|  |  |
| --- | --- |
| **К Г Э У** | МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»**  (ФГБОУ ВО «КГЭУ») |

Отчет по лабораторной работе №5

по дисциплине «Информационная безопасность»

по теме «Администрирование пользователей и правил разграничения доступа в ОС Astra Linux»

**Выполнил:**

студент Тазеев Р.Р.

**Группа:**

ТРП-1-23

**Проверил:**

Доцент ИТИС  
Хуснутдинов Рамиль Миннегаязович

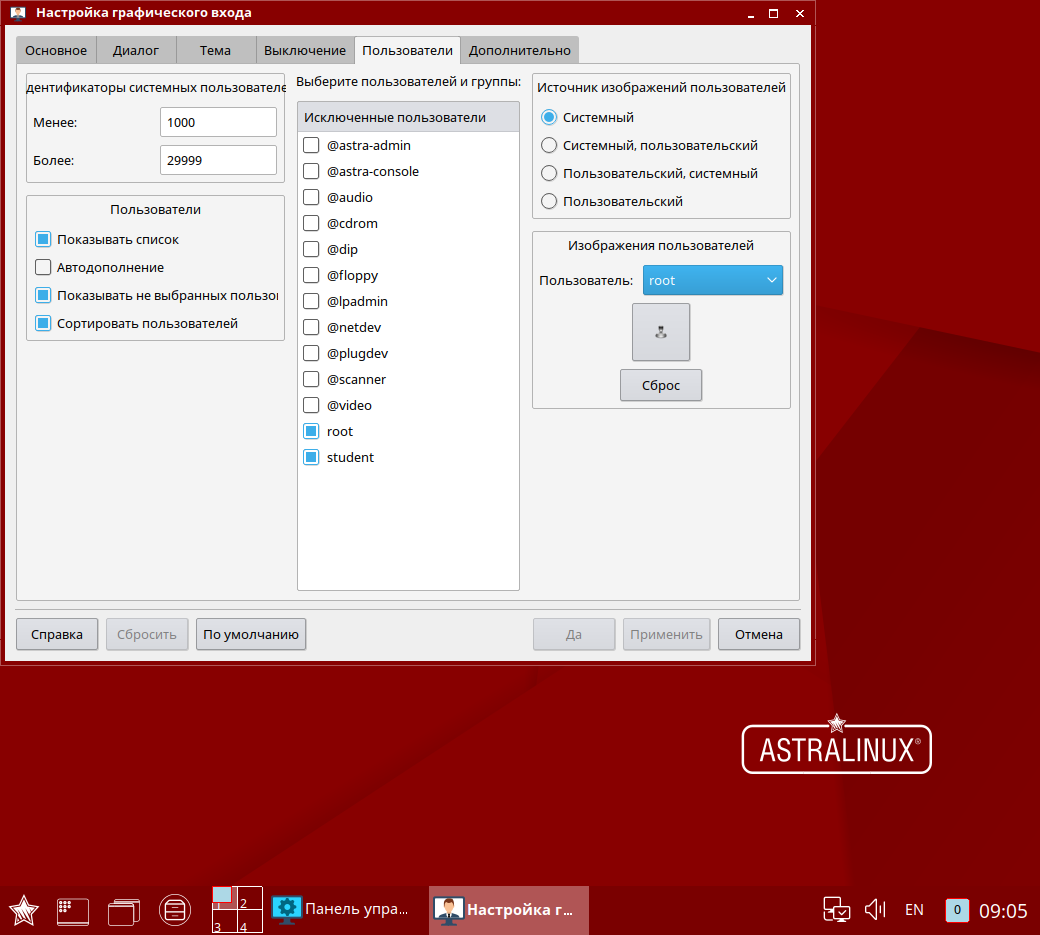
Казань, 2024 г.

Администрирование пользователей и групп

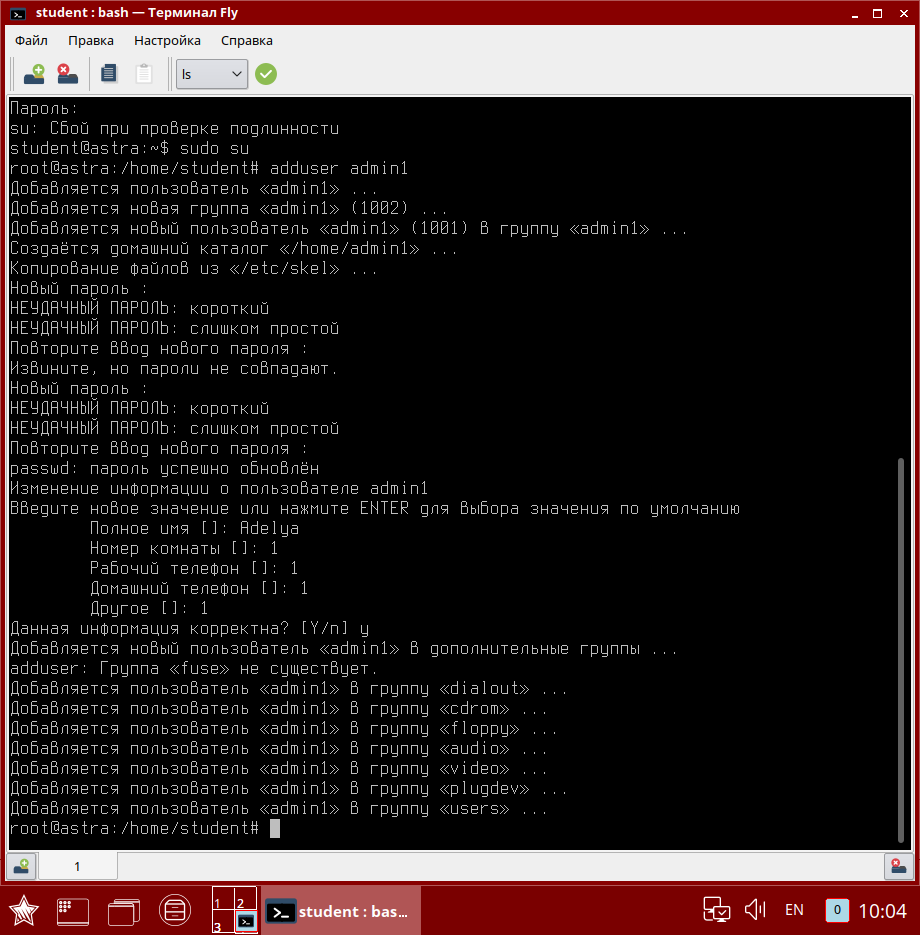
1. Скачайте образ виртуальной машины (AstraLinuxSE) по ссылке.

2. Разверните ее и войдите в систему (имя пользователя: student; пароль: Asdf1234)

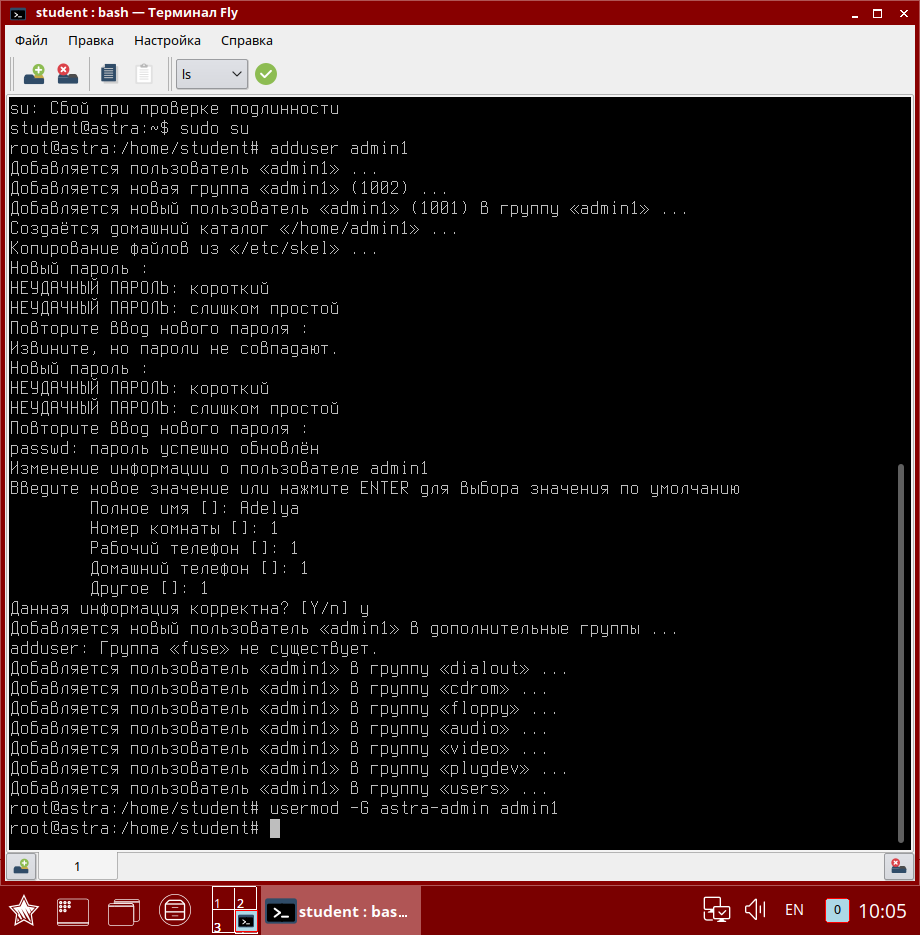
3. Авторизуйтесь под пользователем root. Выполните команды.



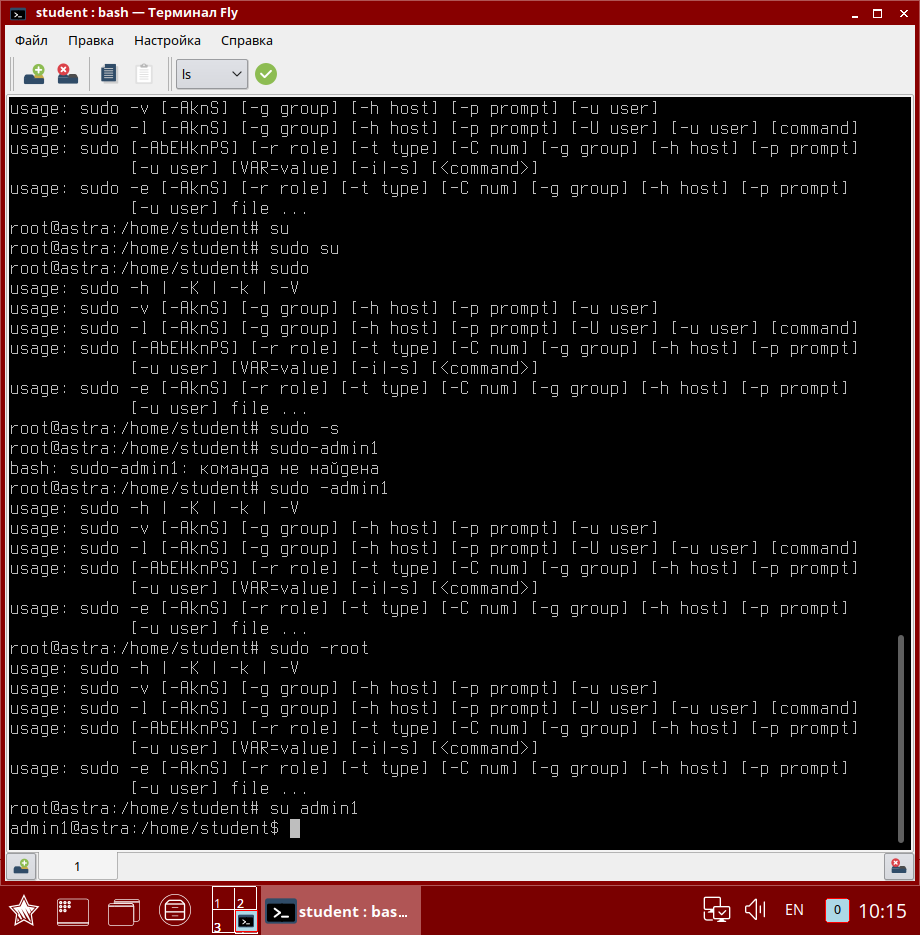
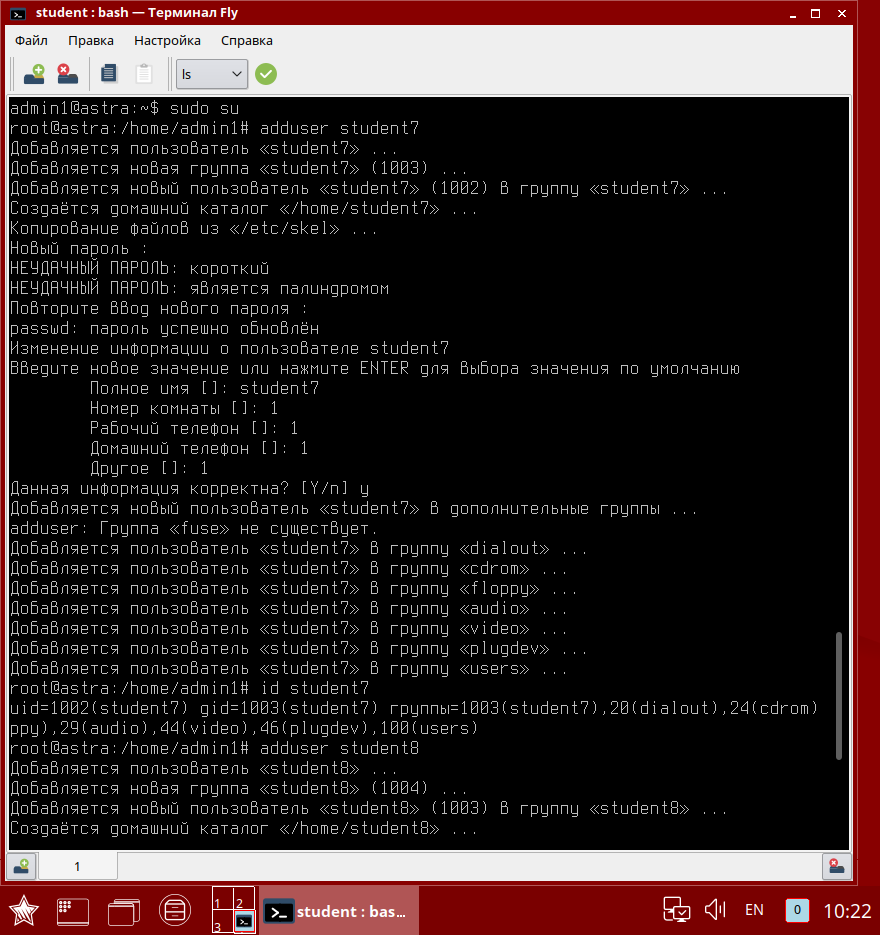
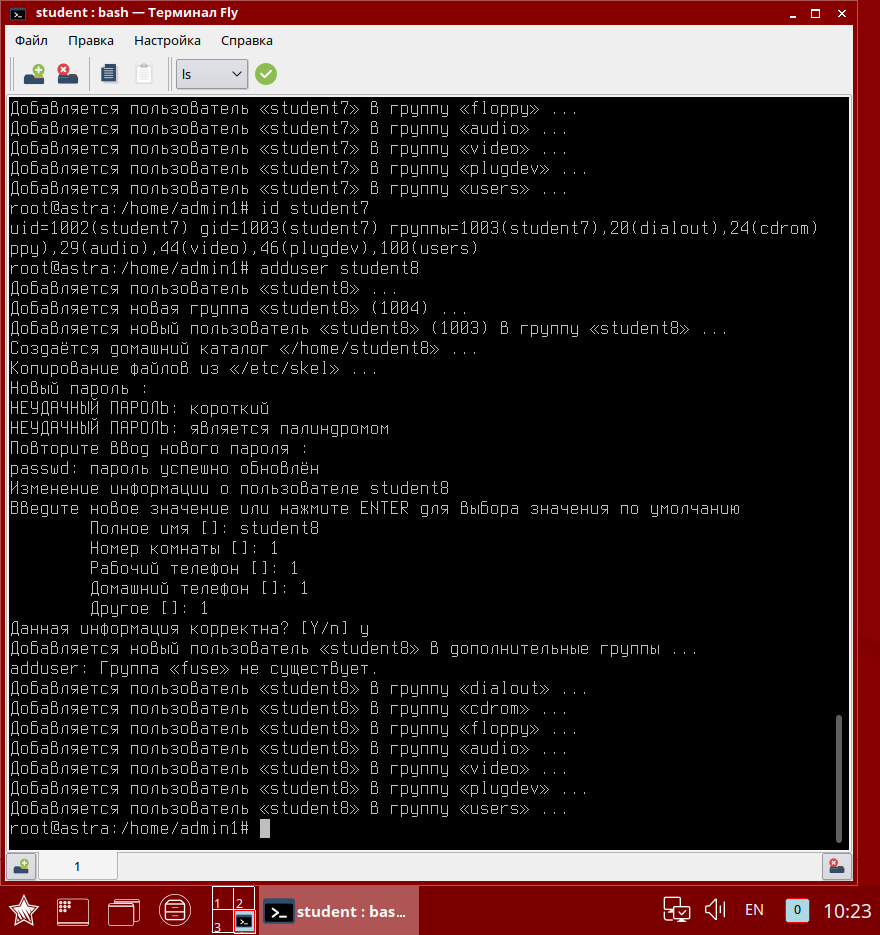
**$ adduser admin1**

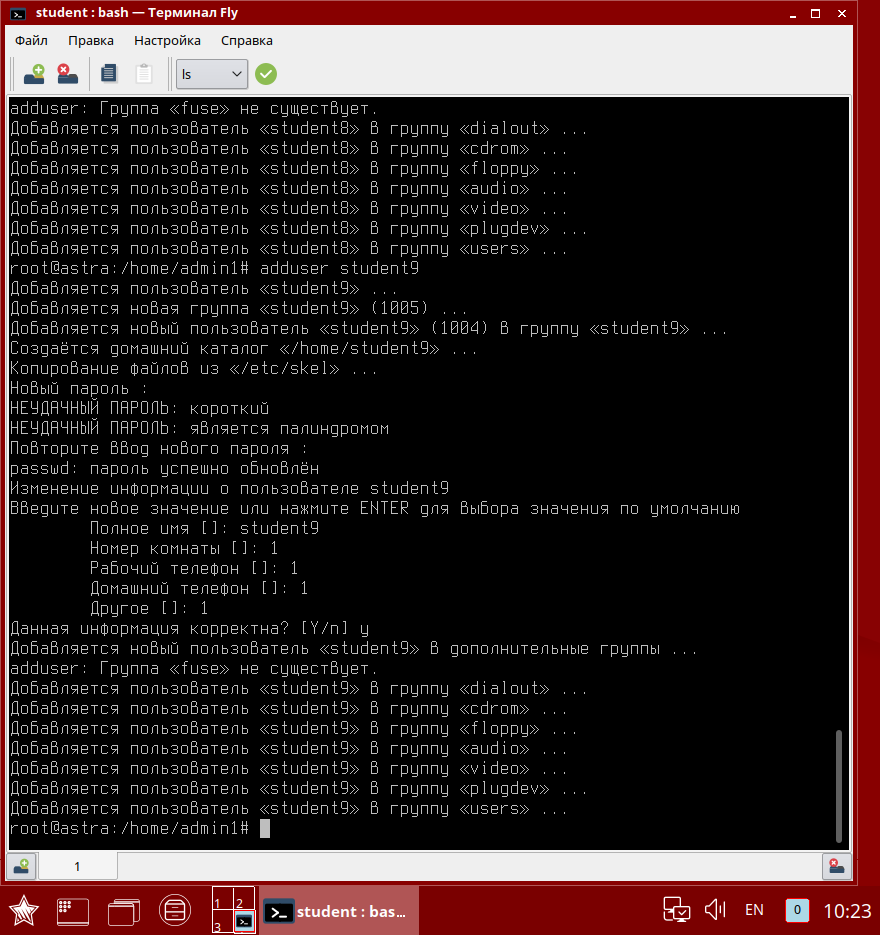


**$ usermod -G astra-admin admin1**

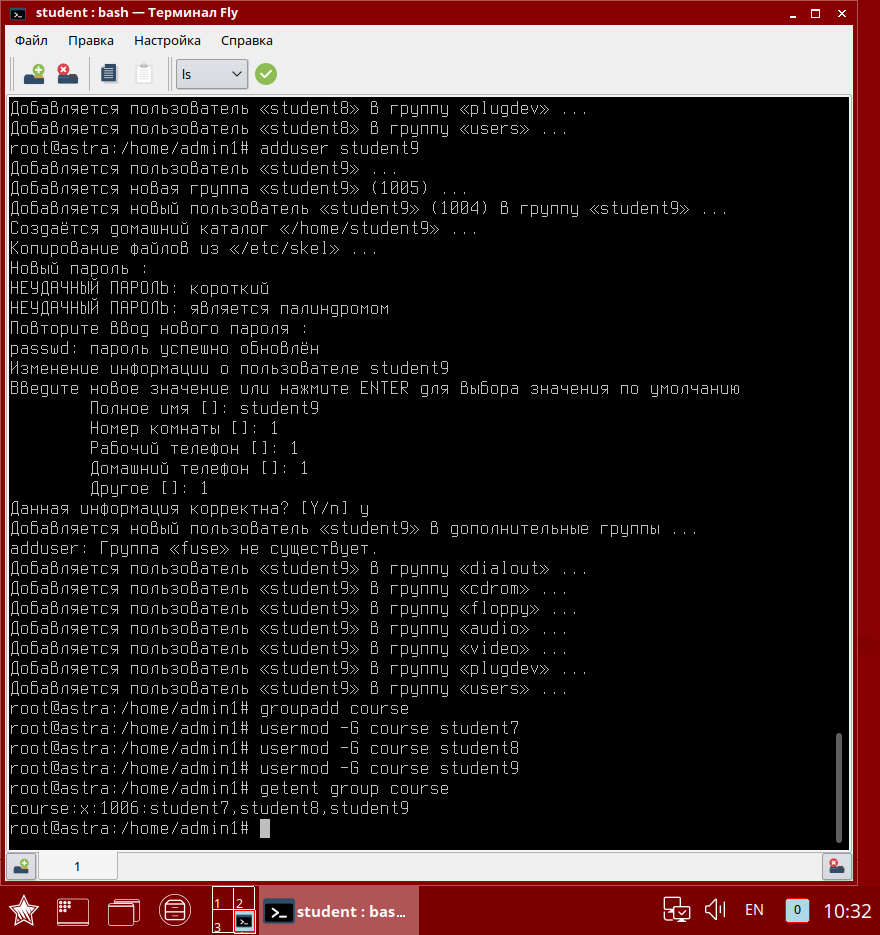


4. Авторизуйтесь под пользователем admin1. Добавьте трех новых пользователей с соответствующими домашними директориями: student7, student8, student9. Задайте пароли для каждого из них, используйте команду adduser.

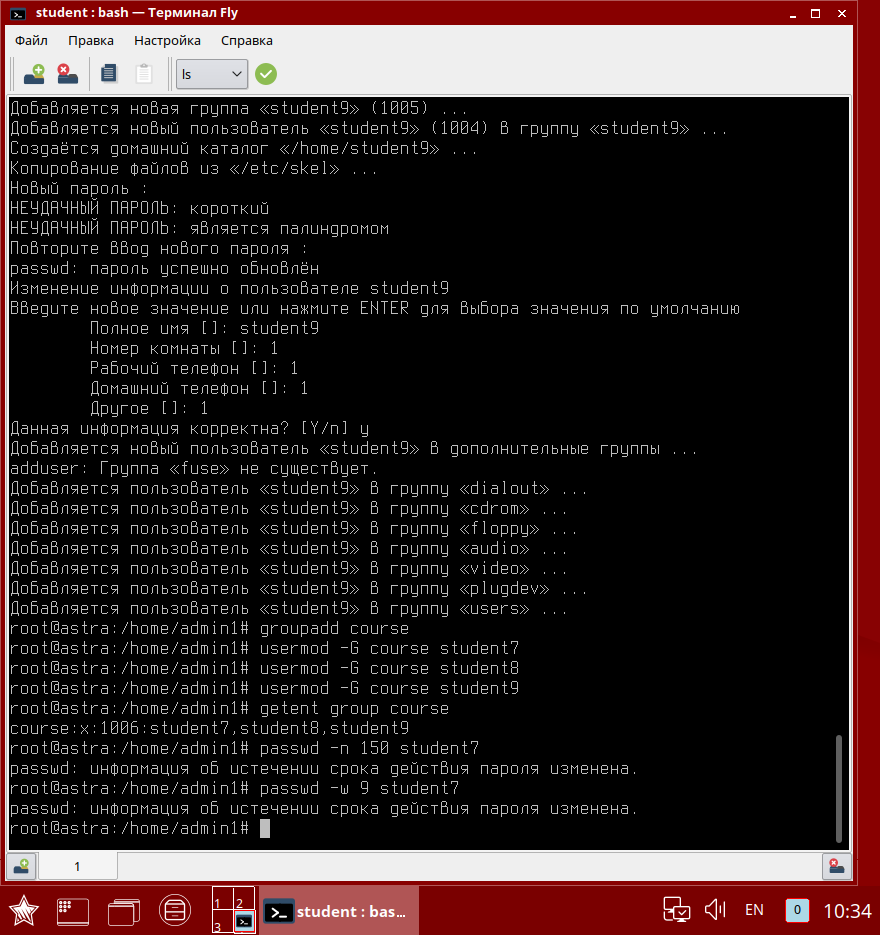
  



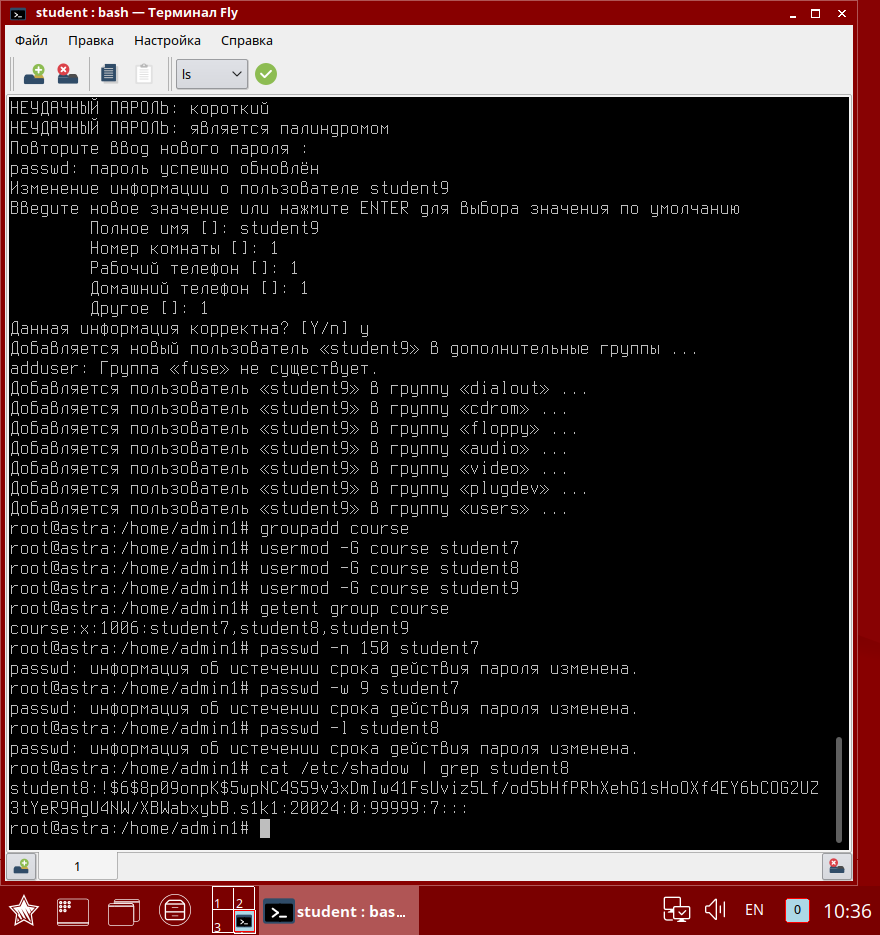
5. Создайте группу course и добавьте в нее всех трех пользователей.



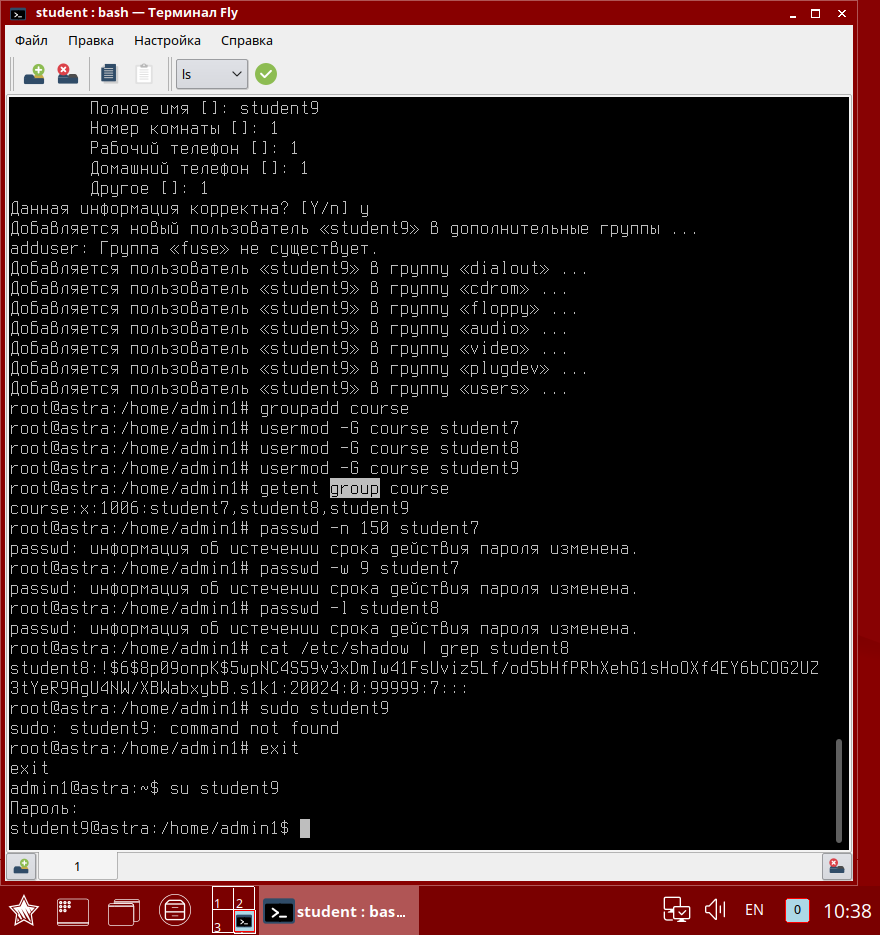
6. Для пользователя student7 выставите ограничение: срок действия пароля 5 месяцев (150 дней) и предупреждение об окончании срока действия пароля 9 дней.



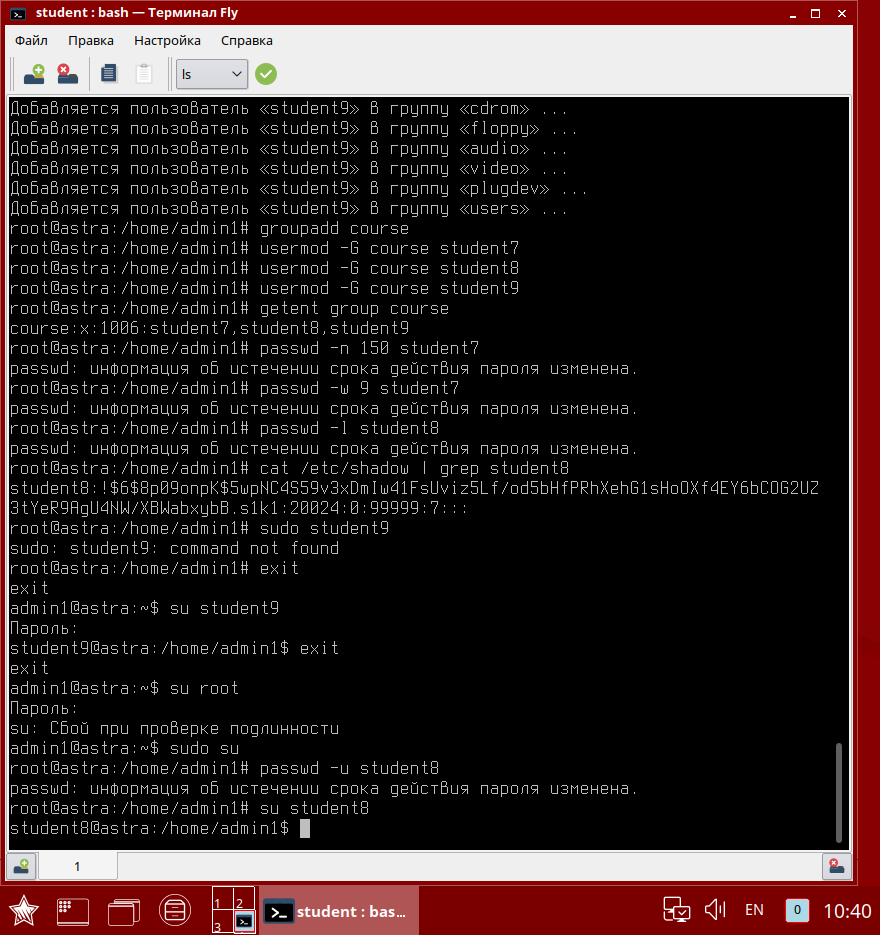
7. Заблокируйте пользователя student8, заблокировав его пароль. Проверьте, что блокировка подействовала.



8. Войдите в систему под пользователем student9, находясь в этом же терминале.

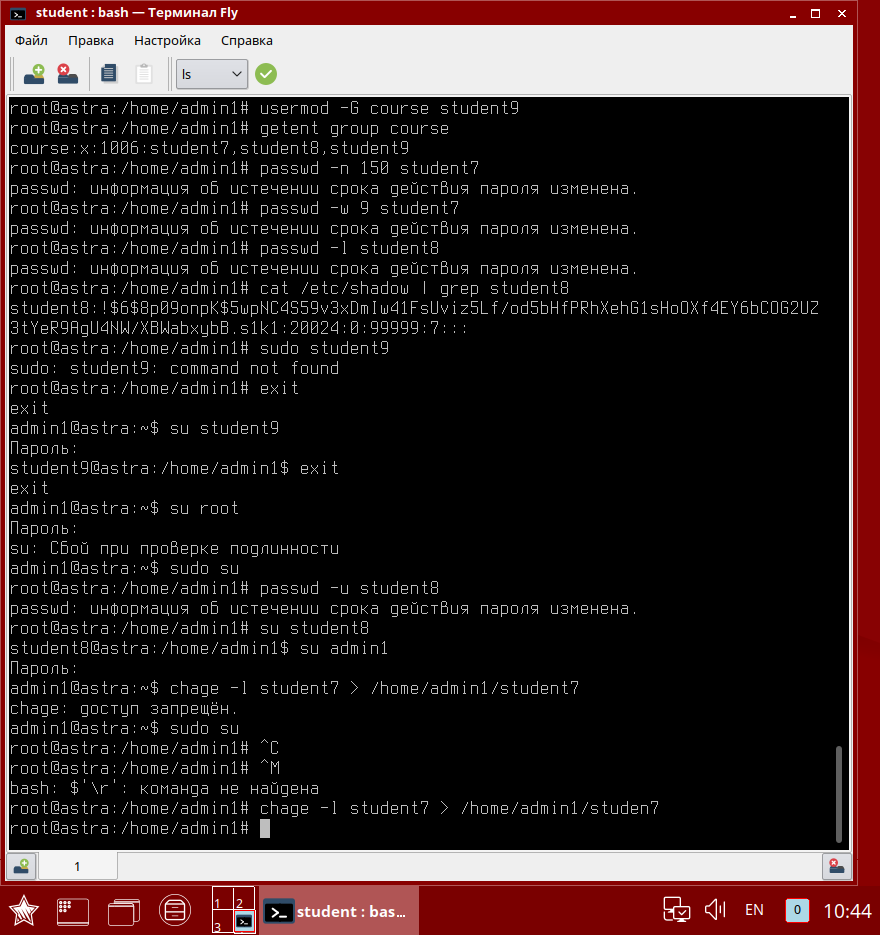


9. Войдите в систему под пользователем root. Разблокируйте пользователя student8. Проверьте, что блокировка снята.



10. Войдите в систему под пользователем admin Выполните команду

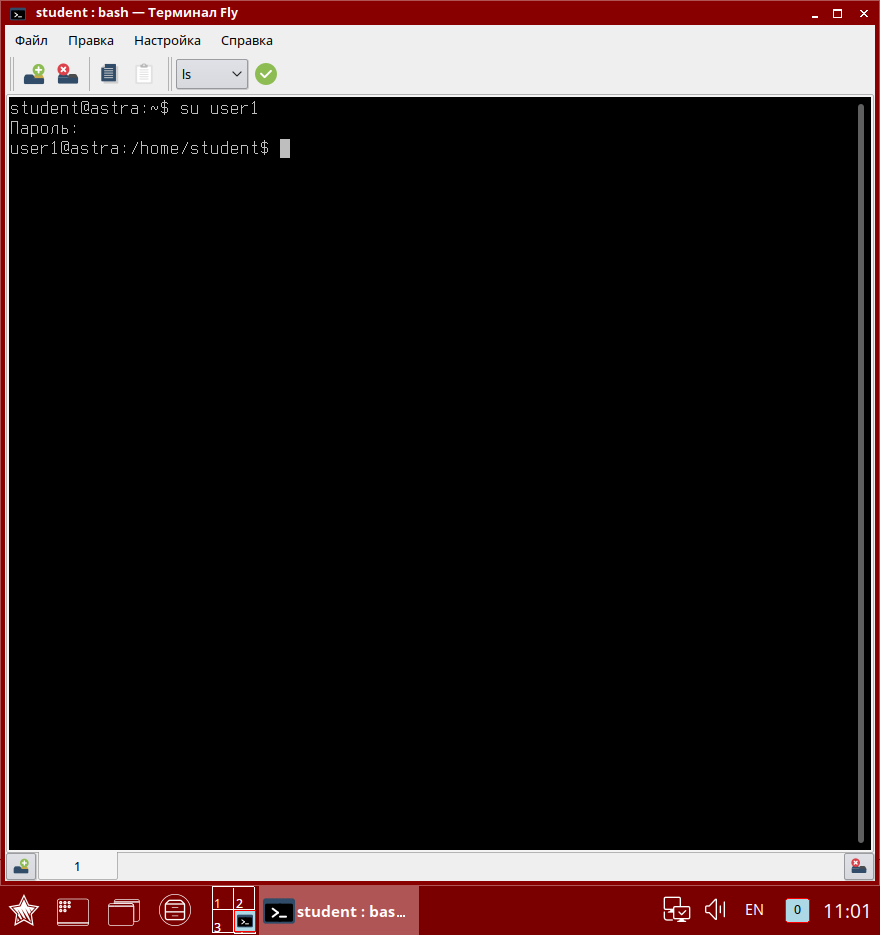
**chage -l student7 > /home/admin1/student7**

****

**Разграничение доступа к файлам**

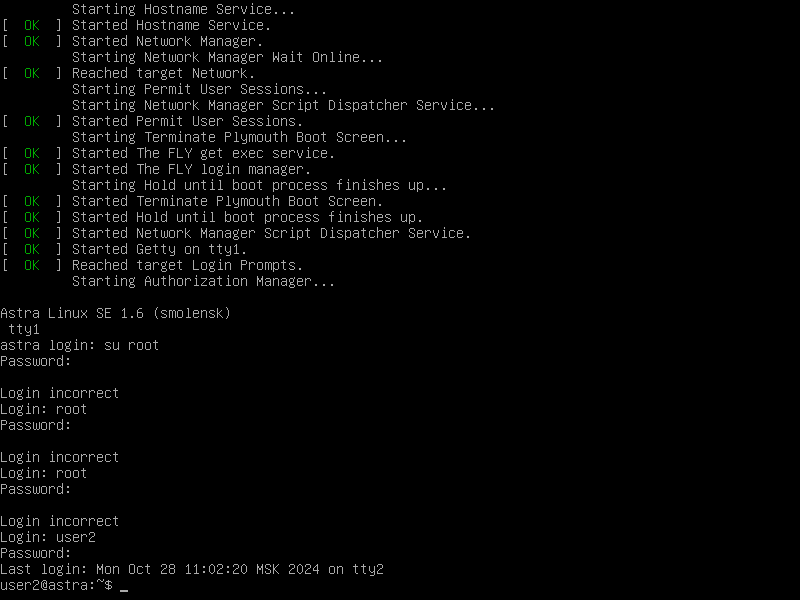
1. Авторизуйтесь под root. Создайте двух пользователей (user1 и user2) и задайте их пароли.

2. Откройте первую консоль и зарегистрируйтесь в ней как user1.



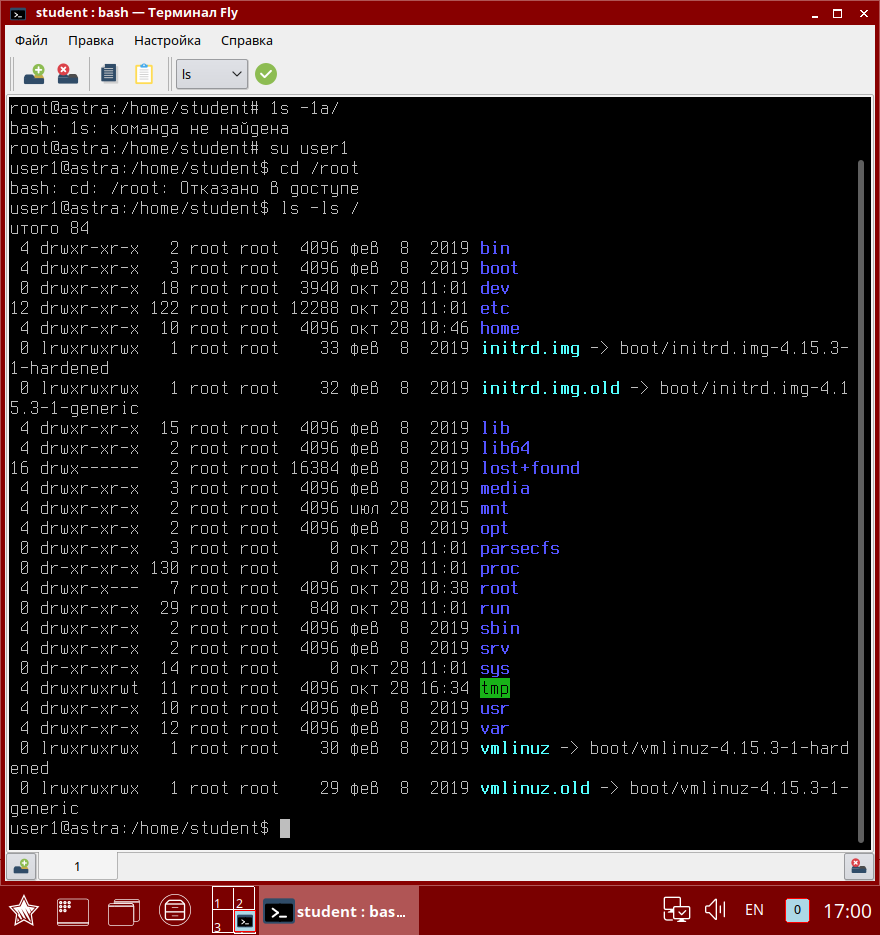
3. С помощью Ctrl+Alt+F2 (Alt+F2) откройте второй текстовый терминал и зарегистрируйтесь как user2



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

5. Нажатием Ctrl+Alt+F7 (Alt+F7) вернитесь в первую консоль. Теперь, переключая консоль, вы можете работать с объектами операционной системы от имени двух разных пользователей и администратора системы.

6. С правами user1 попробуйте войти в каталог /root. С помощью команды ls -la / просмотрите список основных каталогов и посмотрите, каких прав доступа вам недостает для входа в каждый из каталогов.

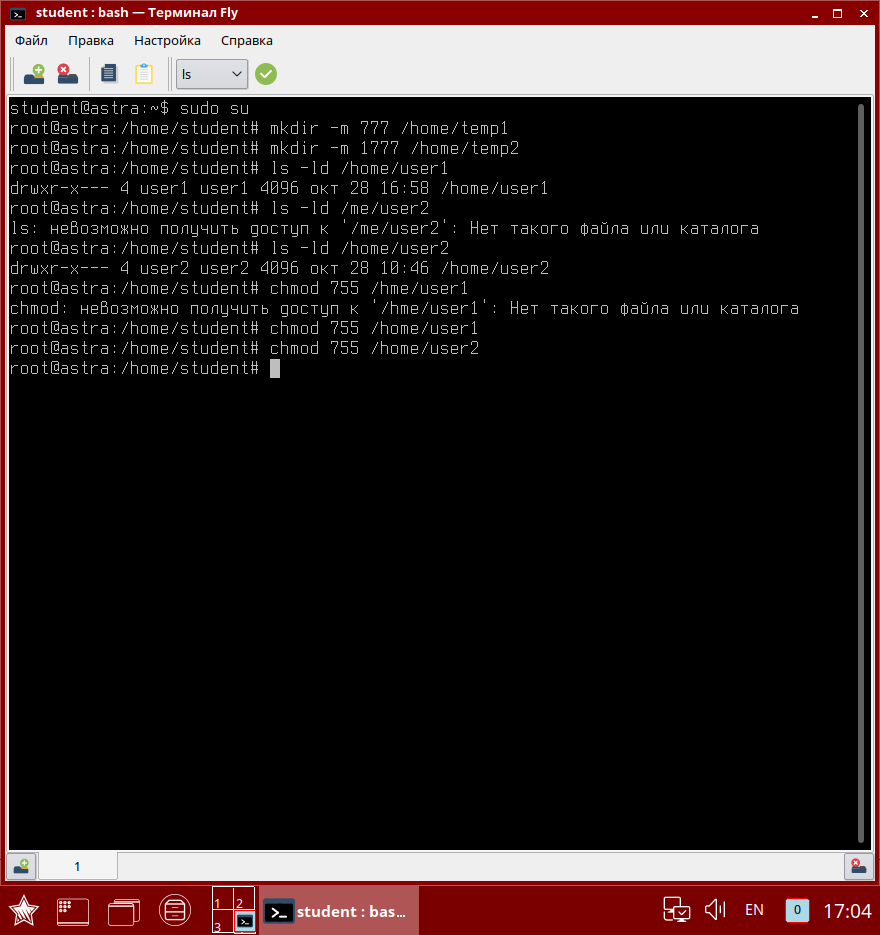


7. Переключитесь в консоль администратора и создайте два новых временных каталога командами

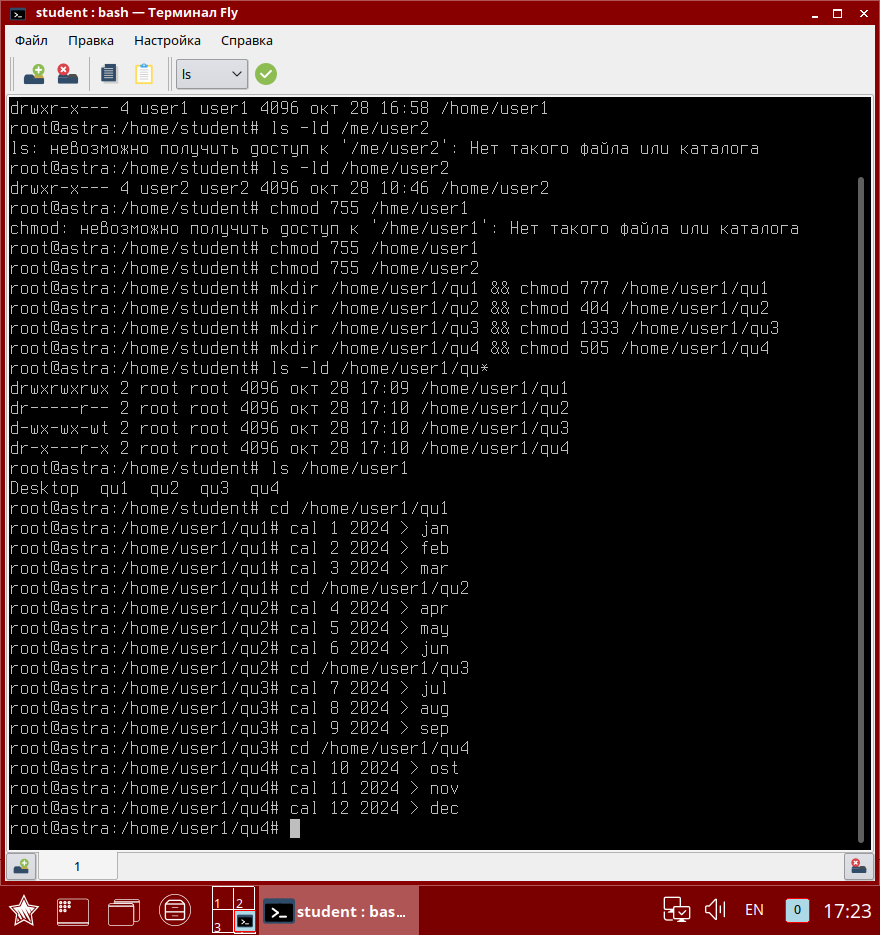
**mkdir -m 777 /home/temp1**

**mkdir -m 1777 /home/temp2**.

Проверьте права доступа к каталогам /home/user1 и /home/user2: они должны быть установлены в 755. Вернитесь в консоль user1.

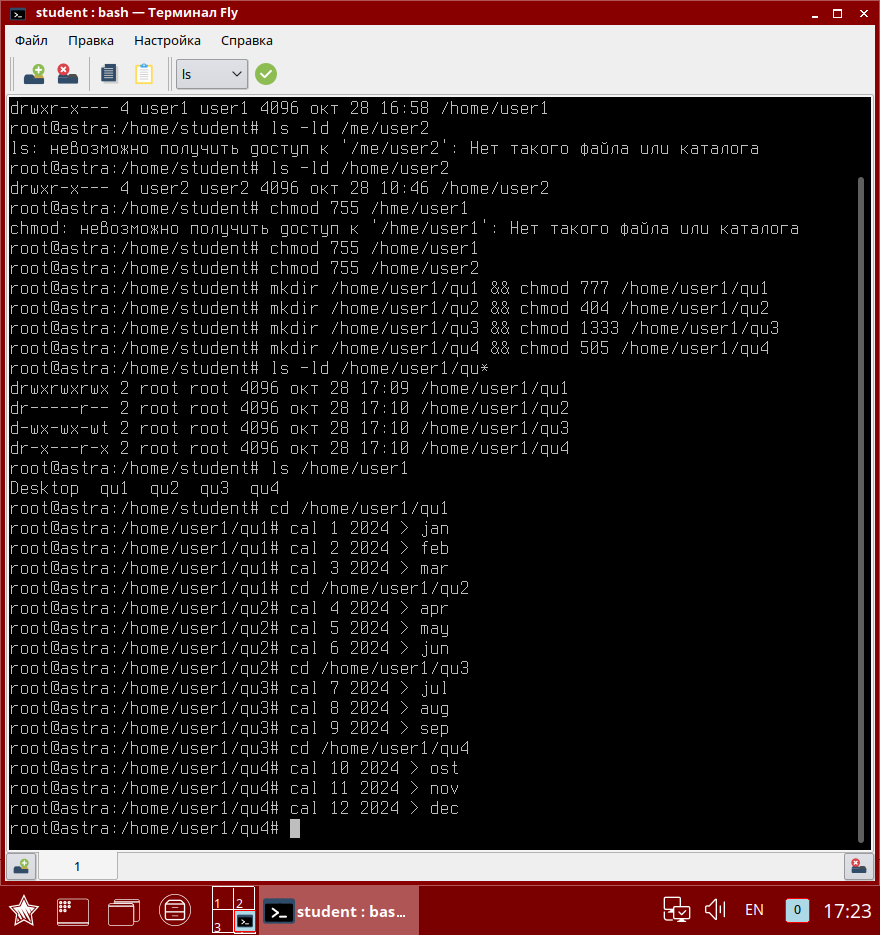


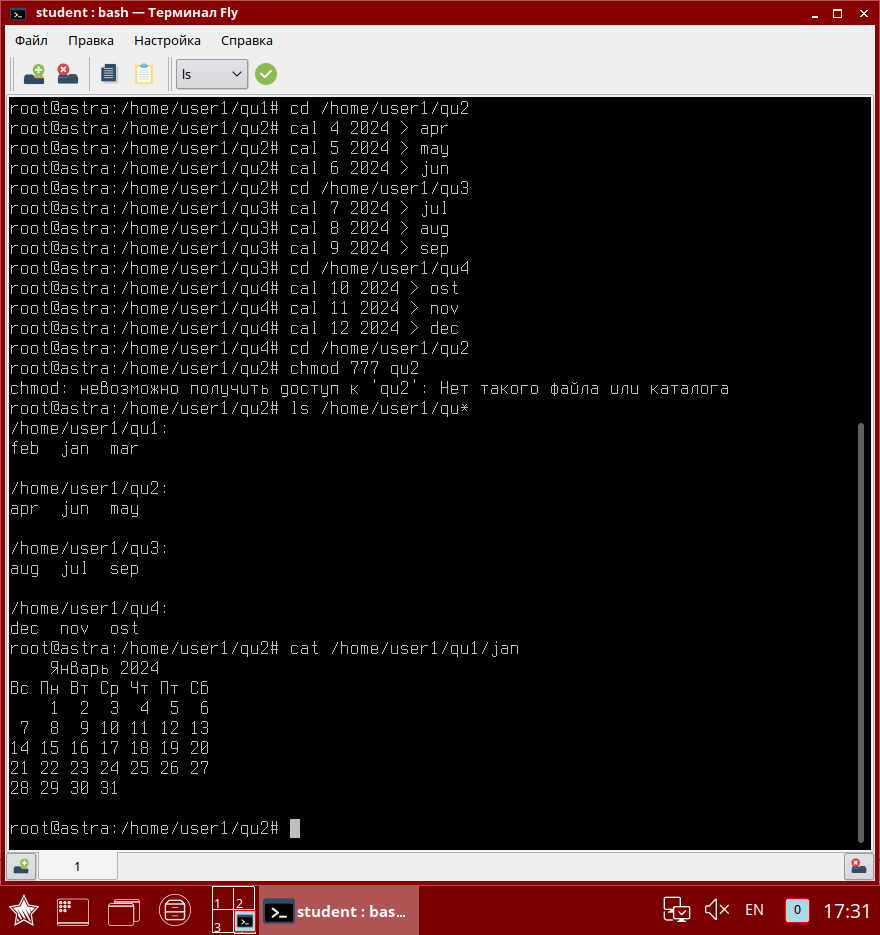
8. Создайте в домашнем каталоге пользователя /home/user1 четыре каталога с именами: qul, qu2, qu3, qu4. При создании каталогов объявите следующие права доступа к ним: (qul - 777, qu2 - 404, qu3 - 1333, qu4 - 505).

9. С помощью команды ls /home/user1 убедитесь в том, что каталоги созданы. В каждом из каталогов создайте по три текстовых файла с именами (jan, feb, mar), (apr, may, jun), (jul, aug, sep), (oct, nov, dec). В каждый файл запишите календарь на определенный месяц текущего года. Например, команда

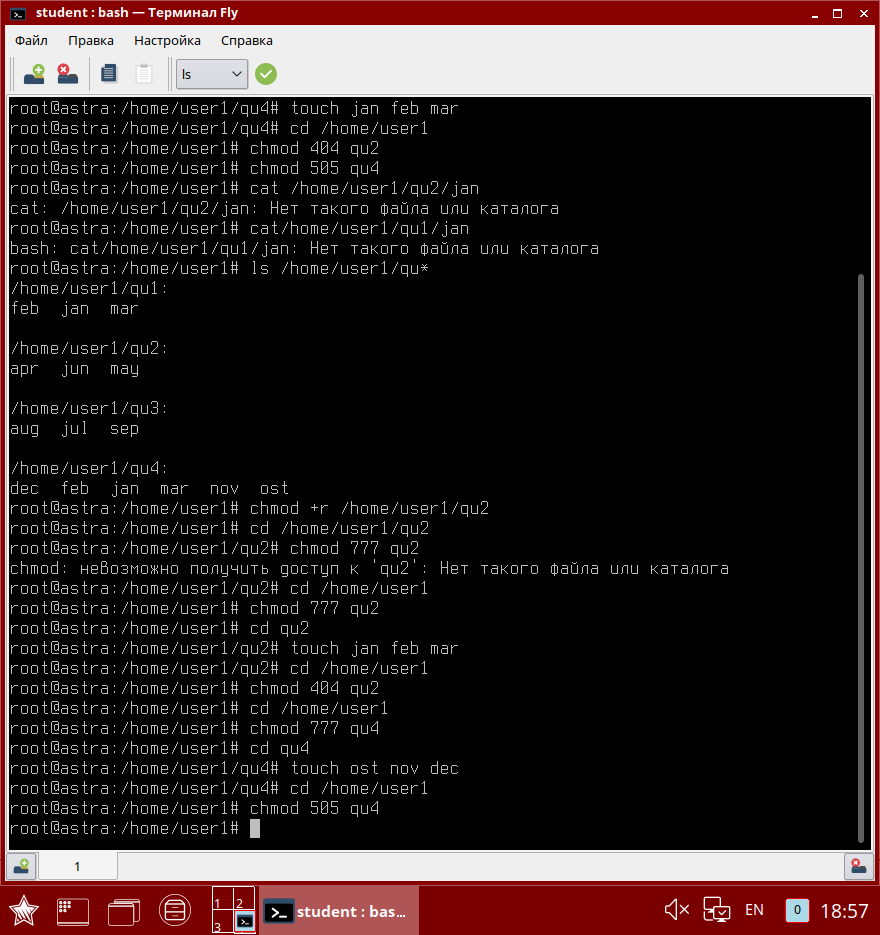
**cal 1 2022 > jan**

создает в текущем каталоге файл jan и записывает в него календарь на январь 2024 года.





10. Измените нужные права доступа в "недоступные" каталоги qu2, qu4 и создайте там указанные файлы. После этого верните каталогам прежние права доступа.

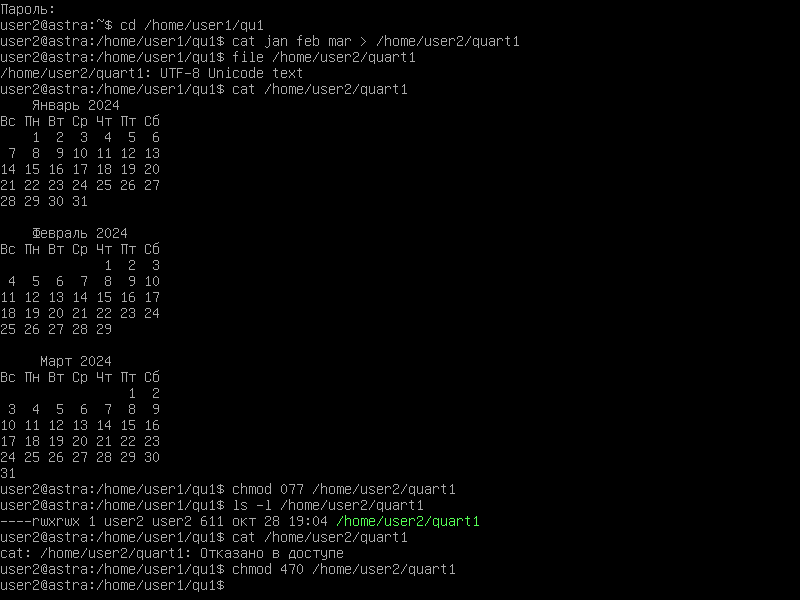


11. Прочитайте содержимое одного из файлов в "темном" каталоге.

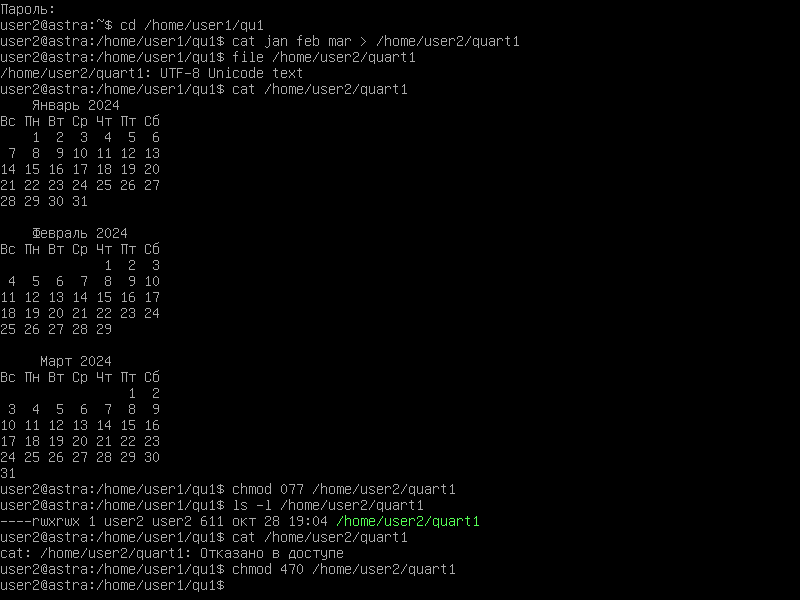
12. Перейдите во 2-ю консоль и с правами пользователя user2 войдите в каталог /home/user1/qul. Создайте в каталоге /home/user2 новый файл quart1 путем конкатенации нескольких имеющихся

**cat jan feb mar > /home/user2/quart1).**

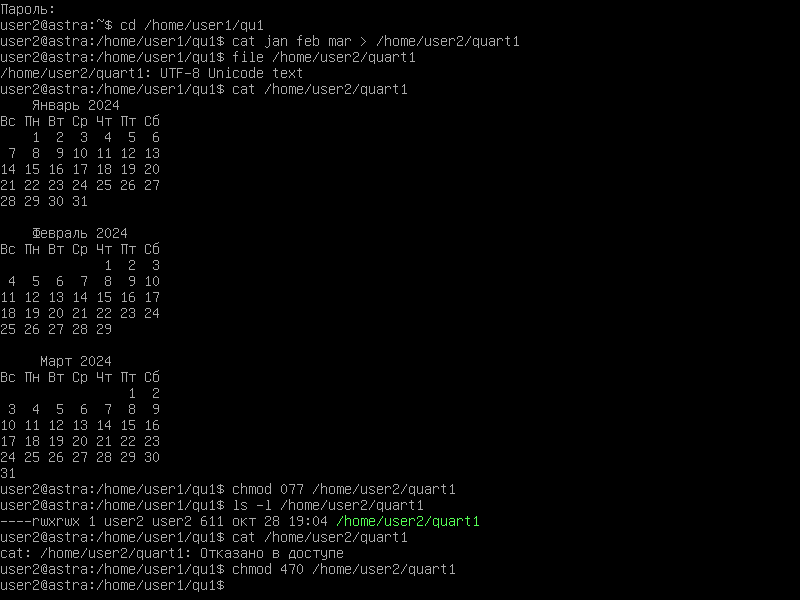
С помощью команды file определите тип созданного файла. Попробуйте вывести его на экран командой cat.



13. Установите права доступа 077 на созданный файл quart1. Вновь попробуйте прочесть его.



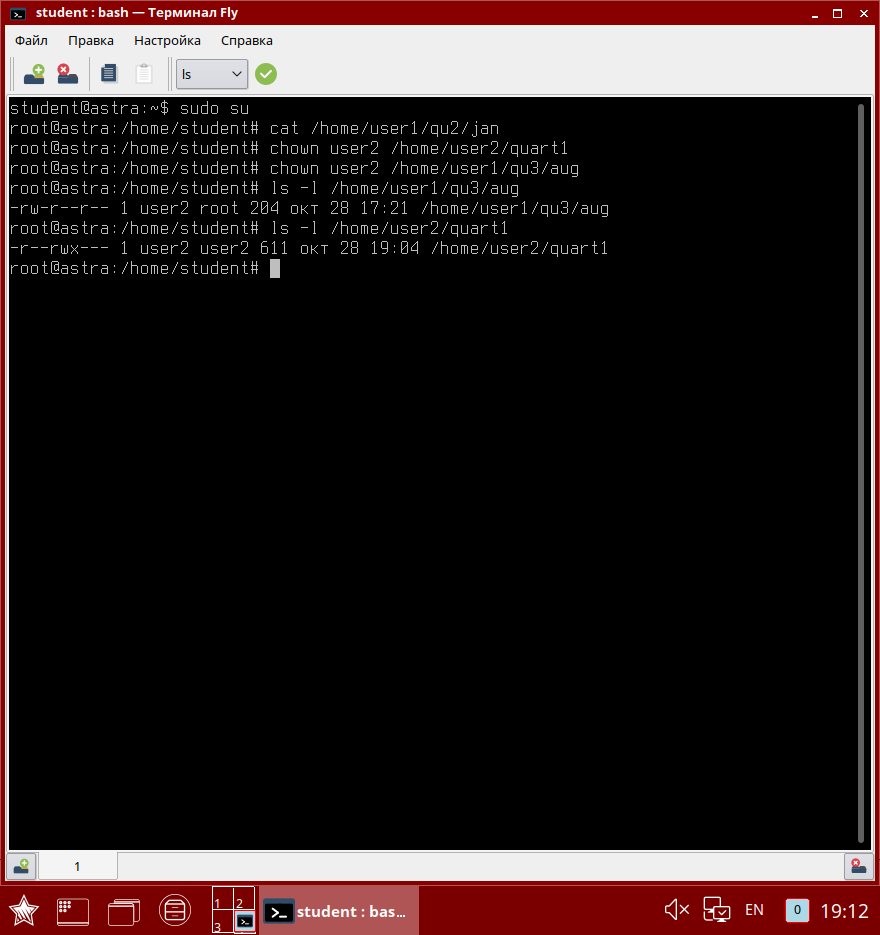
14. Установите для файла quatr1 права на доступ 470.



15. Перейдите в консоль администратора и передайте право владения на файлы и aug пользователю user2:

**chown user2 aug.**

Поочередно из консолей user1 и user2 проверьте, как изменились права владения файлами после его передачи.

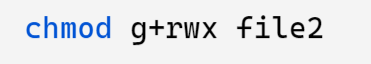


**Контрольные вопросы**

1. **Как назначить права на чтение и исполнение для файла file.conf для всех остальных? Напишите команду**

****

1. **Измените права доступа на чтение, запись и выполнение для группы файла file2? Напишите команду**

****

1. **Что является результатом выполнения команды chmod 755 file?**

Команда `chmod 755 file` устанавливает следующие права доступа:  
    **Владелец:** Чтение, запись, исполнение (7 = 4 + 2 + 1)  
    **Группа:** Чтение, исполнение (5 = 4 + 1)  
    **Остальные:** Чтение, исполнение (5 = 4 + 1)

1. **С помощью какой команды можно изменить владельца файла?**

****

1. **Что означает запись rw-r-xr-- ?**

Эта запись представляет собой права доступа к файлу в виде octal mode:  
    `rw-` - Владелец: Чтение (`r`), запись (`w`), без исполнения (`-`).  
    `r--` - Группа: Чтение (`r`), без записи (`-`), без исполнения (`-`).  
    `r--` - Остальные: Чтение (`r`), без записи (`-`), без исполнения (`-`).

1. **В чем отличие между дискреционным и мандатным методам разграничения доступа? Какие у них достоинства и недостатки?**

**Дискреционное разграничение доступа (DAC)**:  
        **Достоинства:** Гибкое, позволяет владельцу файла или каталога управлять правами доступа.  
        **Недостатки:** Может быть сложно контролировать и управлять правами доступа, особенно в больших системах.  
        **Пример:** `chmod` команда в Linux/Unix.  
    **Мандатное разграничение доступа (MAC)**:  
        **Достоинства:** Более строгий контроль, защищает от несанкционированного доступа даже со стороны владельца.  
        **Недостатки:** Менее гибкое, может ограничивать некоторые законные действия.  
        **Пример:** SELinux в Linux.

**Выводы:** на данной лабораторной работе мы исследовали парольные подсистемы аутентификации пользователей. Реализовали генераторы паролей в Python, обладающие требуемой стойкостью ко взлому.

**Код программ и отчеты лабораторных работ доступны на моем github:**

**https://github.com/ironsast/kpfu-information-security**