ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

В Г. СМОЛЕНСКЕ

Кафедра вычислительной техники

Дисциплина: ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Лабораторная работа № 2.

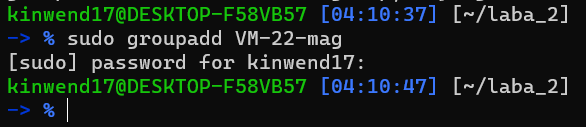
АДМИНИСТРИРОВАНИЕ ПОЛЬЗОВАТЕЛЕЙ В LINUX

|  |  |  |
| --- | --- | --- |
|  | Студент: | Старостенков А.А. |
|  | Группа: | ВМ-22 (маг.) |
|  | Вариант: | 15 |
|  | Преподаватель: | Федулов Я.А. |

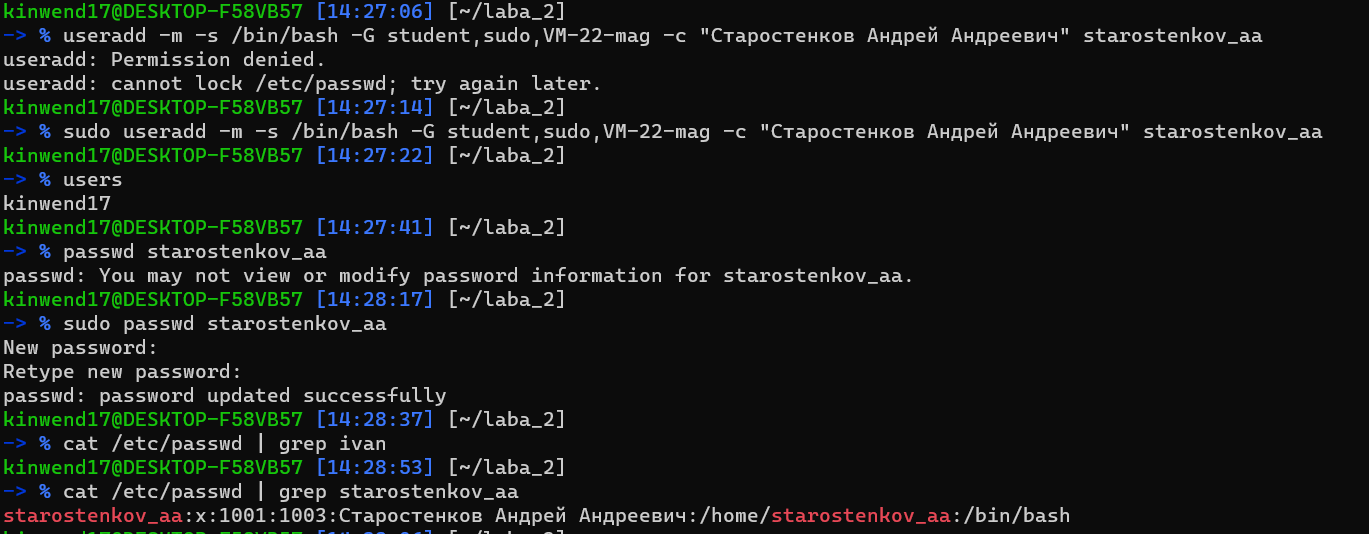
СМОЛЕНСК

2023

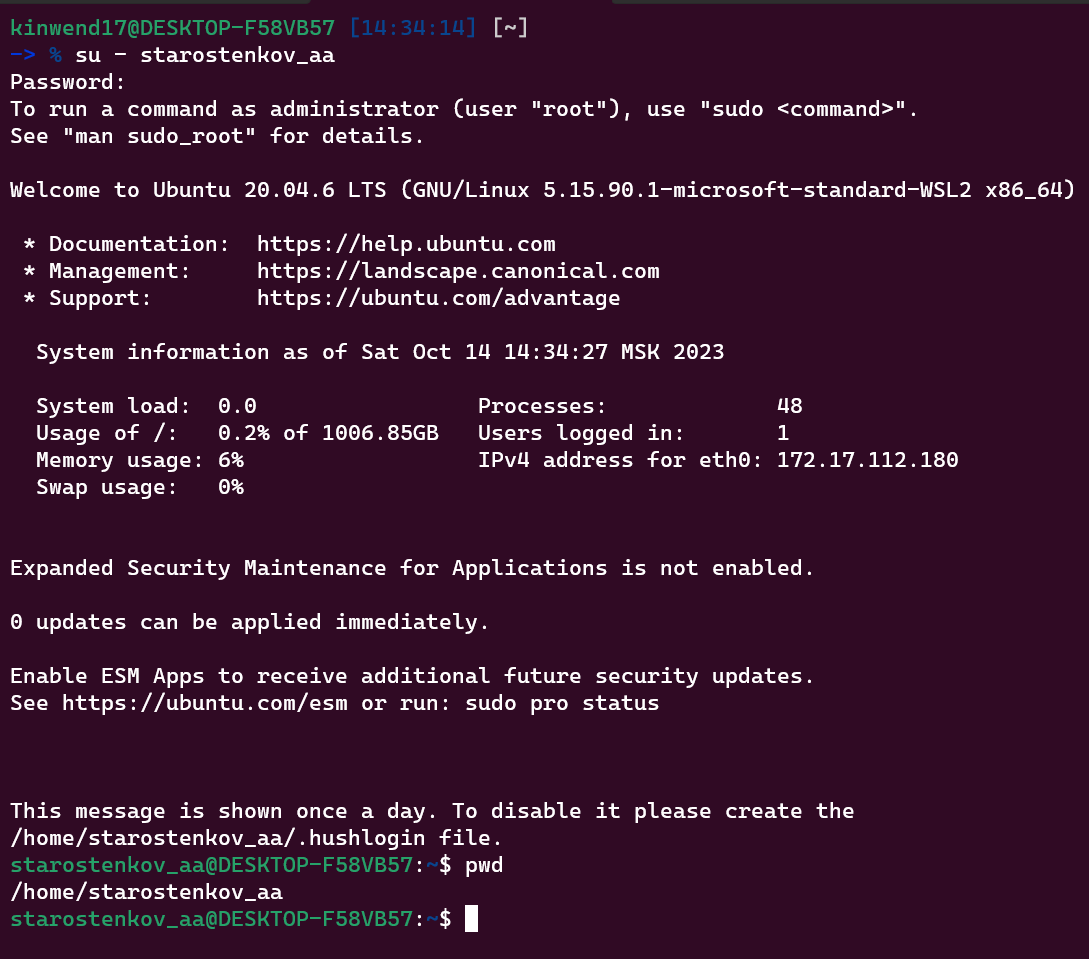
1. Создайте новую группу с именем вашей группы



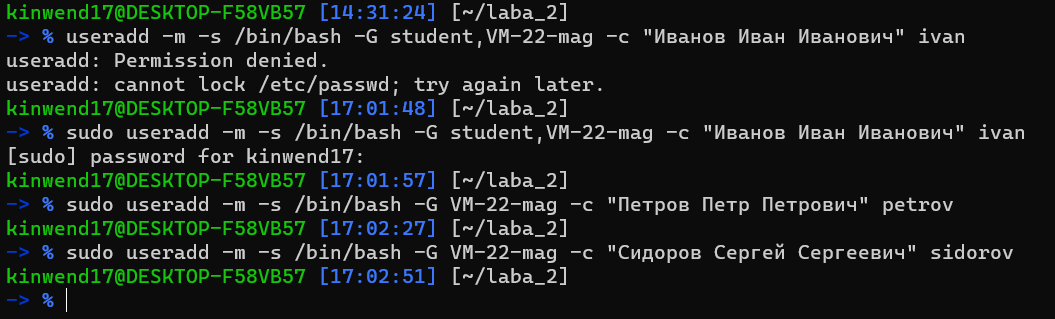
1. Создайте нового пользователя с вашей фамилией, входящего в созданную в п. 2 группу, группы student и sudo. При создании пользователя выберите оболочку /bin/bash, создайте свой домашний каталог и укажите в примечании свое полное имя (опциями команды useradd). Установите пароль для входа в систему.

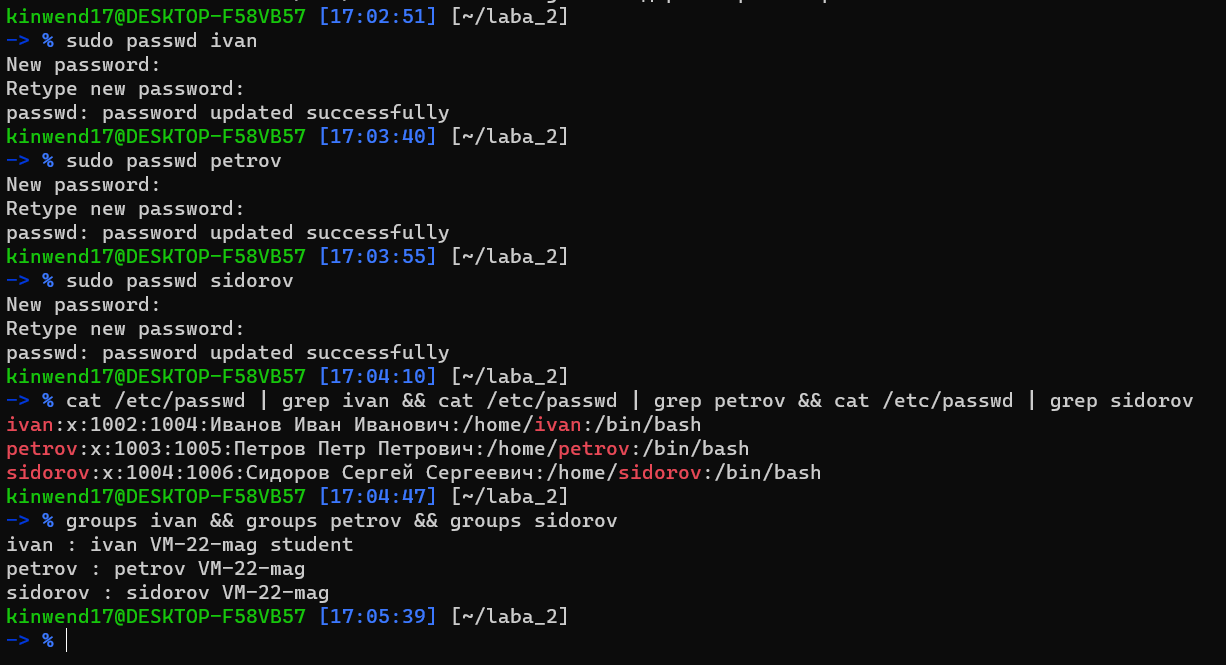


1. Войдите в терминал tty1 созданным в п. 2 пользователем.

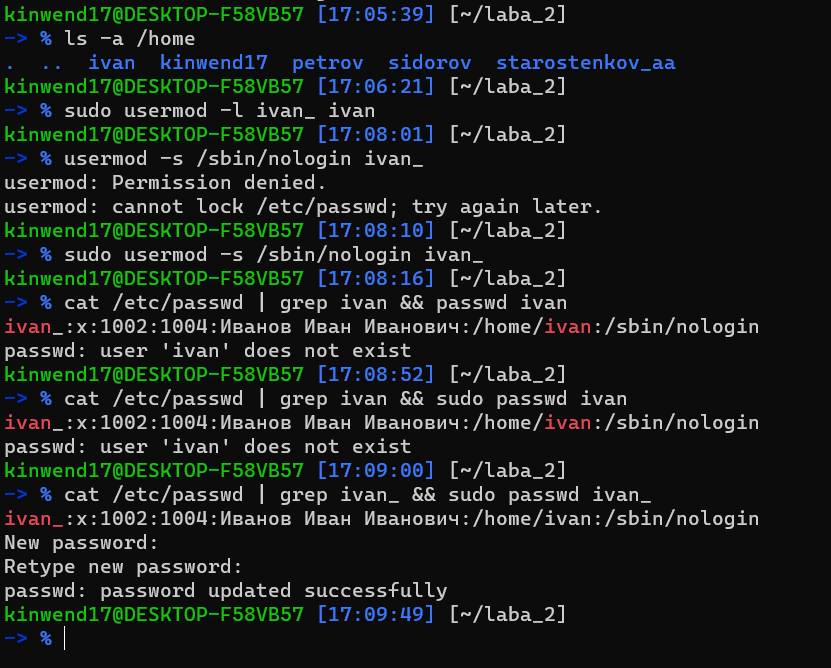


1. Создайте три новых пользователя для студентов группы. Для всех пользователей создайте свой домашний каталог, выберите оболочку /bin/bash, указав в примечании полное имя пользователя. Каждый пользователь должен входить в группу, созданную в п. 2, один пользователь должен также входить в группу student. Для каждого пользователя установите свой пароль.

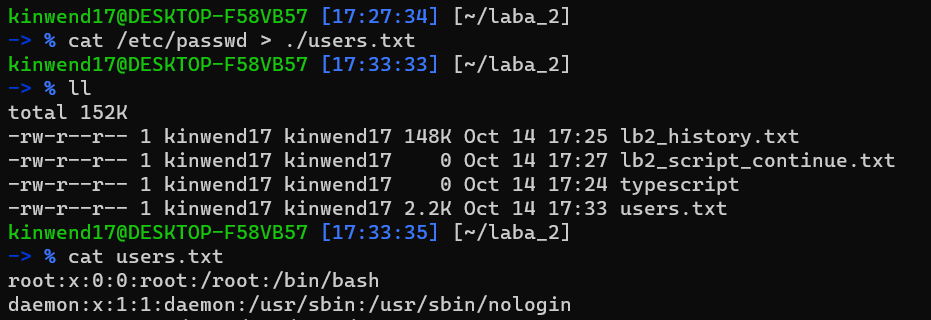




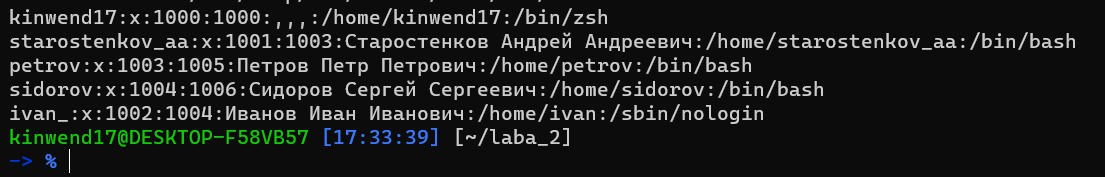
1. Переименуйте одного из пользователей <имя\_пользователя> в <имя\_пользователя>\_ (добавьте в конец символ подчеркивания \_) и установите для него командную оболочку /sbin/nologin.



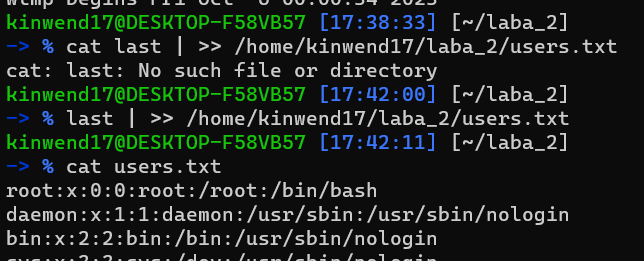
1. Соберите информацию обо всех новых пользователях в файле users.txt.



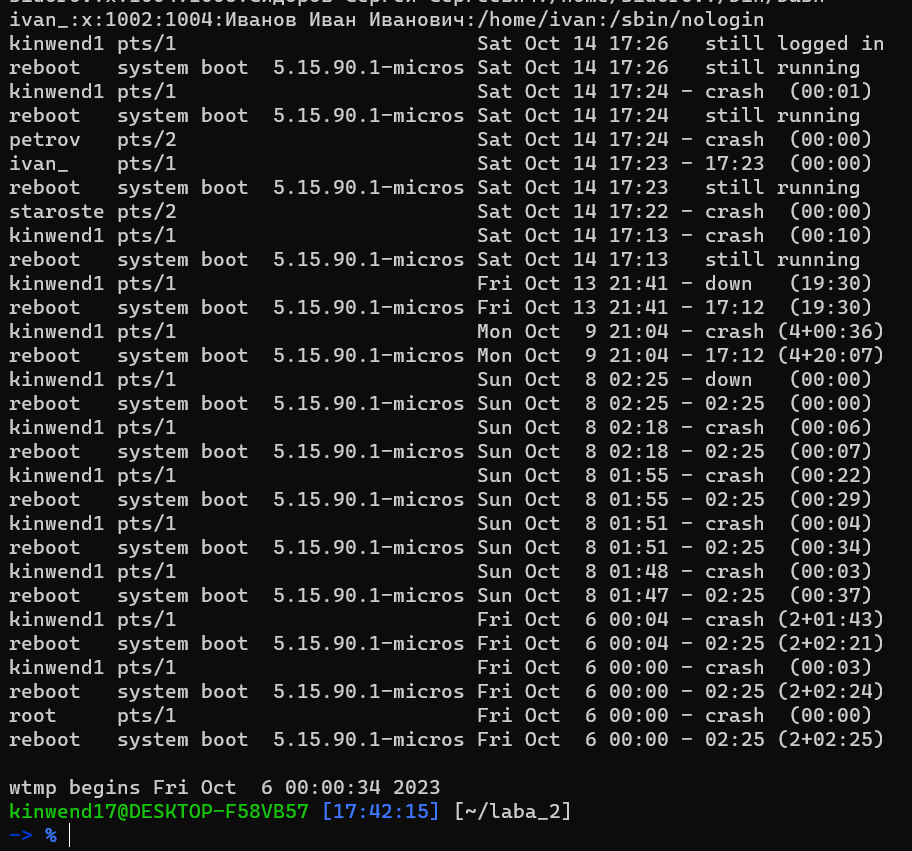
…



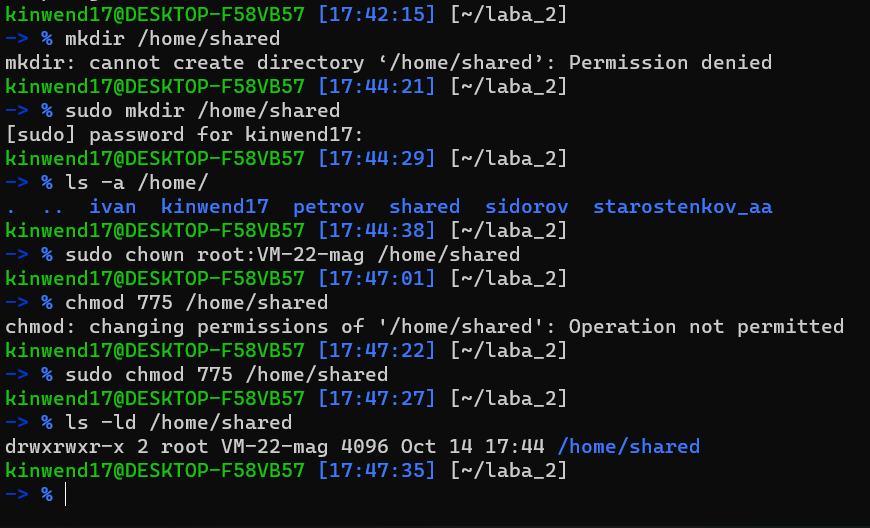
1. Дополните файл users.txt информацией о последних входах в систему (см. last).



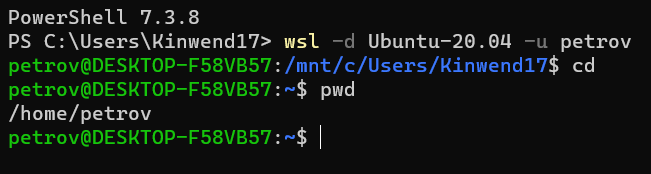
…

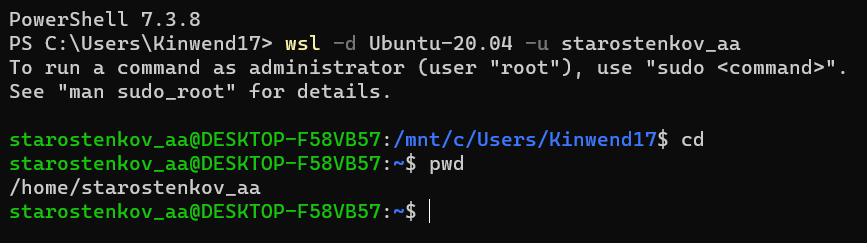


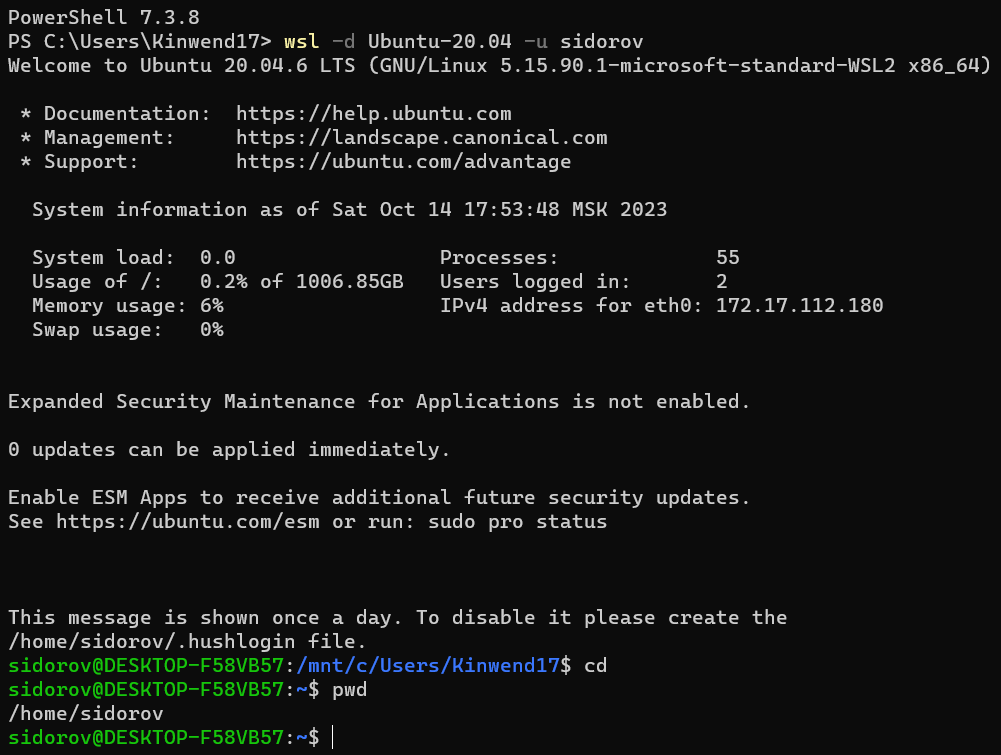
1. Создайте каталог /home/shared, доступный всем пользователям группы, созданной в п. 2.



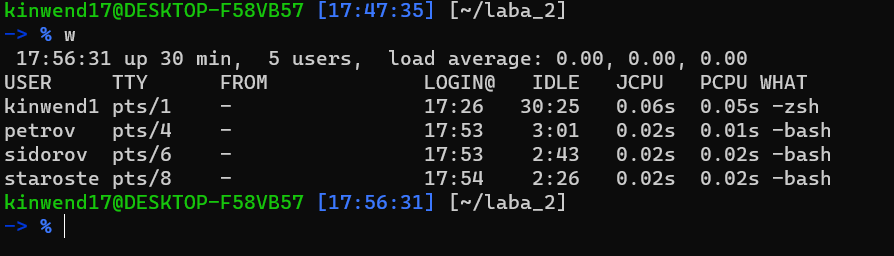
1. Войдите в систему всеми новыми пользователями и пользователем student (в терминалах tty2–tty4).



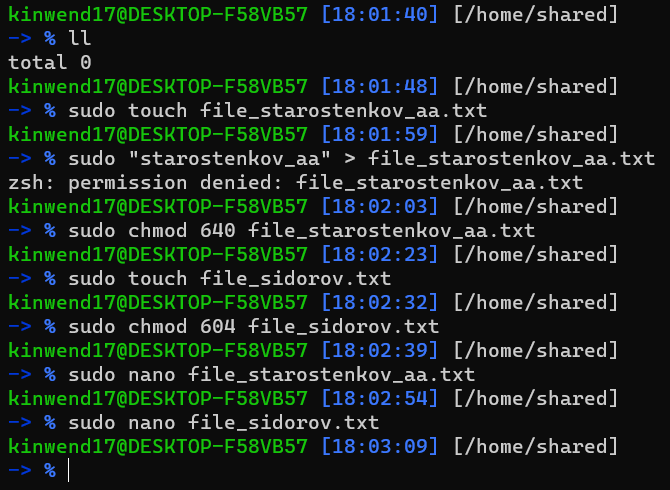




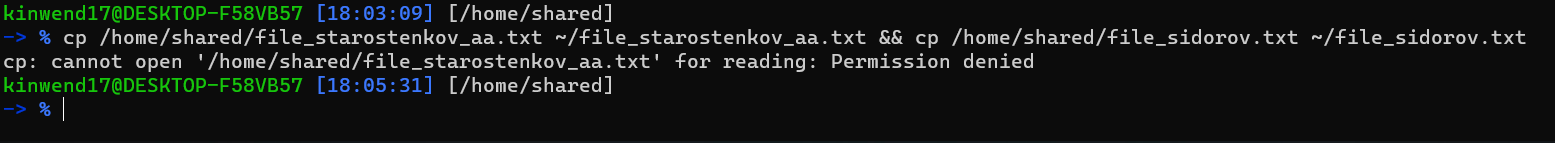
1. Получите список активных пользователей (см. w).

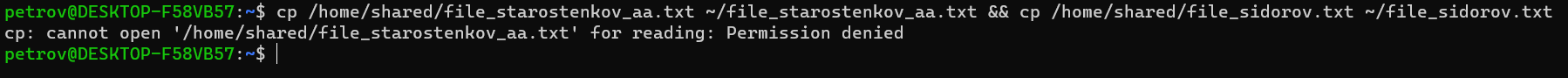


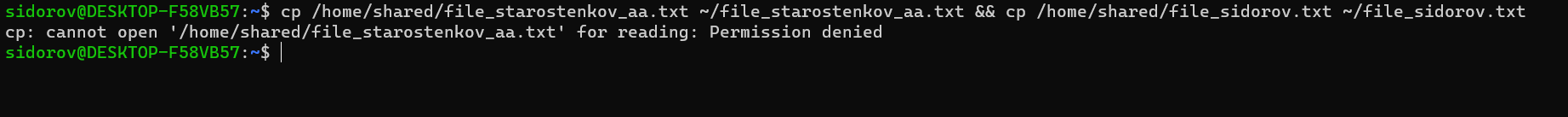
1. Создайте в каталоге /home/shared текстовые файлы file\_<имя пользователя>\_1.txt, file\_<имя пользователя>\_2.txt с правами 640 и 604 соответственно для каждого пользователя. Запишите в файлы их имена.



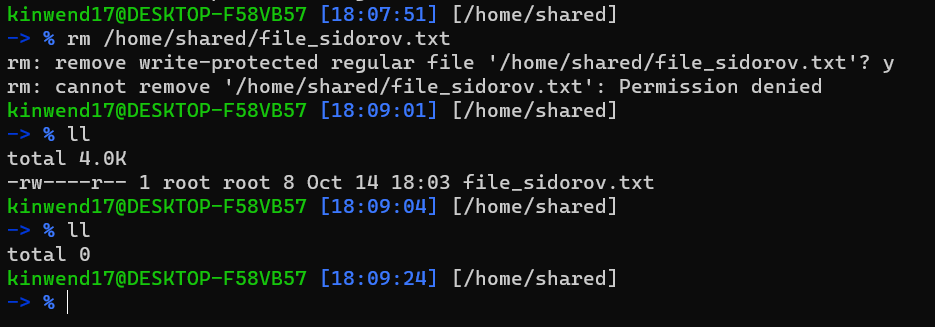
1. Убедитесь, в наличии или отсутствии возможности скопировать файлы из п.11 в свою домашнюю папку всеми пользователями (без команд su или sudo).

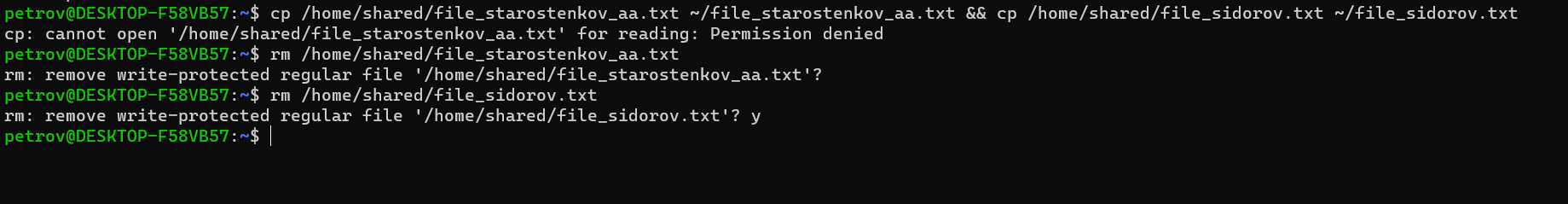


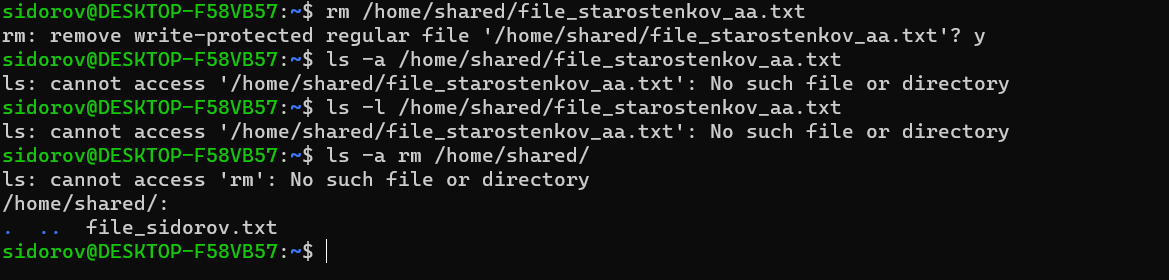




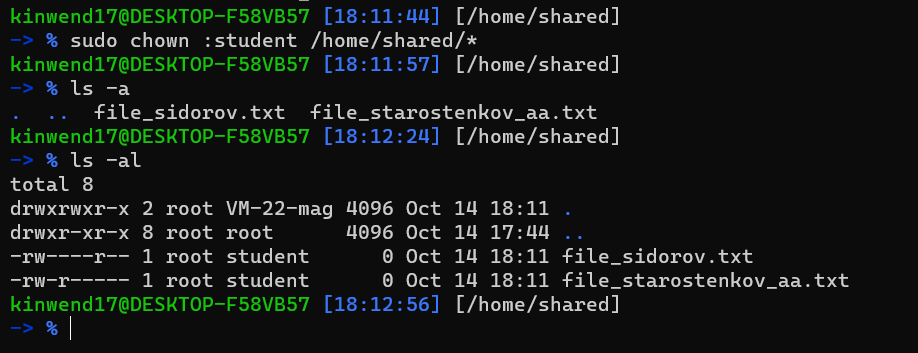
1. Попытайтесь удалить один из файлов, недоступных для чтения в п. 12. Проанализируйте результат.



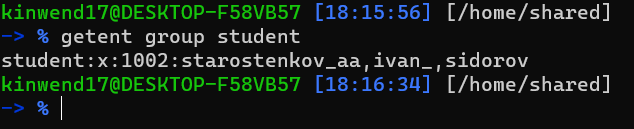


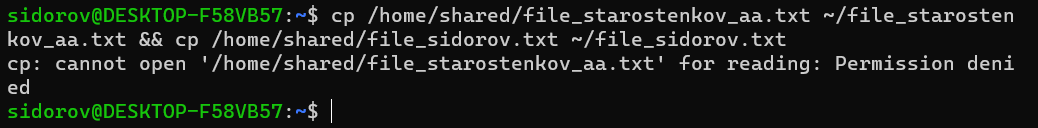


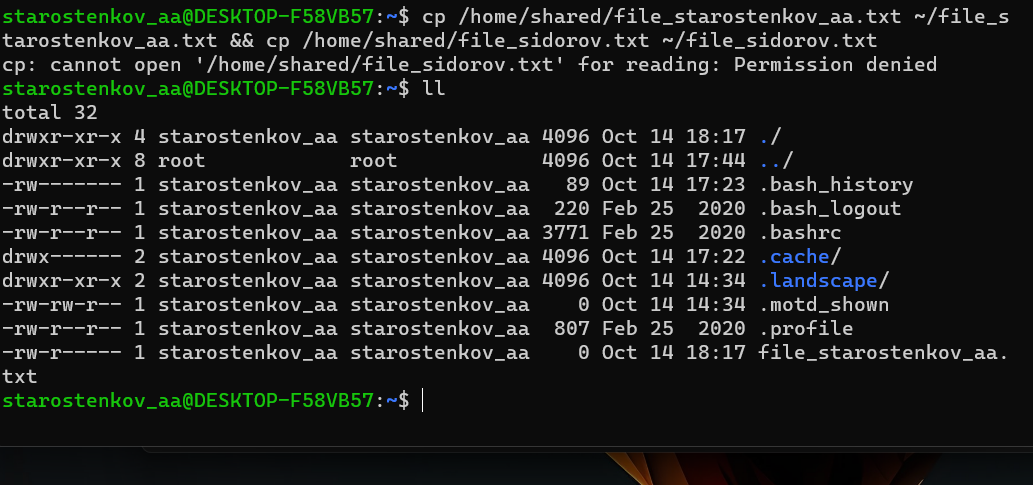
1. Измените группу-владельца всех файлов на student



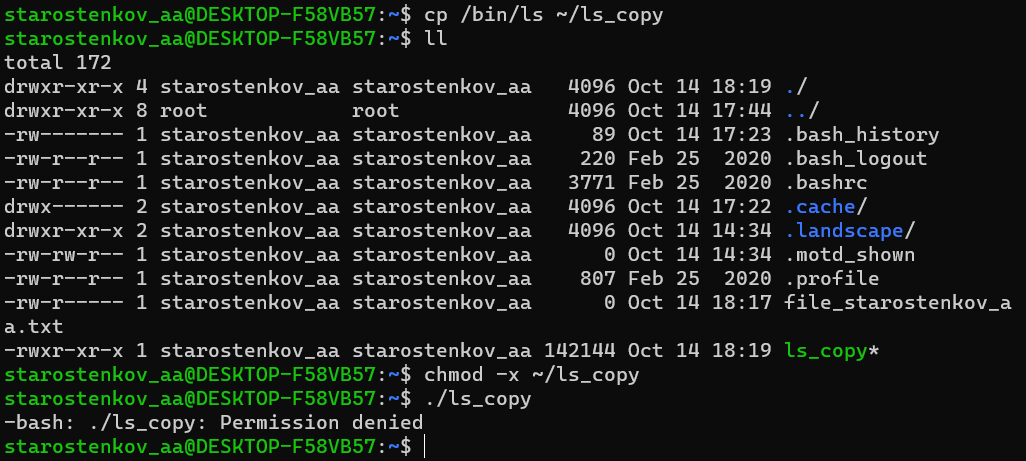
1. Проделайте п.12 пользователем student. Проанализируйте результат.



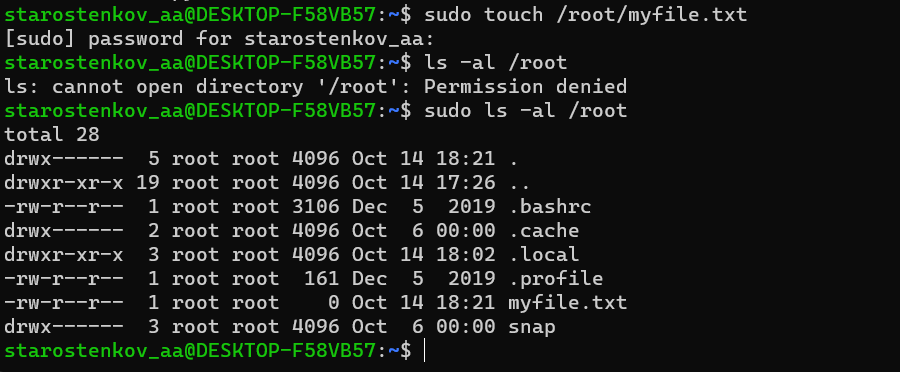




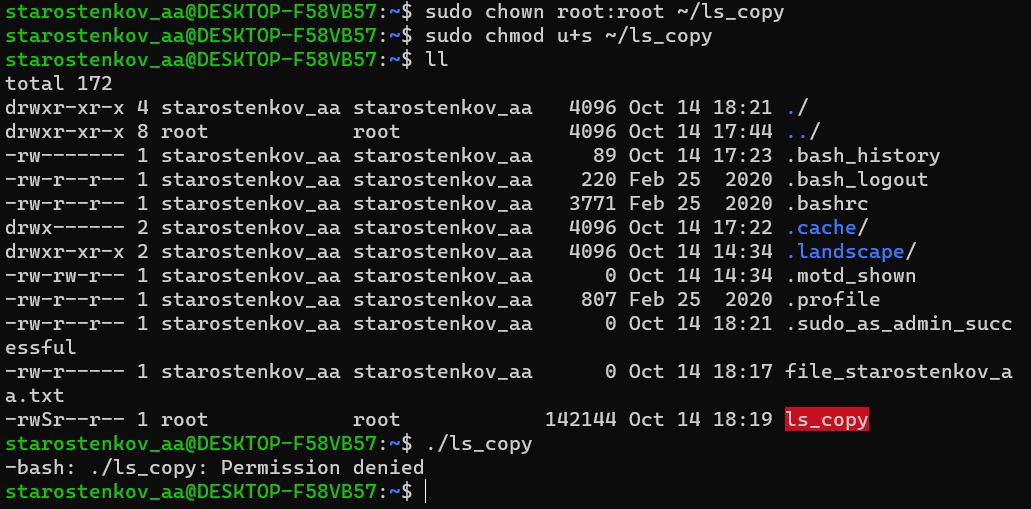
1. Скопируйте в свой домашний каталог файл /bin/ls, запретите его исполнение. Попытайтесь запустить на исполнение этот файл из домашнего каталога и проанализируйте результат.



1. Попытайтесь просмотреть содержимое домашнего каталога суперпользователя /root. Предварительно создайте в каталоге /root текстовый файл.



1. Установите файлу ~/ls (см. п. 17) пользователя-владельца суперпользователя root и бит смены идентификатора пользователя, и с его помощью проделайте п. 18. Проанализируйте результат.



***Контрольные вопросы***

1. На какие операции с файлами оказывают влияние права доступа к файлу, а на какие — права доступа к каталогу, в котором содержится указанный файл?

Права доступа к файлам оказывают влияние на операции, связанные с самим файлом, такие как чтение, запись и выполнение файла. Права доступа к каталогу влияют на операции, связанные с каталогом, такие как создание, удаление и переименование файлов внутри каталога, а также поиск файлов внутри каталога.

1. Можно ли отредактировать файлы с правами доступа 204 и 240 и каким образом?

Файлы с правами доступа 204 (например, -r--r-----) и 240 (например, -r-----r--) не могут быть отредактированы обычными пользователями, так как они не имеют прав на запись в файл. Только владелец файла или суперпользователь может изменять такие файлы.

1. Пользователь установил права доступа к файлу только на чтение — 444, но хакеру удалось отредактировать этот файл. Какие ошибки мог совершить пользователь?

Если пользователь установил права доступа на файл только на чтение (444), и хакер смог отредактировать файл, это может произойти из-за недостаточной защиты самой системы. Это может быть связано с недавно установленными уязвимостями в системе, слабыми паролями или некорректной настройкой системы. Пользователь, который установил права доступа 444, вероятно, считал, что это предотвратит любые изменения файла, но другие факторы могут позволить хакеру изменить файл.

1. Как разрешить пользователю удалять из каталога только те файлы, владельцем которых он является?

Чтобы разрешить пользователю удалять только те файлы из каталога, владельцем которых он является, вы можете установить бит SUID на каталоге. Это делается следующим образом:

chmod +t /путь/к/каталогу

После установки бита SUID, пользователь сможет удалять только свои собственные файлы из этого каталога.

1. Что такое тёмный каталог?

Тёмный каталог (Dark Directory) – это термин, который иногда используется для описания каталога, к которому пользователи не имеют доступа. Это может быть скрытый каталог или удаленный каталог, к которому нет прав доступа у текущего пользователя.

1. Как определить только с помощью команды cp в какие группы входит пользователь student?

Чтобы определить, в какие группы входит пользователь student с помощью команды cp, можно воспользоваться командой id. Например:

id student

Эта команда выведет информацию о пользователе student, включая список его групп.

1. Как суперпользователю root запретить всем пользователям самостоятельно изменять пароль?

Для того чтобы суперпользователь root запретил всем пользователям самостоятельно изменять пароль, можно установить минимальный срок действия пароля (-1) и максимальный срок действия пароля (-1) для пользователя root с помощью команды chage:

sudo chage -M -1 -m -1 root

Это запретит изменение пароля суперпользователя.

1. Как запретить вход в систему суперпользователю root?

Для запрета входа в систему суперпользователю root, можно отключить его вход через SSH или другие методы, а также установить пароль для root каким-либо неизвестным значением.

1. Как получить список всех пользователей системы?

Для получения списка всех пользователей системы, вы можете воспользоваться командой getent следующим образом:

getent passwd

1. В чем разница между командами su и sudo?

Разница между командами su и sudo заключается в том, как они позволяют пользователям получать временные привилегии суперпользователя. su (Switch User) позволяет пользователю сменить пользователя на другого, включая суперпользователя, после ввода пароля этого пользователя. sudo (Superuser Do) позволяет пользователям выполнять отдельные команды с привилегиями суперпользователя, обычно после ввода собственного пароля, а не пароля суперпользователя.