один из ключей

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Чтобы удалить один из ключей, используйте команду, которая представлена ниже:  sudo cryptsetup luksRemoveKey /dev/sdb4  Note  Вместо /dev/sdb4 может быть абсолютно другой диск или раздел. |

12. Чтобы операционная система сама научилась подключать и

монтировать нужные криптованные устройства во время загрузки, а затем

корректно отключать их во время останова системы, добавьте по одной строке

в файлы /etc/crypttab и /etc/fstab:

# vi /etc/crypttab

lkfs /dev/sda5 none luks,cipher=aes-cbc-essiv:sha256"

# vi /etc/fstab

/dev/mapper/lkfs /mnt/lkfs ext4 defaults 0 0

115

Теперь во время каждой загрузки ОС будет спрашивать пароль для

доступа к криптованному разделу, если он будет указан неправильно –

загрузка остановится.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Для начала откроем файл, используя команду, которая представлена ниже:  sudo nano /etc/crypttab  Note  У меня данный файл был пустой.  Нужно теперь добавить данные строки в файл:  disk1 /dev/sdb4 none luks  Теперь откроем другой файл:  sudo nano /etc/fstab  Теперь добавим данную строку в файл:  /dev/mapper/disk1 /mnt/disk1 ext4 defaults 0 0  Important  После проделанных действий у меня не включалось ничего. Советую зайти в Recovery Mode и подождать пока вылетит Timeout, после этого в терминале удалите все параметры, которые выставили в лабораторной работе. |

13. Выполните шифрование домашнего каталога.

Шифрование домашнего каталога производится по точно такой же схеме

с тем лишь исключением, что перед добавлением новой записи в /etc/fstab

следует удалить старую запись, ссылающуюся на /home.

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Для начала форматируем, как показано ниже:  sudo cryptsetup luksFormat /dev/sdc1  Теперь делаем команду, которяа представлена ниже:  sudo cryptsetup luksOpen /dev/sdc1 diskhome  Создаем разметку, используя команду ниже:  sudo mkfs.ext4 /dev/mapper/diskhome  Создаем теперь место для маунта:  sudo mkdir /mnt/diskhome  Делаем маунт:  sudo mount /dev/mapper/disk1 /mnt/diskhome |

14. Выполните шифрование флешки.

При создании шифрованной флешки специальные записи в /etc/crypttab

и /etc/fstab не требуются. Подсистема HAL сама определит наличие на

устройстве хранения LUKS-раздела и передаст эту информацию среде

рабочего стола (Gnome, KDE, XFCE), которая, в свою очередь, выведет на

экран окно с просьбой ввести пароль. Единственное, что необходимо сделать

– при первом монтировании изменить права доступа на ее корневой каталог:

$ sudo chown -R student:student /media/usb\_name

$ sudo chmod g+s /media/usb\_nam

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Теперь выполните команды, которые представлены ниже:  sudo chown -R c3equalz:c3equalz <путь к флешке>  sudo chmod g+s <путь к флешке> |

Лабораторная работа №7

РАМ - идентификация и аутентификация пользователей в

AstraLinuxSE

Цель работы – понимать, как работает система PAM и как составлять

конфигурационные файлы.

1.

Создать собственное PAM-приложение, которое поможет понять,

как работает сеанс PAM. Для этого:

-включите заголовочные файлы, необходимые для использования PAM

(например, pam\_appl.h, pam\_misc.h);

-в функции main инициализируйте библиотеку PAM libpam.so (которая

загружает модули, указанные в файле конфигурации для приложения) при

помощи уникального идентификатора;

- попытайтесь выполнить аутентификацию для всех модулей и

рассмотрите сценарии отказов;

- проверьте учетные данные пользователей и параметры учетных

записей;

- откройте новый сеанс PAM;

- создайте среду для пользователя при помощи учетных данных;

- по завершении работы пользователя закройте пользовательскую среду;

- закройте сеанс PAM;

-

Выйдите из библиотеки libpam.so с соответствующим идентификатором;- выход.

|  |
| --- |
| Для компиляции программы используйте команду, которая представлена ниже:  gcc -o pam\_example pam\_example.c -lpam -lpam\_misc  Теперь необходимо создать конфигурационный файл PAM, используя команду ниже:  sudo nano /etc/pam.d/my\_pam\_app  Пример содержимого представлено ниже:  auth required pam\_unix.so  account required pam\_unix.so  session required pam\_unix.so |

2. Вы должны находится под пользователем root/ Перейдите в каталог

/etc/pam.d/. Перенесите файл su в домашнюю директорию (чтобы можно было

восстановить его). Выполните команду su из под пользователя student в

терминале, чтобы перейти в режим суперпользователя. После ввода пароля

система выдаст ошибку аутентификации, так как отсутствует конфигурационный файл для программы su, сделать скриншот.

|  |
| --- |
| Для выполнения задания я пользовался терминалом, который открывается через приложение Konsole.  Перейдем в рута, используя команду, которая представлена ниже:  sudo su  Теперь перейдем в директорию /etc/pam.d/, используя команду, которая представлена ниже:  cd /etc/pam.d  Теперь сделаем перенос файла su, используя команду ниже:  sudo mv /etc/pam.d/su ~/su\_backup  Теперь попробуем выполнить команду, которая представлена ниже:  sudo su  Important   * Будет выведен сбой при проверке подлинности. * Лучше верните su обратно. Для этого выполните команду: sudo mv ~/su\_backup /etc/pam.d/su   Бэкап  #  # The PAM configuration file for the Shadow `su' service  #  # This allows root to su without passwords (normal operation)  auth sufficient pam\_rootok.so  # Uncomment this to force users to be a member of group wheel  # before they can use `su'. You can also add "group=foo"  # to the end of this line if you want to use a group other  # than the default "wheel" (but this may have side effect of  # denying "root" user, unless she's a member of "foo" or explicitly  # permitted earlier by e.g. "sufficient pam\_rootok.so").  # (Replaces the `SU\_WHEEL\_ONLY' option from login.defs)  # auth required pam\_wheel.so  # Uncomment this if you want wheel members to be able to  # su without a password.  # auth sufficient pam\_wheel.so trust  # Uncomment this if you want members of a specific group to not  # be allowed to use su at all.  # auth required pam\_wheel.so deny group=nosu  # Uncomment and edit /etc/security/time.conf if you need to set  # time restrainst on su usage.  # (Replaces the `PORTTIME\_CHECKS\_ENAB' option from login.defs  # as well as /etc/porttime)  # account requisite pam\_time.so  # This module parses environment configuration file(s)  # and also allows you to use an extended config  # file /etc/security/pam\_env.conf.  #  # parsing /etc/environment needs "readenv=1"  session required pam\_env.so readenv=1  # locale variables are also kept into /etc/default/locale in etch  # reading this file \*in addition to /etc/environment\* does not hurt  session required pam\_env.so readenv=1 envfile=/etc/default/locale  # Defines the MAIL environment variable  # However, userdel also needs MAIL\_DIR and MAIL\_FILE variables  # in /etc/login.defs to make sure that removing a user  # also removes the user's mail spool file.  # See comments in /etc/login.defs  #  # "nopen" stands to avoid reporting new mail when su'ing to another user  session optional pam\_mail.so nopen  # Sets up user limits according to /etc/security/limits.conf  # (Replaces the use of /etc/limits in old login)  session required pam\_limits.so  # The standard Unix authentication modules, used with  # NIS (man nsswitch) as well as normal /etc/passwd and  # /etc/shadow entries.  @include common-auth  @include common-account  @include common-session  session required pam\_parsec\_cap.so  session required pam\_parsec\_aud.so  account required pam\_su.so |

3. Создать файл /etc/pam.d/su и написать в нем такую строку:

auth sufficient pam\_permit.so

Сохранить.

Снова выполнить команду su из под пользвателя student, что произошло?

Скриншот. Это произошло потому, что модуль pam\_permit.so всегда

возвращает положительный результат, sufficient тут же прерывает выполнение

цепочки и система PAM возвращает положительный результат.

Отредактируйте файл к следующему виду:

auth required pam\_permit.so

auth requisite pam\_deny.so

auth sufficient pam\_permit.so

Модуль pam\_deny.so всегда возвращает ошибку. Какой будет результат?

Проверьте. А если заменить requisite на required? Скриншоты.

|  |
| --- |
| Для выполнения задания я пользовался терминалом, который открывается через комбинацию (CTRL + ALT + F<number>), где number - это число от 1 до 6.  В начале войдите под главного пользователя, котого создали в системе. В моем случае - это c3equalz.  Теперь перейдем к созданию файла /etc/pam.d/su, для этого используйте команду, которая представлена ниже:  echo "auth sufficient pam\_permit.so" | sudo tee /etc/pam.d/su  Note  Всегда разрешает создавать.  Для редактирование файла /etc/pam.d/su используйте команду, которая представлена ниже:  nano /etc/pam.d/su  Теперь в файле замените все строки полностью, чтобы  auth required pam\_permit.so  auth requisite pam\_deny.so  auth sufficient pam\_permit.so  Note  После этого всегда будет выводится ошибка. |

4.Напишите в файле следующее правило:

auth required pam\_unix.so

После выполнения команды su будет запрошен пароль пользователя

root. Если пароль ввести правильно, то вы станете root-ом, если пароль будет

неверный, то останетесь обычным пользователем. Скриншоты.

|  |
| --- |
| Для выполнения данного задания я использовал терминал, который открывается через Konsole.  Теперь добавьте строки в файл /etc/pam.d/su, используя команду ниже:  nano /etc/pam.d/su  В файле должна быть только эта строка, которая представлена ниже:  auth required pam\_unix.so  Теперь после того, как сохранили попробуйте выполнить команду, которая представлена ниже:  sudo su  Important   * Спросит пароль, но зайти не получится. * После выполнения задания советую удалить строчку из файла, в который мы добавили. |

5. Добавьте в файл еще одну строку так, чтобы получились следующие

правила:

auth requisite pam\_wheel.so

auth required pam\_unix.so

Модуль pam\_wheel.so возвращает успех если учетная запись пользователя принадлежит группе wheel (в некоторых версиях группе root).

Выполнить команду su, что произошло? Скриншот. Команду su смогут

выполнить только пользователи, который входят в группу wheel и знают

пароль учетной записи root.

Создайте группу wheel и добавьте туда свою учетную запись, выполните

команду su. Скриншот.

После выполнения задания удалите из группы учетную запись и удалите

123

группу wheel.

|  |
| --- |
| Для выполнения данного задания я использовал терминал, который называется Konsole.  Добавление строк в файл /etc/pam.d/su:  nano /etc/pam.d/su  Теперь добавим строки в файл:  auth requisite pam\_wheel.so  auth required pam\_unix.so  Теперь создадим пользователя, который принадлжит группе wheel, для этого используйте команды, которые представлены ниже:  Создаем пользователя:  sudo useradd wheeluser  Ставим пароль:  sudo passwd wheeluser  Note  Я для удобства поставил пароль 123  Теперь создаем группу wheel:  sudo groupadd wheel  Теперь добавляем пользователя в группу, используя команду ниже:  sudo usermod -aG wheel wheeluser |

6. Измените файл, укажите две строки:

auth requisite pam\_wheel.so

auth required pam\_permit.so

Ответить кто сможет успешно выполнить команду su и, что для этого

нужно будет сделать?

После выполнения задания верните на место оригинальный файл su.

|  |
| --- |
| Для изменения файла /etc/pam.d/su используйте команду ниже:  nano /etc/pam.d/su  В файле должна быть только:  auth requisite pam\_wheel.so  auth required pam\_permit.so  Important  У меня из-под консоли, которая открывается через (CTRL + ALT + F<number>) не получается перейти в root. Скорее всего настройка не актуальна на Astra 1.8.    Доступ будет запрещен |

7. Конфигурационные файлы в каталоге /etc/pam.d/ можно создавать

только для файлов которые используют систему PAM. Создайте файл

/etc/pam.d/ls со строкой

auth requisite pam\_deny.so

# touch /etc/pam.d/ls

# vi /etc/pam.d/ls

auth required pam\_permit.so

Проверьте, будет ли выполнятся команда ls? Какой результат?

Скриншоты.

|  |
| --- |
| Для выполнения этого задания я использовал Konsole.  Создание файла /etc/pam.d/ls с содержимым:  echo "auth requisite pam\_deny.so" | sudo tee /etc/pam.d/ls  Important  У меня ничего не заблокировалось, из-под любых пользователей можно использовать команду ls. |

8.

Если Команда не использует систему PAM, То создание

конфигурационного файла в директории pam.d ни на что не повлияет.

Проверить использует ли команда систему PAM позволяет команда ldd,

которой в качестве параметра передается полный путь к файлу команды.

Команда ldd покажет какие библиотеки использует программа и если в

перечне есть libpam.so.0, libpam\_misc.so.0 значит программа использует

систему PAM.

Проверьте использует ли команда su PAM библиотеки? Скриншоты

Протестируйте на выбор другие две команды, доступные пользователю

root, скриншоты.

|  |
| --- |
| Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Проверка использования PAM библиотек командой ldd:  ldd /bin/su | grep libpam  Note  Здесь у меня нормально все отобразилось, как сказано в задании.  Список других команд для тестов с ldd, вы можете посмотреть здесь:  ls /bin/ |

9. Проверьте, используется ли в вашей системе аутентификация через

PAM. Для этого посмотрите содержимое файла /etc/nsswitch.conf. Первые три

строки этого файла как раз и задают какая система аутентификации будет

работать в системе. Ключевое слово compat показывает, что в качестве

124

системы аутентификации будет использована система PAM. Скриншот.'

|  |
| --- |
| Для выполнения данного задания я использовал консоль, которая открывается через терминал Konsole.  Проверка использования аутентификации через PAM в файле /etc/nsswitch.conf:  grep "^passwd:" /etc/nsswitch.conf  Note  Лично у меня слова compat не было, но это настройки системы по умолчанию. Так-то я ничего не менял. Результат можете увидеть на фото, это все актуально на Astra Linux 1.8. |

10. Создайте стандартного пользователя student10. Задайте ему пароль.

Измените минимальную длину пароля, вместо 8 символов установите 9.

Проверьте, работают ли новые настройки. Для этого войдите в систему под

обычным пользователем student10 в текстовом терминале (Ctrl+Alt+F1), и

поменяйте пароль используя команду # passwd. Выйдите из под пользователя

student10.

Усложните пароль (под пользователем root). Обязательными символами

в пароле должны быть: минимум 1 прописная буква, минимум одна строчная

буква и хотя бы одна цифра. Проверьте что изменения сработали, войдя под

пользователем student10.

|  |
| --- |
| Для выполнения данного задания я использовал консоль, которая открывается через комбинацию клавиш (CTRL + ALT + F<number>), где number - это число от 1 до 6.  Создание пользователя student10:  sudo useradd -m student10  Ставим пароль на пользователя, используя команду, которая представлена ниже:  sudo passwd student10  Note  Я для удобства использовал пароль 123.  Теперь попробуем поменять минимальную длину пароля. В этом случае мы будем использовать GUI, переходите по такому направлению: Настройки-> Политики учетной записи -> Параметры системы -> сложность пароля -> минимальная длина пароля.  Теперь нажмите CTRL + ALF + F<number>, где number - это число от 1 до 6. Войдите под пользователем student10, заново введите команду passwd. Теперь если ввести 8 символов, то он скажет, что пароль короткий.  Теперь перейдем к усложению пароля. Заново перейдите в GUI по такому пути: Настройки-> управление политикой безопасности -> политика учётной записи -> политика паролей -> сложность. Поставьте, чтобы была минимум 1 прописная буква, минимум 1 строчная буква, 1 цифра минимум, как на фото ниже.  Усложнить пароль: 1 прописная минимум, 1 строчная миниум, 1 цифра минимум.  Для проверки откроем терминал, используя комбинацию CTRL + ALT + F<number>, где number - это число 1 до 6.  Important  Не забывайте сохранять последние изменения в GUI. |

11. Создайте файл /etc/nologin. Добавьте текстовое сообщение в файл.

Попробуйте зайти в систему под обычным пользователем. Почему обычному

пользователю удалось или не удалось войти в систему? Удалите файл

/etc/nologin.

|  |
| --- |
| Создание файла /etc/nologin:  sudo touch /etc/nologin  Теперь откройте файл, используя команду ниже:  sudo nano /etc/nologin  Внутри файла надо написать сообщение оно будет выведено, если пользователь пострается войти: Жестко вошел. Вход в оккошке через граф : завершение работы -> новый вход.  Удаление файла /etc/nologin:  sudo rm /etc/nologin |

Лабораторная работа №8

Основы мандатного управления доступом. Настройка

параметров мандатного управления доступом и мандатного

контроля целостности

Цель работы – изучить особенности администрирования локальных

учётных записей пользователей и групп в ОССН (операционная система

специального назначения) и основы мандатного управления доступом.

Освоить администрирование основных параметров мандатного управления

доступом и мандатного контроля целостности в ОССН с применением

графических утилит и консольных команд.

Ход работы:

1 Основы мандатного управления доступом

1. В ОССН версии 1.6 создать учётную запись пользователя user, с

параметрами: максимальный и минимальный уровни доступа — 0,

неиерархические категории — нет, уровень целостности — «Высокий»,

входит в группу администраторов — astra-admin (вторичная группа),

разрешено выполнение привилегированных команд (sudo). Войти в ОССН с

учётной записью пользователя user (Уровень\_0, «Высокий»).

|  |
| --- |
| Important  Для выполнения данного задания я использовал GUI.  Проверим, что у вас есть группа astra admin. Для начала перейдите в Параметры -> Пользователи и группы (вниз пролистайте) -> Группы.    Теперь, если у вас нет группы astra admin, то создайте её. Смотрите на фото ниже для примера вам.    Note  Группа по умолчанию у меня была с самого начала установки системы. Я вручную не создавал  Теперь перейдем к созданию пользователя user. Для начала перейдите в Параметры -> Пользователи и группы (вниз пролистайте) -> Пользователи. Теперь нам нужно создать пользователя user. Выставите ему такие параметры, как показано ниже:   * Макс. уровень доступа - 0 * Мин. уровень доступа - 0 * Уровень целостности - Высокий * Входит в группу админтистраторов (вторичная группа) - astra-admin, sudo   В результате в GUI настройка выглядела у меня так:    Note  Я для удобства поставил пароль 1234.  Теперь вам остается войти под user (Уровень\_0, Высокий). |

2. Запустить графическую утилиту редактирования учётных записей

пользователей «Политика безопасности» через меню «Панель управления»

главного пользовательского меню. Открыть раздел настройки локальных

пользователей, и для созданных учётных записей пользователей user1, user2,

user3, user4 произвольно задать их параметры:

- максимальный и минимальный уровни доступа;

- минимальные и максимальные наборы неиерархических категорий;

- максимальный уровень целостности.

|  |
| --- |
| Для выполнения данного задания я использовал GUI, который есть в Astra Linux.  Переходим по такому пути: Параметры -> Пользователи и группы (вниз пролистайте) -> Пользователи.  Через граф. утилиту теперь нужно создать user1, user2, user3, user4 произвольно задать:   * максимальный и минимальный уровни доступа; * максимальный уровень целостности;   Для user1 я выставил такие параметры, которые представлены на фото ниже:    Для user2 я выставил такие параметры, которые представлены на фото ниже:    Для user3 я выставил такие параметры, которые представлены на фото ниже:    Для user4 я выставил такие параметры, которые представлены на фото ниже:    Important  Неиерархические категории в версии 1.8 называется Категории конфиденциальности. |

3. Настроить параметры учётной записи пользователя user2:

- установить минимальное количество дней между сменой пароля – 180

дней, число дней до выдачи предупреждения о смене пароля — 5 дней;

- выбрать максимальный уровень — «Уровень\_3»;

- проверить возможность задать минимальный или максимальный

набор неиерархических категорий.

Войти в ОССН с учётной записью пользователя user2, выбрав уровень

доступа «Уровень\_1». Проверить возможность выбора набора неиерархических категорий и уровня целостности. Создать в каталоге

«Документы» файл 1.txt. Выйти из ОССН.

Войти в ОССН с учётной записью пользователя user2, выбрав уровень

доступа «Уровень\_2». Создать в каталоге «Документы» файл 2.txt.

Проверить возможность чтения объектов файловой системы ОССН,

владельцем которых является учётная запись пользователя user2 (на текущем

уровне доступа «Уровень\_2»):

- открыть каталог «Документы» уровня доступа «Уровень\_1» (Компьютер/Домашний/mac/l1i0c0x0t0x0/Документы);

- открыть файл 1.txt, проверив возможность его чтения или записи;

- выйти из ОССН.

|  |
| --- |
| Important  Для выполнения данного задания я пользовался GUI.  Перейдите по такому пути в графическом интерфейсе: Параметры -> Пользователи и группы (вниз пролистайте) -> Пользователи.  Теперь перейдем к настройке user2:   * Мин. кол-во дней между сменой пароля – 180 дней * число дней до выдачи предупреждения о смене пароля — 5 дней; * максимальный уровень — «Уровень\_3»;   Мои настройки представлены на фото ниже:    Теперь надо выйти из-под вашего пользователя, надо войти через GUI под user2, выставив параметр "Уровень конфиденциальности", равный "Уровень 1".  Note  У меня в GUI есть возможность выбора набора неиерархических категорий и уровня целостности.  Теперь попробуем создать файл 1.txt в директории Документы, используя команду, которая представлена ниже:  touch ~/Документы/1.txt  Note  У меня спокойно создался файл 1.txt.    Теперь войдите под user2 с уровнем конфиденциальности, равный "Уровень 2" через GUI. Попробуем теперь заново создать документ  touch ~/Документы/2.txt  Note  У меня система запросила пароль, после ввода спокойно создала файл.  Теперь перейдем к проверке чтения объектов.  Для просмотра содержимого директории "Документы" используйте команду, которая представлена ниже:  ls -l ~/Документы/  Note  Находясь за user2 у меня не было видно файла 1.txt, когда находился под уровнем конфидициальности "Уровень\_2", но в состоянии "Уровень\_1" все было видно.  Если файл 1.txt недоступен, то как его найти? Тут приходит на помощь магический путь, который надо использовать. В моем случае комбинация символов была другая, чем в условии задания. Команду прилагаю ниже:  ls mac/l1i0c0x3t0x0/Документы  Теперь попробуем просмотреть файл 1.txt, проверив возможность его чтения:  cat mac/l0i0c0x0t0x0/Документы/1.txt  Note  У меня считывается все нормально.  Теперь попробуем записать данные в файл, для этого используйте команду в терминале:  echo "Dlinnoe soobshenie" >> mac/l1i0c0x3t0x0/Документы/1.txt  Note  Не получилось записать в файл. |

4. Проверить наличие и возможность чтения объектов файловой

системы ОССН, владельцем которых является учётная запись пользователя

user2 на текущем уровне доступа («Уровень\_1»):

- войти в ОССН с учётной записью пользователя user2, выбрав

уровень доступа

- «Уровень\_1»;

- проверить возможность открытия каталога «Документы» для уровня

доступа «Уровень\_2» (Компьютер/Домашний/mac/l2i0c0x0t0x0/Документы);

- выйти из ОССН.

|  |
| --- |
| Important  Для выполнения данного задания я использовал GUI и приложение Konsole.  Войдите из-под GUI в user2, выставив уровень конфиденциальности равный "Уровень 1". Теперь наша задача сводится к тому, чтобы прочитать файл 2.txt, который мы создали в прошлом задании из-под user2 с уровнем конфиденциальности "Уровень\_2".  ls mac/l1i0c0x1t0x0/Документы  Note   * Адрес mac могут различаться от устройства к устройству, как я понимаю, учитывайте это. * У меня не было видно файла 2.txt, все было скрыто. |

5. Войти в ОССН с учётной записью пользователя user. Запустить

графическую утилиту «Политика безопасности». Сравнить списки вторичных

групп для учётных записей пользователей user, user1, user2, user3, user4, при

этом определив:

- учётные записи пользователей, являющиеся администраторами

(входящими в группу astra-admin);

- учётные записи пользователей, входящие в группу users.

|  |
| --- |
| Important  Для выполнения данного задания я использовал GUI в Astra Linux.  На момент версии 1.8 название поменяли, сейчас данный раздел называется "Пользователи и группы". Вам нужно идти по такому пути: Пуск -> Параметры -> Пользователи и группы (вниз пролистать надо). |

6. Создать новую учётную запись пользователя user10, при этом:

- установить минимальное количество дней между сменой пароля — 180

дней и число дней выдачи предупреждения до смены пароля — 5 дней;

- выбрать максимальный уровень доступа — «Уровень\_3»,

минимальный уровень доступа – «Уровень\_0», уровень целостности —

«Высокий»;

- добавить в список вторичных групп группы astra-admin и lpadmin;

- проверить возможность входа в ОССН с учётной записью

пользователя user10 с уровнями доступа «Уровень\_2» или «Уровень\_3»

(уровень целостности «Низкий»).

Войти в ОССН с учётной записью пользователя user10 (уровень доступа

– «Уровень\_0», уровень целостности «Высокий»). Проверить возможность

создания новой учётной записи пользователя user11 с использованием

графической утилиты fly-admin-smc без использования и с использованием

команды sudo. Выйти из ОССН.

|  |
| --- |
| Important  Для выполнения данного задания я использовал просто GUI, который есть в Astra Linux.  Перейдите по такому вот пути: Пуск -> Параметры -> Пользователи и группы -> Пользователи.  Теперь создайте пользователя в GUI, чтобы были такие параметры, которые предложены на фото ниже:    Если войти под пользователем user10 с уровнем доступа "Уровень\_2" и низким уровнем целостности, то не получится войти, вылетит экран, который представлен ниже:    Note  Если пробовать создавать пользователя из-под терминала Konsole, то он пишет, что не существует команда при обычном использовании, а с приставкой sudo пишет, что отказано в доступе.  Теперь попробуем войти под пользователем user10, выставив уровень доступа "Уровень\_0" и уровень целостности "Высокий".  Через GUI спокойно получилось создать. В случае терминала только с приставкой sudo. |

7. Войти в ОССН с учётной записью пользователя user1 с уровнем

доступа – «Уровень\_0». Осуществить попытки запуска графической утилиты

«Политика безопасности» через главное пользовательское меню и запуска её

с использованием терминала Fly командой fly-admin-smc. Проанализировать

результаты и предупреждения ОССН.

|  |
| --- |
| Для выполнения данного задания я использовал GUI.  Если пробовать войти в user1 с "Уровень\_0", то не пускает в приложения, где можно управлять группами и пользователями.  Если же пытаться использовать данную команду fly-admin-smc для запуска приложения, то выдает ошибку. Вызов через sudo также не помогает. |

8. Осуществить переключение между сеансами различных учётных

записей пользователей без выхода из ОССН:

- через меню «Завершение работы» главного пользовательского меню

перейти в подменю «Сессия» и далее «Отдельная» и войти в ОССН с учётной

записью пользователя user (уровень целостности «Высокий»);

- аналогично вернуться и далее закрыть сеанс от имени учётной записи

пользователя user1.

|  |
| --- |
| Для выполнения данного задания я использовал GUI. Описанный ниже алгоритм работает точно для Astra 1.8  Чтобы переключиться без выхода все выполнияем в следующей последовательности:   1. Нажимаем на кнопку "Пуск" (ЛКМ по звезде внизу или кнопка Win). 2. Нажимаем через ЛКМ аватар нашего пользователя. 3. Нажимаем на "Новый сеанс в окне" |

9. С использованием графической утилиты «Политика безопасности»

заблокировать пароль учётной записи пользователя user1. Проверить

изменения файлов /etc/passwd и /etc/shadow, осуществив следующие действия:

- в терминале Fly выполнить команды sudo cat /etc/passwd и sudo cat

/etc/shadow;

- проверить наличие блокировки учётной записи пользователя по файлу

/etc/shadow (должен быть установлен знак «!» в начале свёртки пароля);

- проверить функционирование блокировки путём осуществления

попытки входа в ОССН в отдельном сеансе от имени учётной записи

пользователя user1;

- снять блокировку (выполнить удаление пароля и блокировки входа,

задать повторно пароль) и проверить возможность входа в ОССН с учётной

записью пользователя user1.

|  |
| --- |
| Для выполнения данного задания я буду использовать GUI и терминал Konsole.  Я не нашел возможности заблокировать пользователя через GUI. Выставив актуальность аккаунта на дату вчера не дало результата. Попробую заблокировать пользователя, используя Konsole.  sudo passwd -l user1  Note  Вы можете установить пустой пароль для пользователя, что также заблокирует его.  В файле /etc/passwd ничего не поменялось, у меня вывод был такой, используя команду cat /etc/passwd | grep user1:  user1:x:1004:1006:,,,:/home/user1:/bin/sh  В файле /etc/shadow поменялось, у меня вывод был такой, используя команду sudo cat /etc/shadow | grep user1:  user1:!$gost12512hash$gdu79Vbx75gfovWd$DGBCQPQjrSkj3fF4aM912by76l35pPtnonDWBME3z5cLFpGKkfZ9t7dJsnr23uNc4o50lETjWQAGf4y/yV00S1:20144::99999:7:::  Note  Эта команда добавляет символ ! перед хешем пароля в файле /etc/shadow, что делает невозможным вход в систему.  Теперь снимем блокировку, используя команду, которая представлена ниже:  sudo passwd -u user1  Теперь попробуйте войти под пользователя user1 в GUI. |

10. Выполнить удаление учётных записей пользователей:

- удалить учётную запись пользователя user10 с использованием

графической утилиты «Политика безопасности»;

- удалить учётную запись пользователя user2 командой sudo deluser

user2;

- удалить учётную запись пользователя user1 командой sudo userdel

user1;

- проверить наличие домашних каталогов учётных записей пользователей user1 и user2, после чего с использованием справочной

информации по команде userdel определить её параметры, позволяющие

удалять содержимое домашнего каталога учётной записи пользователя;

- удалить домашние каталоги учётных записей пользователей user1 и

user2 непосредственно командами rm -r /home/userone и rm -r /home/usertwo,

осуществив попытки удаления без использования и с использованием

команды sudo;

- проверить наличие домашних каталогов учётных записей пользователей user1, user2 и user10 в каталоге /home/.pdp.

|  |
| --- |
| Для выполнения данного задания я использовал и GUI, и терминал, который открывается через Konsole.  Давайте в начале удалим user10, используя GUI. Проделайте алгоритм, который предложен: Пуск -> Параметры -> Пользователи и группы -> Пользователи. Далее слева будет видно, как удалить пользователя.  Теперь удалим user2, используя команду, которая представлена ниже:  sudo deluser user2  Note  Если хочется удалить с домашней директорией, то используйте это sudo deluser --remove-home user2  Теперь удалим user1, используя команду, которая представлена ниже:  sudo userdel user1  Note  Чтобы удалить и домашний каталог, используйте опцию -r  Теперь попробуем удалить домашние директории user1, как было сказано в задании:  sudo rm -r /home/user1  Теперь попробуем удалить домашниюю директорию user2, как было указано в задании:  sudo rm -r /home/user2  Note  Без sudo не получилось удалить вообще у меня.  Проверить существование домашних каталогов можно, используя команду ниже:  ls /home/.pdp |

11. Создать новые группу group3 (с использованием графической

утилиты «Политика безопасности») и группу group4 (командой sudo addgroup

group4, выполненной в терминале Fly).

|  |
| --- |
| Для выполнения данного задания я использовал и GUI, и Konsole.  Для создания группы через GUI выполните такую последовательность действий: Пуск -> Параметры -> Пользователи и группы -> Группы.    Теперь для добавления группы group4 через консоль используйте команду ниже:  sudo addgroup group4 |

12. Добавить учётную запись пользователя user3 во вторичную группу

group3 командой usermod -a -G group3 user3 и во вторичную группу group4 с

помощью графической утилиты «Политика безопасности». Проверить

включение учётной записи пользователя user3 в группы group3 и group4 путем

просмотра содержимого файла /etc/group командами cat /etc/group | grep

"^group3" и cat /etc/group | grep "^group4"

|  |
| --- |
| Important  Для выполнения данного задания я использовал и GUI, и Konsole.  Попробуем добавить пользователя user3 во вторичную группу group3, используя команду, которая представлена ниже:  sudo usermod -a -G group3 user3    Теперь для добавления в group4 через графическую утилиту выполните данный алгоритм: Пуск -> Параметры -> Пользователи и группы -> Пользователи. Дальше у вас будет раздел с группами для установки. Выполните то же самое, что представлено на фото ниже.    Остается только применить изменения и все.  Теперь просмотрим изменения для файла /etc/group для group3, используя команду ниже:  cat /etc/group | grep "^group3"  Note  У меня в выводе было такое: group3:x:1023:user3  Теперь просмотрим изменения для файла /etc/group для group4, используя коианду ниже:  cat /etc/group | grep "^group4" |

13. Выполнить удаление учётной записи пользователя user3 из группы

group3 с использованием графической утилиты «Политика безопасности» и из

группы group4 командой gpasswd -d user3 group4.\

|  |
| --- |
| Для выполнения данного задания я буду использовать и GUI, и терминал, который открывается через приложение Konsole.  Для удаления пользователя user3 из группы group3 с помощью GUI на Astra 1.8 выполните следующий порядок действий: Пуск -> Параметры -> Пользователи и группы (вниз пролистать) -> Пользователи. Теперь у вас откроется такое окно, здесь дальнейшие действия очевидны.  Для удаления user3 из группы group4 из-под терминала используйте команду, которая представлена ниже:  sudo gpasswd -d user3 group4 |

14. Удалить группу group3 командой sudo delgroup group3 в терминале

Fly и группу group4 с помощью графической утилиты «Политика

безопасности».

|  |
| --- |
| Important  Для выполнения данного задания я буду пользоваться и GUI, и терминалом, который открывается в приложении Konsole.  В Astra 1.8 уже нет приложения политика безопасности, уже здесь действия по-другому. Открываем приложение по данному алгоритму: Пуск -> Параметры -> Пользователи и группы -> Группы. Там дальше нажимаете group4 и снизу удалить.  Теперь перейдем к удалению с помощью терминала, для этого выполните команду, которая представлена ниже:  sudo delgroup group3 |

15. Изучить порядок хранения параметров мандатного управления

доступом и мандатного контроля целостности для учётных записей

пользователей. Для этого выполнить следующие действия:

- определить уровни доступа, заданные в ОССН, для этого вывести в

терминал Fly содержимое файла /etc/parsec/mac\_levels;

- определить неиерархические категории, заданные в ОССН, для этого

вывести в

терминал Fly содержимое файла /etc/parsec/mac\_categories;

- определить идентификатор учётной записи пользователя user1 по

файлу /etc/passwd командой cat /etc/passwd | grep "^user1:" | cut -d : -f 3;

- считать параметры мандатного управления доступом и мандатного

контроля целостности для учётной записи пользователя user1 командой cat

/etc/parsec/macdb/$(cat /etc/passwd | grep "^user1:" | cut -d : -f 3) и проверить их

соответствие данным, отображаемым в графической утилите «Политика

безопасности».

|  |
| --- |
| Important  Для выполнения данного задания я буду пользоваться и GUI, и терминалом, который открывается через приложение Konsole.  Чтобы определить уровни доступа, нам нужно увидеть содержимое файла /etc/parsec/mac\_levels:  cat /etc/parsec/mac\_levels    Теперь определим неиерархические категории. Для этого нужно вывести в терминал содержимое файла /etc/parsec/mac\_categories:  cat /etc/parsec/mac\_categories    Для определения идентификатора учетной записи user1 буду использовать команду, которая представлена ниже:  cat /etc/passwd | grep "^user1:" | cut -d : -f 3    Теперь считаем параметры мандатного управления доступом и мандатного контроля целостности для user1, используя команду, которая представлена ниже:  cat /etc/parsec/macdb/$(cat /etc/passwd | grep "^user1:" | cut -d : -f 3) |

2 Настройка параметров мандатного управления доступом и

мандатного контроля целостности

1.

Войти в ОССН в графическом режиме с учётной записью

пользователя user (уровень доступа — 0, неиерархические категории — нет,

уровень целостности — «Высокий»).

Запустить графическую утилиту редактирования учётных записей

пользователей «Политика безопасности» через меню «Панель управления»

главного пользовательского меню.

Модифицировать параметры мандатного управления доступом, для

этого осуществить следующие действия:

-открыть раздел «Мандатные атрибуты», «Уровни конфиденциальности» и выбрать «0»:Уровень\_0» и переименовать данный

уровень доступа: «Уровень0»;

- выполнить создание уровня доступа с именем «Уровень\_4», задав

значение равное 4, после чего проверить наличие записи «Уровень\_4» в списке

«Уровни конфиденциальности»;

-выполнить обратное переименование: «Уровень0» в «Уровень\_0».

|  |
| --- |
| Important  Для выполнения данного задания я буду пользоваться GUI. Я выполняю работу на Astra 1.8.  Для начала войдите в систему из-под user.  Теперь из-под GUI выполните такой алгоритм: Пуск -> Параметры -> Управление доступом -> Мандатное управление доступом. Теперь откройте аутентифицируйтесь. Снизу будет кнопка для изменения уровней. У вас появится такое же окно, как у меня на фото ниже:    Для создания "Уровень\_4" внизу нажмите на плюсик. Теперь можете переименовать обратно в "Уровень\_0" по алгоритму, который представлен выше был. |

2. Создать учётную запись пользователя user1, установив максимальный

Уровень доступа: «Уровень\_4».

|  |
| --- |
| Important  Для выполнения данного задания я использовал GUI.  Для создания пользователя можете использовать следующий алгоритм: Пуск -> Параметры -> Пользователи и группы -> Пользователи. После этого выполните все, как показано на фото ниже: |

3. Выполнить удаление уровня доступа 4 из раздела «Уровни

конфиденциальности»

путём выбора в контекстном меню пункта «Удалить».

|  |
| --- |
| Important  Для выполнения данного задания я использовал GUI в Astra 1.8.  Перейдите по такому пути: Пуск -> Параметры -> Управление доступом -> Мандатное управление доступом. Теперь здесь вам нужно будет удалить уровень 4, нажам на кнопочку минус. |

4. Открыть учётную запись пользователя user1 и в вкладке «МРД» в

элементе «Максимальный уровень» проверить отсутствие записи имени

уровня, при этом, в списке выбора уровня «Уровень\_4» также будет

отсутствовать.

|  |
| --- |
| Important  Для выполнения данного задания я использовал GUI.  Теперь перейдите по такой последовательности: Пуск -> Параметры -> Пользователи и группы -> Пользователи.  У меня первоначально было такое: |

5. Вывести в терминал Fly параметры мандатного управления доступом

для учётной записи пользователя user1. Для этого выполнить следующие

действия:

-запустить терминал Fly и перейти в каталог /etc/parsec/macdb;

-прочитать параметры учётной записи user1 командой sudo grep

“^user1:” \*;

-определить максимальный уровень доступа учётной записи user1

командой sudo

grep “user1:” \* | cut -d : -f 5;

-определить минимальный уровень доступа учётной записи user1

командой sudo

grep “user1” \* | cut -d : -f 3 и проверить его соответствие данным,

отображаемым в графической утилите «Политика безопасности».

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Попробуем теперь вывести параметры мандатного управления для user1. В начале перейдите в нужную директорию, используя команду, которая представлена ниже:  cd /etc/parsec/macdb  Теперь просмотрим содержимое всех файлов в данной директории, фильтруя записи, где есть user1.  sudo grep "^user1:" \*  Note  У меня вывелись такие параметры: 1005:user1:0:2:4:3  Что за магические параметры?  Запись 1005:user1:0:2:4:3 представляет собой параметры учетной записи пользователя user1, которые могут быть связаны с мандатным управлением доступом (MAC) или другими системами управления доступом. Давайте разберем каждую часть этой записи:   * 1005: Это, скорее всего, UID (идентификатор пользователя) для user1. UID — это уникальный числовой идентификатор, который используется системой для идентификации пользователя. * user1: Это имя учетной записи пользователя. * 0: Это может быть минимальный уровень доступа (или привилегий) для пользователя. В контексте мандатного управления доступом это может означать, что пользователь имеет доступ к объектам с минимальным уровнем безопасности 0. * 2: Это может быть максимальный уровень доступа для пользователя. В контексте мандатного управления доступом это может означать, что пользователь может получать доступ к объектам с максимальным уровнем безопасности 2. * 4: Это может быть уровень доступа к объектам, которые пользователь может создавать или изменять. В некоторых системах это может быть уровень, который указывает на дополнительные права или ограничения. * 3: Это может быть дополнительный параметр, который может указывать на другие настройки или права доступа, специфичные для вашей системы.   Теперь определим максимальный уровень доступа user1, используя команду, которая представлена ниже:  sudo grep "user1:" \* | cut -d : -f 5  Note  Самое, что интересное после удаления "Уровень\_4" у пользователя user1 вывело 4.  Теперь для вывода минимального уровня используйте команду, которая представлена ниже:  sudo grep "user1:" \* | cut -d : -f 3    Какой вывод у меня был в графическом интерфейсе: |

6. Создать неиерархические категории с использованием графической

утилиты «Политика безопасности». Для этого выполнить следующие

действия:

-в разделе «Категории» удалить исходные неиерархические категории;

- создать новую неиерархическую категорию с именем «Otdel1»,

«Разряд» –0;

-в разделе «Категории» создать новые неиерархические категории:

«Otdel2» («Разряд» – 1), «Upravlenie» («Разряд» – 2).

|  |
| --- |
| Important   * Для выполнения данного задания я буду пользоваться GUI. * В Astra 1.8 нет графической утилиты "Политика безопасности".   Проделайте описанный алгоритм, чтобы попасть в нужное окно: Пуск -> Параметры -> Управление доступом -> Мандатное управление доступом.  Для удаления нажимаем на категорию, а потом нажимаем на значок, где есть минус снизу. Все видно на фото, которое представлено ниже:    Для добавления новой категории нужно нажать на значок, где есть плюсик. Дальше я думаю вы сами разберетесь по условию задания. Должно получится то же самое, что представлено на фото снизу: |

7. Изменить набор неиерархических категорий с использованием

графической утилиты «Политика безопасности», для этого выполнить

следующие действия в разделе «Категории»:

-выбрать неиерархическую категорию «Otdel1» и ввести наименование

«Отдел\_1»;

-аналогично переименовать неиерархические категории «Otdel2» и

«Upravlenie» в «Отдел\_2» и «Управление», соответственно;

-проанализировать возможность одновременного изменения элемента

«Разряд».

|  |
| --- |
| Important  Для выполнения данного задания я использовал GUI.  Два раза нажимаем ЛКМ на категорию, после этого у вас получится переименовать категорию. Должно получится то же самое, что представлено на фото ниже:    Сменить параметр "Разряд" не дает на версии 1.8: |

8. Изменить мандатный уровень доступа с использованием графической

утилиты «Политика безопасности», для этого выполнить следующие

действия:

-создать новую группу с именем «office1» и задать первичную группу

учётной записи пользователя user1 — «office1»;

-создать новую учётную запись пользователя user2 и установить её

первичную группу — «office1»;

-во вкладке «Дополнительные» осуществить попытку выбора минимального набора неиерархических категорий — «Отдел\_2», И проанализировать результат;

- во вкладке «Дополнительные» выбрать максимальный уровень доступа

— «Уровень\_3», максимальный набор неиерархических категорий —

«Отдел\_2», после чего задать минимальный набор неиерархических категорий

— «Отдел\_2»;

-открыть параметры учётной записи пользователя user1 и выбрать Максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_1», минимальный набор неиерархических категорий — «Отдел\_1»;

- создать учётную запись пользователя rukoffice1 и задать первичную

группу: «office1»;

-во вкладке «Дополнительные» выбрать максимальный уровень:

«Уровень\_3», максимальный набор категорий: «Отдел\_1», «Отдел\_2»,

«Управление».

|  |
| --- |
| Important   * Для выполнения данного задания я пользовался GUI. * Данный гайд актуален на версию Astra 1.8.   Теперь переходим по такому вот пути: Пуск -> Параметры -> Пользователи и группы -> Группы. Вам нужно будет создать группу с именем office1. Сразу там можете вписать какие пользователи входят в группу. У вас должно получится то же самое, как на фото, которое представлено ниже:    Теперь, находясь за user2 попробуйте выставить параметр "Уровень конфиденциальности". То же самое сделайте и для user1. В результате проделанных махинаций у меня такое получилось, как на фото ниже:      Теперь нужно создать пользователя. Для этого делаем: Пуск -> Параметры -> Пользователи и группы -> Пользователи. Там нажимаем на кнопку "Добавить", после этого сможете спокойно создать пользователя. Результат представлен на фото ниже: |

9. Создать общий каталог для работы от имени учётных записей

пользователей user1, user2, rukoffice1 в каталоге /home/work. При этом, для

работы от имени учётных записей пользователей с наборами неиерархическими категорий равными «Отдел\_1», «Отдел\_2» и «Управление»

выделить отдельные каталоги «otdel1», «otdel2» и «upr», соответственно. При

этом обеспечить хранение файлов с различными уровнями конфиденциальности в каталогах с использованием специального атрибута

CCNR, для чего осуществить следующие действия:

-запустить терминал Fly в «привилегированном» режиме командой sudo

fly-term;

-создать каталог work и задать параметры мандатного и дискреционного

управления доступом командами:

mkdir /home/work

chown user:office1 /home/work

chmod 750 /home/work

pdpl-file 3:0:Отдел\_1,Отдел\_2,Управление:ccnr /home/work

-создать каталог для работы от имени учётных записей пользователей с

набором неиерархических категорий равным «Отдел\_1» и задать параметры

мандатного и дискреционного управления доступом командами:

user1:office1 otdel1

chmod 770 otdel1

pdpl-file 3:0:Отдел\_1:ccnr otdel1

-создать каталог для работы от имени учётных записей пользователей с

набором

неиерархических категорий равным «Отдел\_2» и задать параметры

мандатного и

дискреционного управления доступом командами:

user2:office1 otdel2

Дать права: владелец – чтение, запись, выполнение; группа – чтение,

запись, выполнение; остальные - ничего не делать.

pdpl-file 3:0:Отдел\_2:ccnr otdel2

-создать каталог upr для работы от имени учётных записей

пользователей с набором неиерархических категорий равным «Управление»

командами:

rukoffice1:office1 upr

Дать права: владелец – чтение, запись, выполнение; группа – чтение,

запись, выполнение; остальные

- ничего не делать.pdpl-file 3:0:Управление:ccnr upr

-создать вложенные каталоги У1, У2, У3 в каталогах otdel1, otdel2, upr

-установить для каталогов otdel1, otdel2, upr необходимые уровни (см.

команды для каталога upr):

pdpl-file 1:0:Управление:0 /home/work/upr/У1

pdpl-file 2:0:Управление:0 /home/work/upr/У2

pdpl-file 3:0:Управление:0 /home/work/upr/У3

chown rukoffice1:office1 upr/У{1,2,3}

chmod 770 upr/У{1,2,3}

|  |
| --- |
| Important  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole, а также терминал, который открывается через комбинацию CTRL + ALT + F<number>, где number - это число от 1 до 6.  Создадим общую директорию для пользователей, используя команду, которая представлена ниже:  sudo mkdir /home/work  Теперь поставим владельцев на данную директорию, используя команду, которая представлена ниже:  sudo chown user1:office1 /home/work  Note  Эта команда изменяет владельца каталога /home/work на пользователя user1 и группу на office1. После выполнения этой команды только user1 и пользователи, принадлежащие к группе office1, будут иметь определенные права доступа к этому каталогу, в зависимости от настроек прав доступа.  Теперь изменим права, как сказано в задании:  sudo chmod 750 /home/work  Note  Владелец каталога имеет права на чтение, запись и выполнение. Члены группы, к которой принадлежит каталог, имеют права на чтение и выполнение, но не имеют права на запись. Остальные пользователи не имеют никаких прав доступа к этому каталогу.  Теперь выполните команду, которая представлена ниже:  sudo pdpl-file 3:0:Отдел\_1,Отдел\_2,Управление:ccnr /home/work  Note  Эта команда устанавливает политику доступа для каталога /home/work, позволяя доступ к нему для указанных отделов (Отдел\_1, Отдел\_2, Управление) с заданными уровнями доступа (максимальный 3 и минимальный 0).  Дальнейшие действия советую делать из-под user1.  Теперь создаем пространство для работы наших пользователей с категорией otdel1:  sudo mkdir /home/work/otdel1  sudo chmod 770 /home/work/otdel1  sudo pdpl-file 3:0:Отдел\_1:ccnr /home/work/otdel1  Теперь создаем пространство для работы наших пользователей с уровнем otdel2:  sudo mkdir /home/work/otdel2  sudo chmod 770 /home/work/otdel2  sudo pdpl-file 3:0:Отдел\_2:ccnr /home/work/otdel2  Теперь создаем пространство для работы наших пользователей с уровнем upr:  sudo mkdir /home/work/upr  sudo chmod 770 /home/work/upr  sudo pdpl-file 3:0:Управление:ccnr /home/work/upr    Теперь нам нужно создать каталоги и установить необходимые уровни:  Для отдела 1:  sudo mkdir /home/work/otdel1/У{1,2,3}  sudo chown rukoffice1:office1 /home/work/otdel1/У{1,2,3}  sudo chmod 770 /home/work/otdel1/У{1,2,3}  sudo pdpl-file 1:0:Отдел\_1:0 /home/work/otdel1/У1  sudo pdpl-file 1:0:Отдел\_1:0 /home/work/otdel1/У2  sudo pdpl-file 1:0:Отдел\_1:0 /home/work/otdel1/У3  Для отдела 2:  sudo mkdir /home/work/otdel2/У{1,2,3}  sudo chown rukoffice1:office1 /home/work/otdel2/У{1,2,3}  sudo chmod 770 /home/work/otdel2/У{1,2,3}  sudo pdpl-file 1:0:Отдел\_2:0 /home/work/otdel2/У1  sudo pdpl-file 1:0:Отдел\_2:0 /home/work/otdel2/У2  sudo pdpl-file 1:0:Отдел\_2:0 /home/work/otdel2/У3  Для отдела "Управление":  sudo mkdir /home/work/upr/У{1,2,3}  sudo chown rukoffice1:office1 /home/work/upr/У{1,2,3}  sudo chmod 770 /home/work/upr/У{1,2,3}  sudo pdpl-file 1:0:Управление:0 /home/work/upr/У1  sudo pdpl-file 2:0:Управление:0 /home/work/upr/У2  sudo pdpl-file 3:0:Управление:0 /home/work/upr/У3    Note  sudo pdpl-file 1:0:Управление:0 /home/work/upr/У1 - эта команда устанавливает политику доступа для каталога /home/work, позволяя доступ к нему для указанных отделов (Отдел\_1, Отдел\_2, Управление) с заданными уровнями доступа (максимальный 3 и минимальный 0). |

10. Установить дискреционные права доступа с разрешением на запись

и чтение для группы office1 в графическом файловом менеджере Fly (fly-fm).

Выполнить последовательные входы в ОССН с учётной записью пользователя

user1 (неиерархическая категория — «Отдел\_1», уровни доступа 1, 2, 3). При

работе на уровнях доступа 1, 2 и 3 создать в каталоге /home/work/otdel1/уровеньX файлы с именами 11.txt, 12.txt, 13.txt,соответственно.

|  |
| --- |
| Important  Данное задание я выполнял в GUI.  Я не нашел, где для группы можно настроить разрешение на запись на чтение для определенной группы. Во fly-fm на Astra 1.8.  Войдем теперь под пользователем user1 в оболочке ОССН, задав параметры, как сказано в условии.  Уровень доступа 1  touch /home/work/otdel1/У1/11.txt  Уровень доступа 2  touch /home/work/otdel1/У2/12.txt  Уровень доступа 3  touch /home/work/otdel1/У3/13.txt  Important   * На все файлы назначить права на чтение и запись. * У меня не получилось на 2 втором и выше уровне создать файлы почему-то.   chmod 660 /home/work/otdel1/уровень\*/1\*.txt |

11. Выполнить последовательные входы в ОССН с учётной записью

пользователя user2 (неиерархическая категория — «Отдел\_2», уровни доступа

1, 2, 3). При работе на мандатных уровнях доступа 1, 2 и 3 создать в каталоге

/home/work/otdel2/уровеньX файлы с именами 21.txt, 22.txt, 23.txt,

соответственно, и установить дискреционные права доступа с разрешением на

запись и чтение для группы office1 в файловом менеджере Fly.

|  |
| --- |
| Note  Для выполнения данного задания я использовал терминал, который открывается через приложение Konsole.  Important  Учитывайте те права, которые я задал в задании 9.  Войдите под пользователем user2.  Уровень доступа 1:  touch /home/work/otdel2/У1/21.txt  chown user2:office1 /home/work/otdel2/У1/2\*.txt  chmod 660 /home/work/otdel2/У1/2\*.txt  Уровень доступа 2:  touch /home/work/otdel2/У2/22.txt  chown user2:office1 /home/work/otdel2/У2/2\*.txt  chmod 660 /home/work/otdel2/У2/2\*.txt  Уровень доступа 3:  touch /home/work/otdel2/У3/23.txt  chown user2:office1 /home/work/otdel2/У3/2\*.txt  chmod 660 /home/work/otdel2/У3/2\*.txt |

12. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень

доступа — 3, неиерархическая категория — «Отдел2») и проверить

возможность получения следующих доступов к файлам: доступ на чтение к

файлам 21.txt, 22.txt, 23.txt, доступ на запись к файлу 23.txt.

|  |
| --- |
|  |

13. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень

доступа — 2, неиерархическая категория — «Отдел\_1») и проверить

возможность получения следующих доступов к файлам: доступ на чтение к

файлам 11.txt, 12.txt, доступ на запись к файлу 12.txt.

|  |
| --- |
|  |

14. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень

доступа — 3, набор неиерархических категорий — «Отдел\_1», «Отдел\_2»,

«Управление») и проверить возможность получения доступа на чтение к

файлам 11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt.

|  |
| --- |
|  |

15. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень

доступа — 3, неиерархическая категория — «Управление»). Создать файл

u3.txt в каталоге /home/work/upr/У3.

|  |
| --- |
|  |

16. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень

доступа — 3, набор неиерархических категорий: «Отдел\_1», «Отдел\_2»,

«Управление») и проверить возможность получения следующих доступов к

файлам: доступ на запись к файлу u3.txt, доступ на чтение к файлам u3.txt,

11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt.

|  |
| --- |
|  |

17. Для доступа к терминалу Fly настроить включение учётных записей

пользователей user1, user2, rukoffice1 во вторичную группу astra-console. Это

позволит данным учётным записям пользователей запускать терминал Fly с

использованием комбинации Win+R.

|  |
| --- |
|  |

18. Вывести в терминал Fly параметры мандатного управления доступом

и мандатного контроля целостности для учётных записей пользователей. Для

этого выполнить следующие действия:

-войти в ОССН с учётной записью пользователя rukoffice1 (уровень

доступа – 2, набор неиерархических категорий: «Отдел\_1», «Управление»);

-в терминале Fly выполнить команду pdp-id -a, проанализировать

результат;

-выполнить избирательный вывод параметров мандатного управления

доступом (с числовыми значениями) командами pdp-id -l и pdp-id -c;

-выполнить избирательный вывод параметров мандатного управления

доступом (с именами) командами pdp-id -ln и pdp-id -cn.

|  |
| --- |
|  |

19. Изменить параметры мандатного управления доступом и мандатного

контроля целостности учётной записи пользователя rukoffice1. Для этого

выполнить следующие действия:

-войти в ОССН с учётной записью пользователя user (уровень доступа

— 0, неиерархические категории — нет, уровень целостности — «Высокий»)

и запустить терминал Fly в «привилегированном» режиме;

- изменить минимальный и максимальный уровни доступа учётной

записи пользователя rukoffice1 командой pdpl-user -l 0:2 rukoffice1, а также

минимальный и максимальный наборы неиерархических категорий пользователя rukoffice1 командой pdpl-user -c 0:2 rukoffice1;

- обнулить значения уровней доступа и наборов неиерархических

категорий в параметрах учётной записи пользователя rukoffice1 командой

pdpl-user -z rukoffice1;

- установить значения уровней доступа и наборов неиерархических

категорий в параметрах учётной записи пользователя rukoffice1 1:3 -c 0:7

rukoffice1.

|  |
| --- |
|  |

20. Считать параметры мандатного управления доступом и мандатного

контроля целостности учётной записи пользователя rukoffice1 из файлов

настроек. Для этого выполнить следующие действия:

-перейти в каталог /etc/parsec/macdb и считать минимальный и

максимальный уровни доступа командами grep “rukoffice1” \* | cut -d : -f 3 и

grep “rukoffice1” \* | cut -d : -f 5, соответственно;

-считать минимальный и максимальный наборы неиерархических

категорий 4 и 6, соответственно.

|  |
| --- |
|  |

21. Создать и модифицировать мандатные уровни доступа, осуществив

следующие действия:

-вывести в терминал созданные уровни доступа командой userlev и

сравнить полученные данные с настройками в утилите «Политика

безопасности»;

-добавить новый уровень доступа с именем «Уровень\_4» (значение 4)

командой userlev Уровень\_4 --add 4 и вывести в терминал уровни доступа

командой userlev;

-выполнить переименование уровня доступа «Уровень\_4» В «НовыйУровень» командой userlev;

-добавить возможность работы от имени учётной записи пользователя

rukoffice1 на уровне доступа 4;

-выполнить попытку изменения значения уровня доступа «НовыйУровень» на 3 командой userlev, проанализировать результат;

-изменить значение уровня доступа «НовыйУровень» на 5 командой

userlev и вывести в терминал максимальный уровень доступа учётной записи

пользователя rukoffice1, проанализировать результат;

-установить максимальный уровень доступа учётной записи пользователя rukoffice1 равным 5;

-удалить уровень доступа с именем «НовыйУровень» командой в

терминале и определить максимальный уровень доступа учётной записи

пользователя rukoffice1 командой в терминале, проанализировать результат;

-восстановить набор неиерархических категорий и уровней доступа

учётной записи пользователя rukoffice1 :3 -c 0:7.

|  |
| --- |
|  |

22. Создать и модифицировать неиерархические категории:

-в терминале Fly, запущенном в «привилегированном» режиме, вывести

неиерархические категории командой usercat;

-добавить новую неиерархическую категорию командой usercat;

-переименовать неиерархическую категорию «otdel3» в «Отдел\_3»

командой usercat;

-осуществить попытку модификации наборов неиерархических категорий учётной записи пользователя rukoffice1 командой pdpl-user,

проанализировать результат;

-добавить неиерархическую категорию «Отдел\_3» В наборы неиерархических категорий учётной записи пользователя rukoffice1 командой

pdpl-user, обратить внимание на то, что неиерархическая категория задаётся в шестнадцатеричном формате;

-осуществить попытку изменения значения неиерархической категории

«Отдел\_3» на значение 2 командой usercat, проанализировать результат;

-изменить значение неиерархической категории «Отдел\_3» на 0x10

командой usercat;

-изменить значение неиерархической категории «Отдел\_3» на 0x20

командой usercat, обратить внимание на то, что независимо от указания типа

числа по префиксу «0x» (десятичное или шестнадцатеричное) значение

неиерархической категории задаётся в шестнадцатеричном формате;

-удалить неиерархическую категорию «Отдел\_3» командой usercat

Отдел\_3 --delete;

-изменить значение неиерархической категории «Управление» на 0x10

командой usercat, проанализировать результат по данным, выводимым

командой pdpl-user rukoffice1;

-изменить значение неиерархической категории «Управление» на 4

командой usercat.

|  |
| --- |
|  |

23. Для настройки привилегий учётных записей пользователей

осуществить следующие действия:

-вывести в терминал заданные в ОССН привилегии учётных записей

пользователей командой usercaps, при работе в терминале Fly В «привилегированном» режиме;

-запустить графическую утилиту «Политика безопасности» и открыть

настройки учётной записи пользователя user1, в вкладке «Привилегии»

установить Linux-привилегии cap\_kill, cap\_fowner и PARSEC-привилегии

parsec\_cap\_chmac, parsec\_cap\_sig, после чего закончить работу с утилитой;

-вывести привилегии учётной записи пользователя user1 командой

usercaps user1;

-в графической утилите «Политика безопасности» открыть параметры

учётной записи пользователя user, в вкладке «Привилегии» выбрать Linux-

привилегии cap\_kill,

cap\_fowner и PARSEC-привилегии parsec\_cap\_chmac, parsec\_cap\_sig;

-запустить терминал Fly в «непривилегированном» режиме командой

fly-term и осуществить попытку запуска команды usercaps;

-определить расположение файла usercaps командой which usercaps,

выполненной из «привилегированного» режима, а затем выполнить в

«непривилегированном» режиме команду /usr/sbin/usercaps, проанализировать

результат;

-запустить терминал Fly в «привилегированном» режиме командой sudo

fly-term и выполнить модификацию Linux-привилегий и PARSEC-привилегий

командами:

usercaps -l 9 user1

usercaps -m 2 user1

usercaps -m 11 user1

-с использованием графической утилиты «Политика безопасности»

определить установленные привилегии и формат параметра модификации

привилегий учётных записей пользователей (десятичная, восьмеричная или

шестнадцатеричная система счисления при этом используется?);

-установить для учётной записи пользователя user1 полный список

привилегий командой usercaps -f user1, затем удалить все привилегии учётной

записи пользователя user1 командой usercaps -z user1;

-вывести списки Linux-привилегий и PARSEC-привилегий командами

usercaps -L и usercaps -M, соответственно.

|  |
| --- |
|  |