**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИцЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

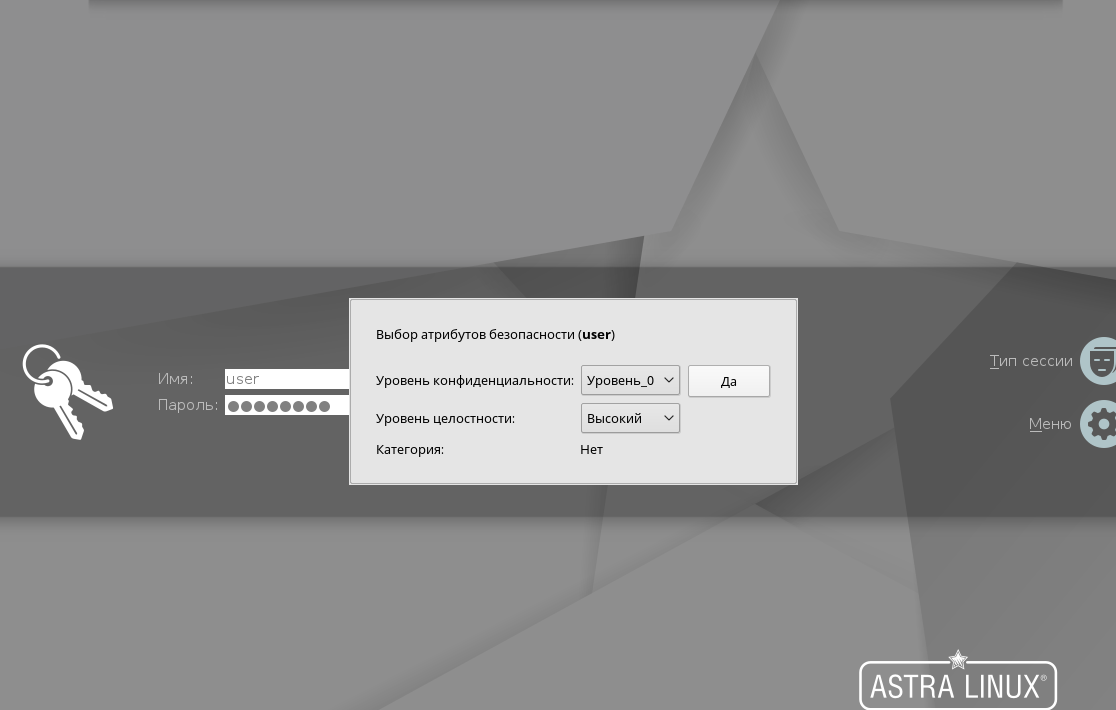
**Лабораторная работа № 7**

на тему «Администрирование локальных учётных записей пользователей и групп пользователей, конфигурирование политики безопасности в ОССН Astra Linux Special Edition»

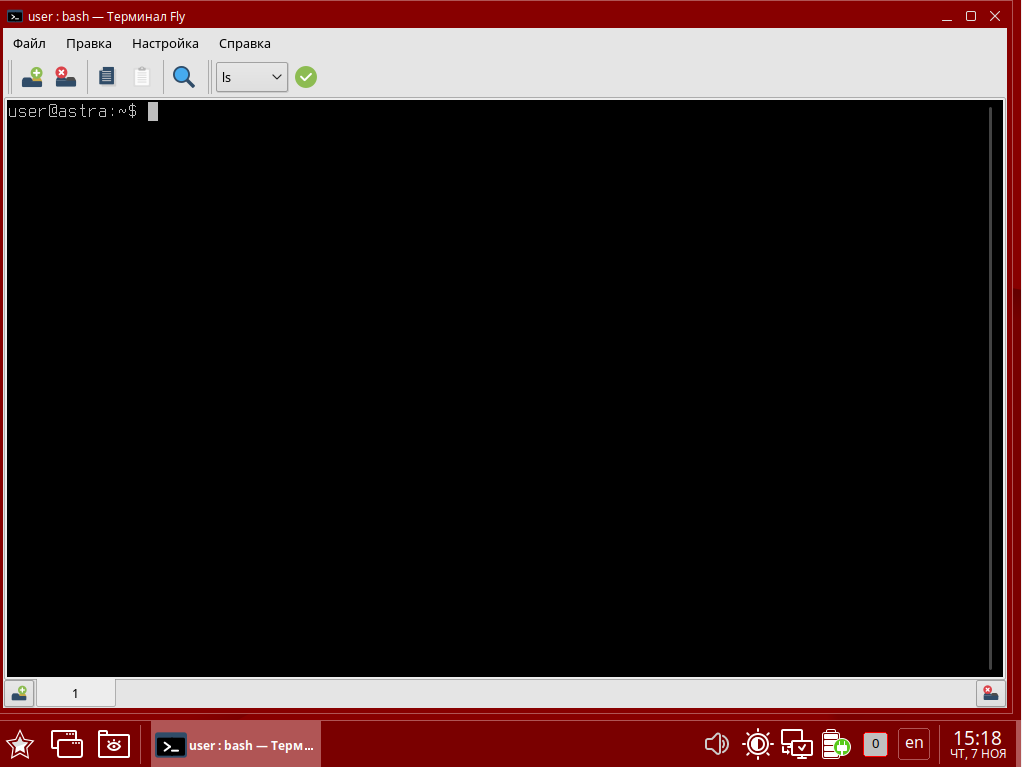
|  |
| --- |
| Выполнил: студент группы ВКБ41 |
| Якушевский Сергей Сергеевич |
| (Фамилия, имя, отчество) |
| Проверил: |
| Скляров Алексей Викторович |
| (Фамилия, имя, отчество) |

1. Авторизоваться в ОССН в графическом режиме с учётной записью пользователя user (уровень доступа — 0, неиерархические категории — нет,

уровень целостности — «Высокий»).

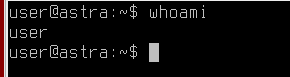


2. Запустить терминал Fly.



3. Определить текущую учётную запись пользователя с использованием

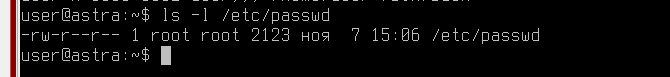
команды whoami.

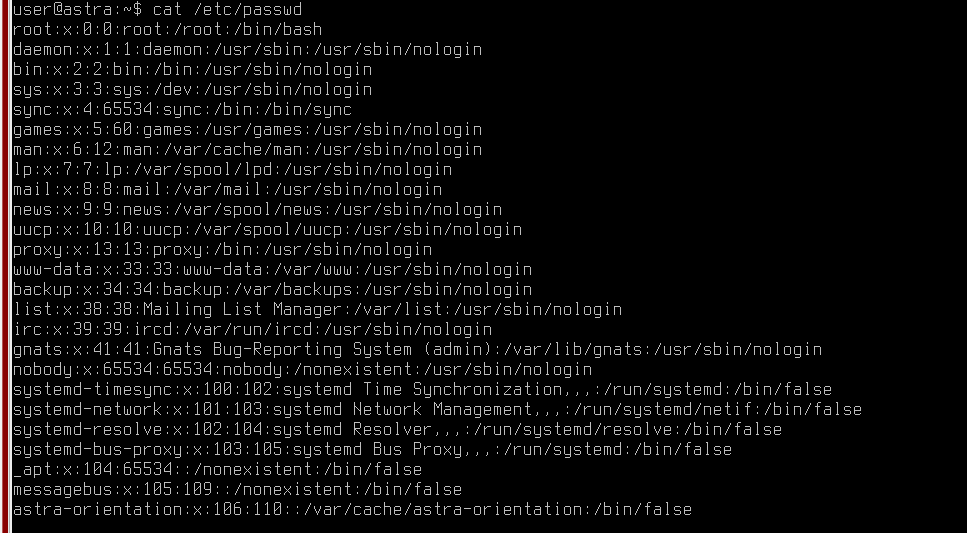


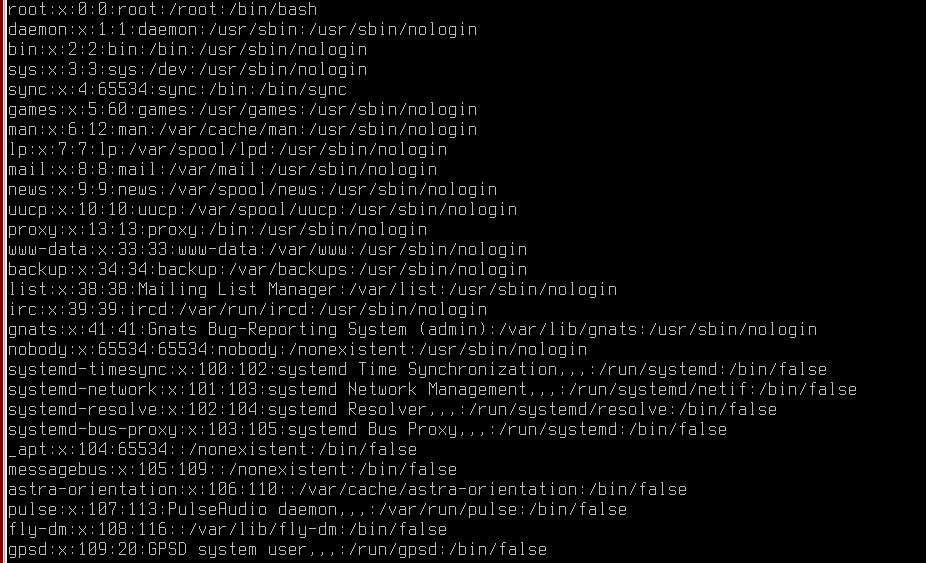
4. Проверить наличие права доступа на чтение к файлу /etc/passwd и

получить следующие данные, выполнив команды cat /etc/passwd или less

/etc/passwd:







количество параметров учётных записей пользователей;

В файле /etc/passwd каждая строка представляет собой одну учетную запись пользователя и состоит из 7 параметров, разделенных двоеточиями (:):

* Имя пользователя
* Пароль (хэш)
* UID
* GID
* Комментарий
* Домашний каталог
* Интерпретатор командной строки (shell)

cat /etc/passwd | head -n 1 | awk -F ':' '{print NF}'

количество параметров, совпадающих у всех учётных записей

пользователей;

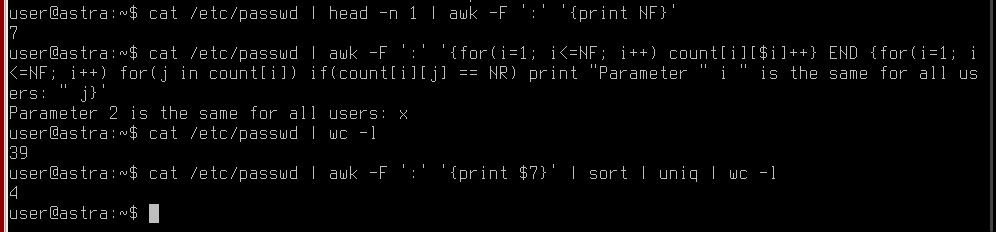
cat /etc/passwd | awk -F ':' '{for(i=1; i<=NF; i++) count[i][$i]++} END {for(i=1; i<=NF; i++) for(j in count[i]) if(count[i][j] == NR) print "Parameter " i " is the same for all users: " j}'

текущее число учётных записей пользователей;

cat /etc/passwd | wc -l

количество различных используемых командных интерпретаторов.

cat /etc/passwd | awk -F ':' '{print $7}' | sort | uniq | wc -l



5. Вывести строку, соответствующую текущей учётной записи

пользователя, из файла /etc/passwd с использованием команды cat

/etc/passwd | grep “^$(whoami)”, при этом получить следующие

данные:

наличие пароля или свёртки пароля (вывести эти данные командой)

cat /etc/passwd | grep "^$(whoami)" | cut -d : -f 2

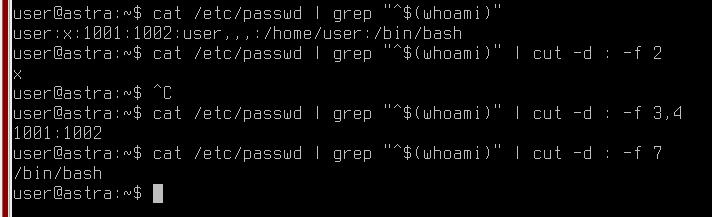
группа и идентификатор текущей учётной записи пользователя;

cat /etc/passwd | grep "^$(whoami)" | cut -d : -f 3,4

командный интерпретатор по умолчанию для текущей учётной записи

пользователя.

cat /etc/passwd | grep "^$(whoami)" | cut -d : -f 7



6. Настроить политику безопасности в соответствии со следующими

требованиями:

- должна осуществляться идентификация и проверка подлинности

субъектов доступа при входе в систему по идентификатору (коду) и паролю

условно-постоянного действия (срок действия пароля не более 90 суток), длиной не менее 6 буквенно-цифровых символов;

- вновь создаваемый пароль субъектов доступа должен удовлетворять

требованиям уникальности, т.е. отличатся не менее чем на 5 символов;

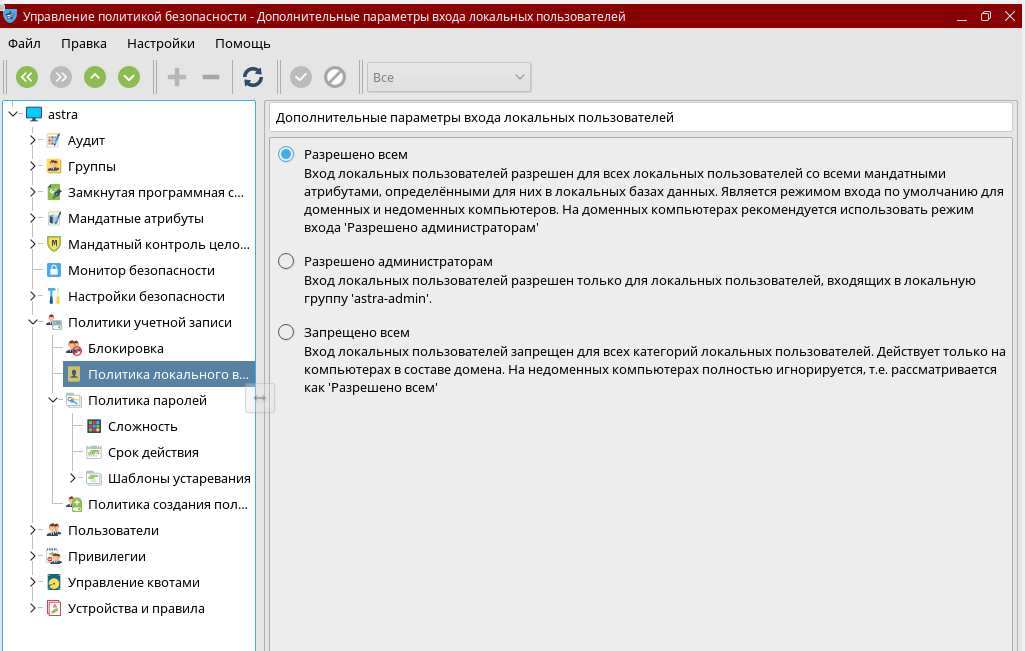
- субъект доступа должен быть предупрежден о необходимости смены

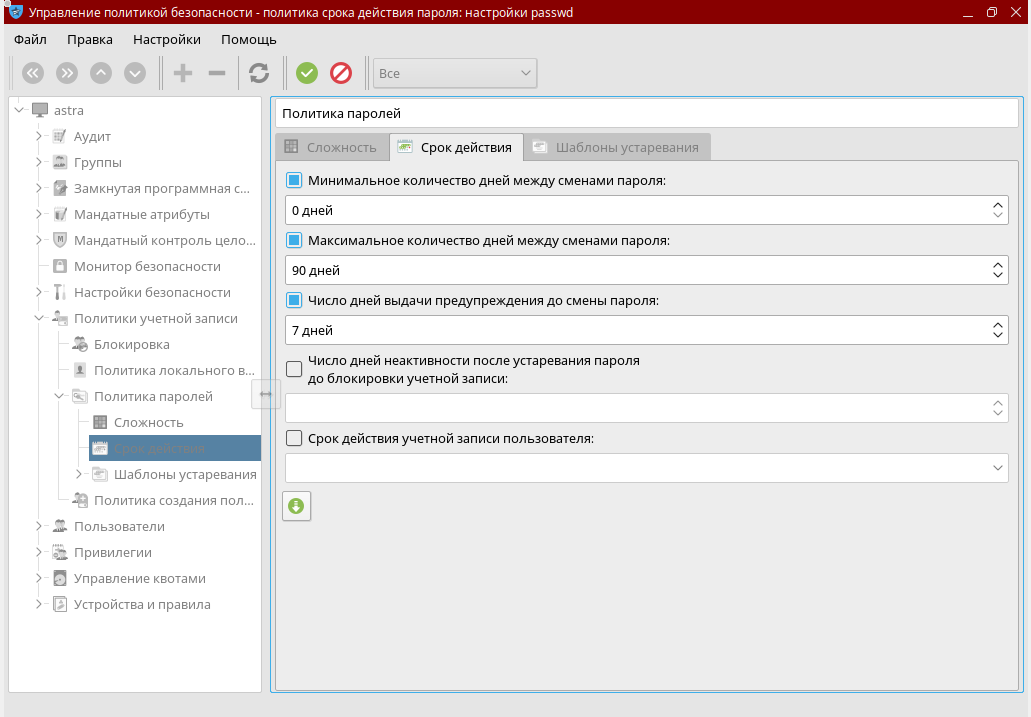
пароля не менее чем за 7 дней;

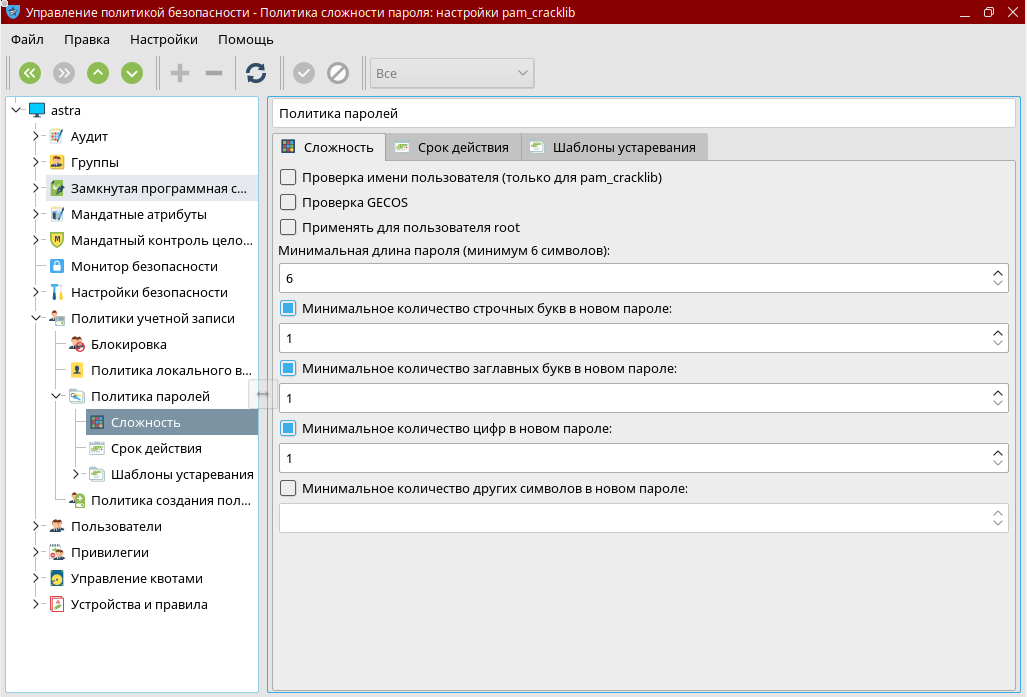
- после 4 неудачных попыток аутентификации учетная запись субъекта

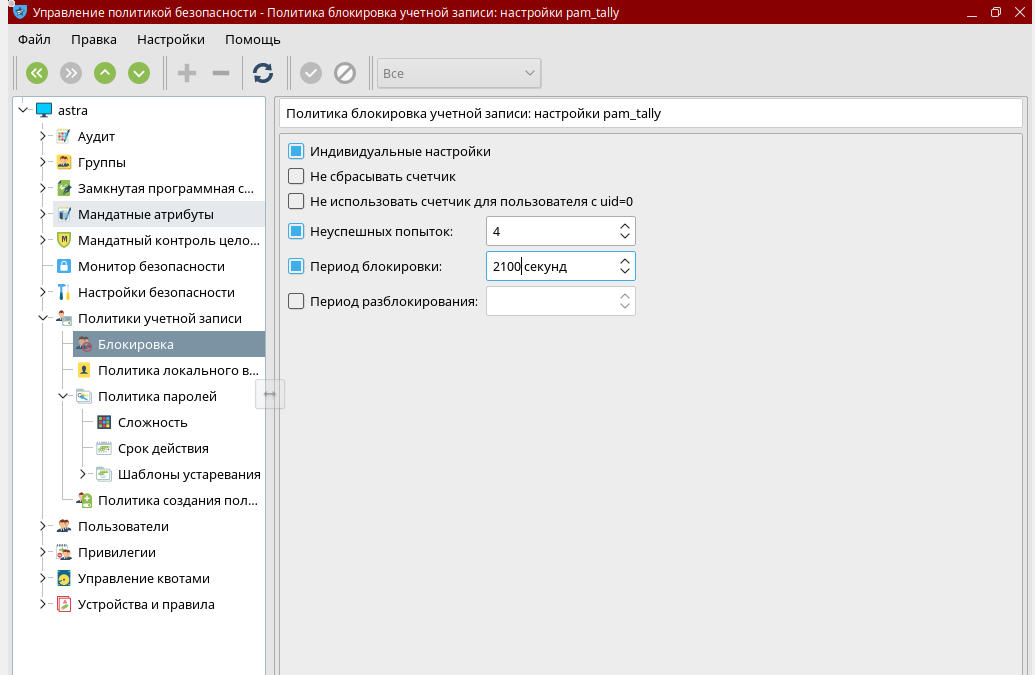
доступа должны быть заблокирована на срок не менее 35 минут (настройки

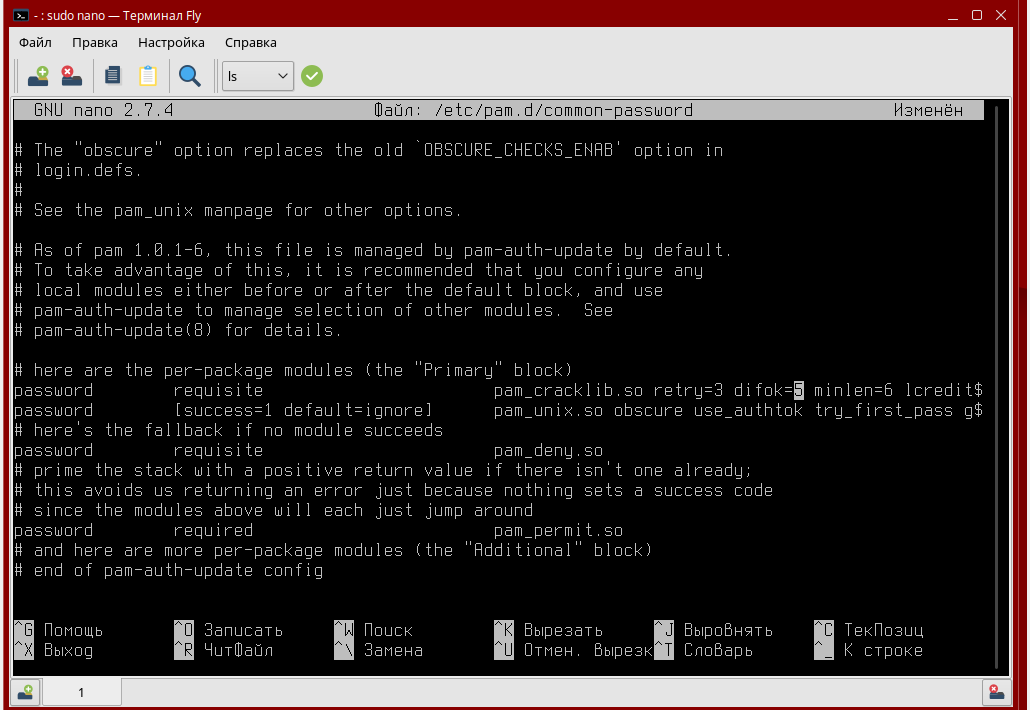
применимы для всех субъекта доступа).





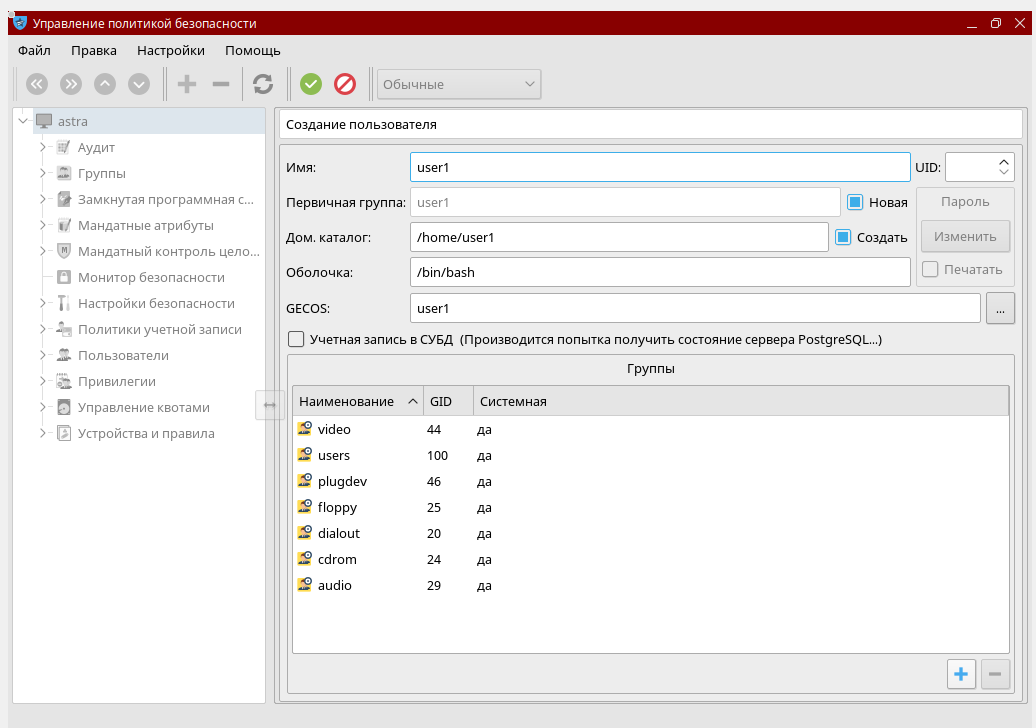


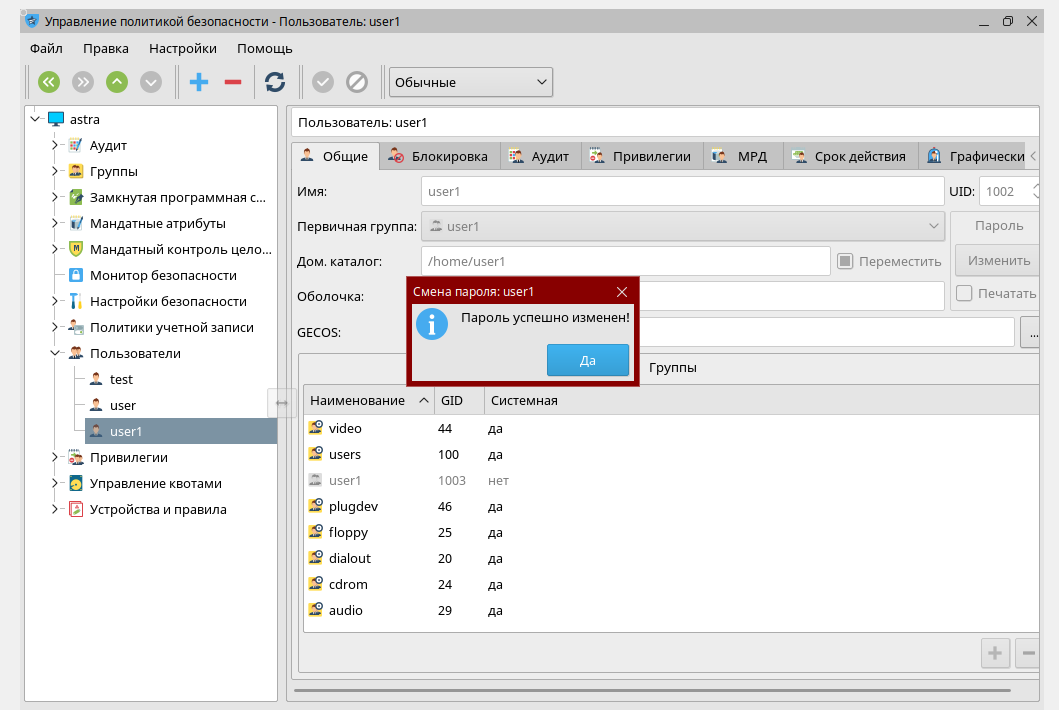




7. Создать учётную запись пользователя userl (с соответствующим

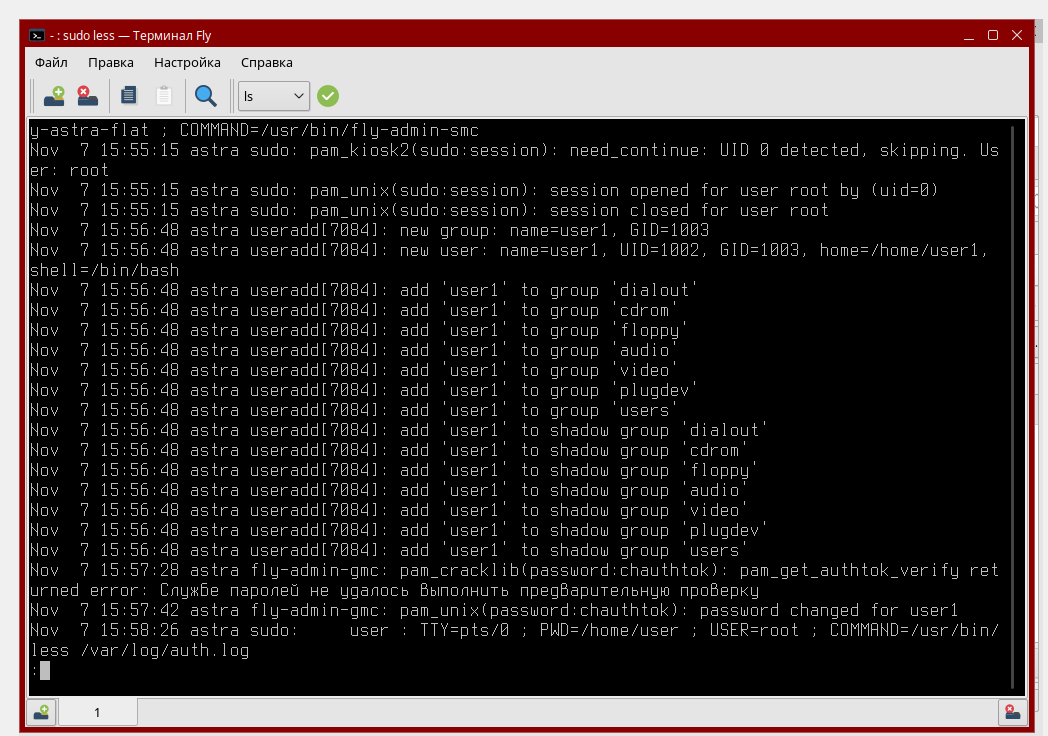
домашним каталогом) с использованием графического интерфейса, установить пароль, соответствующий требованиям политики информационной безопасности.





С помощью системного журнала less /var/log/auth.log определить все записи,

касающиеся рассматриваемого события.



8. Добавить учётную запись пользователя user2 с использованием

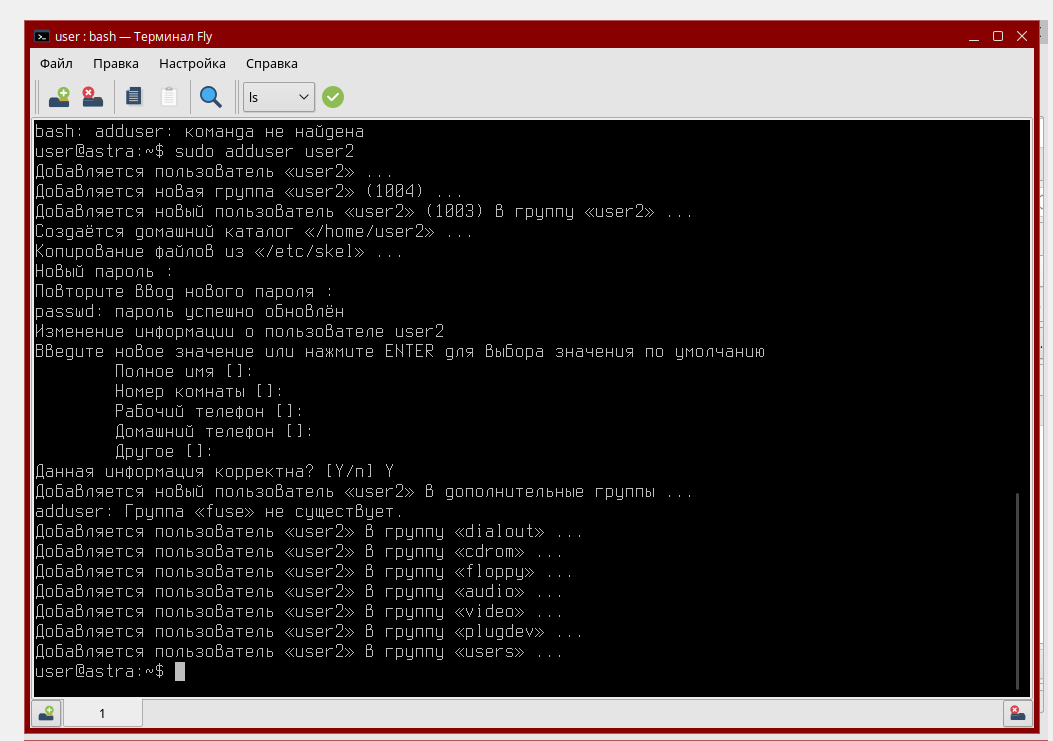
команды adduser user2,без использования команды sudo,

проанализировать и объяснить результат.

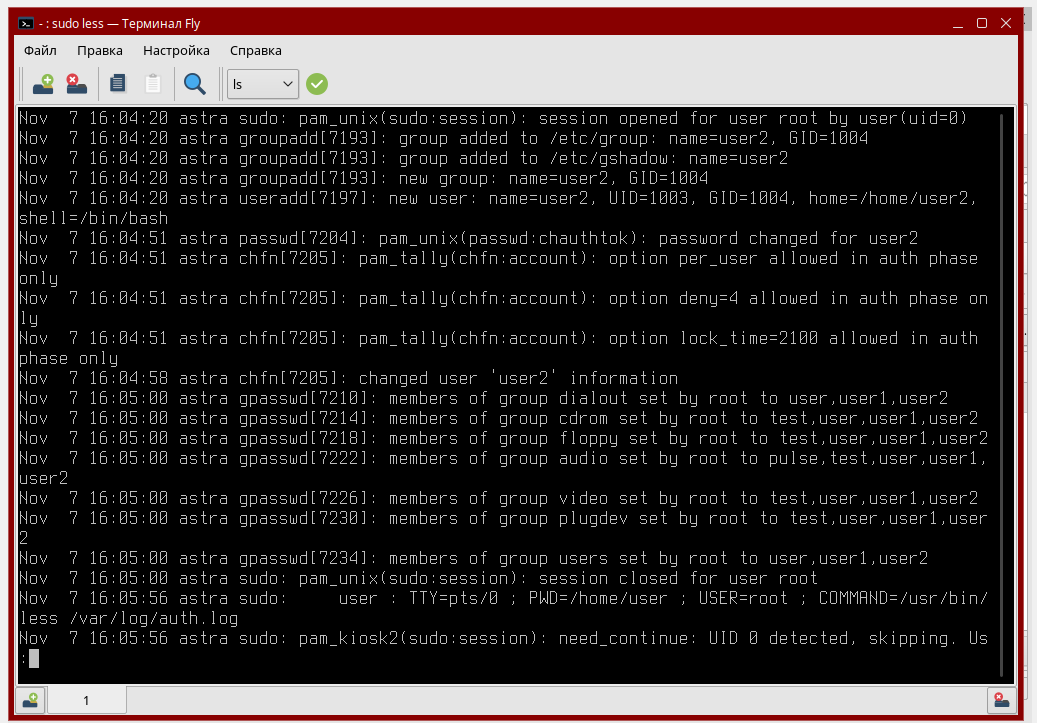


Выполнить те же действия с применением команды sudo. Установить учётной записи пользователя user2

пароль, соответствующий требованиям политики информационной безопасности.



С помощью системного журнала less /var/log/auth.log определить все записи, касающиеся рассматриваемого события.

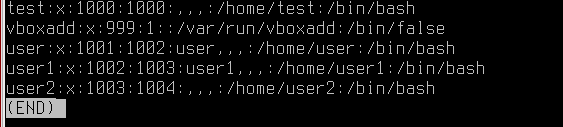


9. Проанализировать изменения в ОССН, связанные с добавлением новых

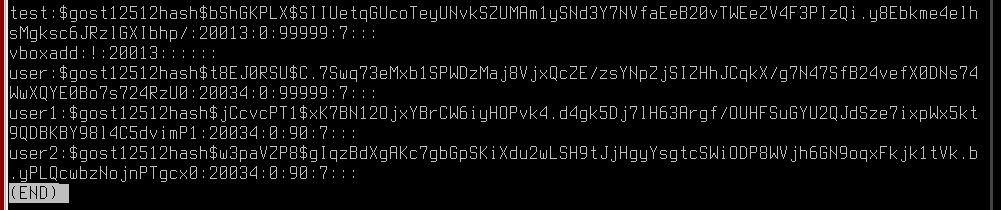
учётных записей пользователей, для чего определить:

домашние каталоги учётных записей пользователей по данным файла

Less /etc/passwd;



содержимое файла /etc/shadow;



алгоритм хеширования пароля, используемый в ОССН;

Алгоритм хеширования gost12512hash — это вариант хеширования, основанный на российском криптографическом стандарте ГОСТ Р 34.12-2015, который определяет алгоритм шифрования и хеширования. ГОСТ Р 34.12-2015 описывает алгоритмы на основе блочного шифрования, такие как **СТРИБУТ** (Стандартный Резервный Инструмент для Блочных Удвоенных Таблиц) и **КУЗНЕЧИК**. Алгоритм хеширования на основе ГОСТ-34.12 может называться **ГОСТ-3411-2012** и является частью семейства хеш-функций с высокой степенью безопасности.

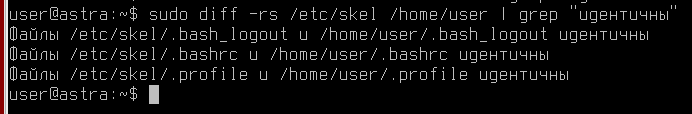
скрипты, которые были перемещены в домашние каталоги учётных

записей пользователей из каталога /etc/skel, при этом сравнить файлы в

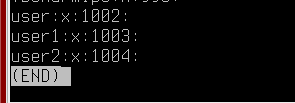
каталоге /etc/skel с файлами домашних каталогов учётных записей

пользователей с использованием команды

sudo diff -rs /etc/skel /home/user | grep “идентичны”;



новые группы в файле /etc/group;



идентификаторы новых учётных записей пользователей и групп в файлах/etc/group и /etc/passwd.

user1- 1003

user2 - 1004

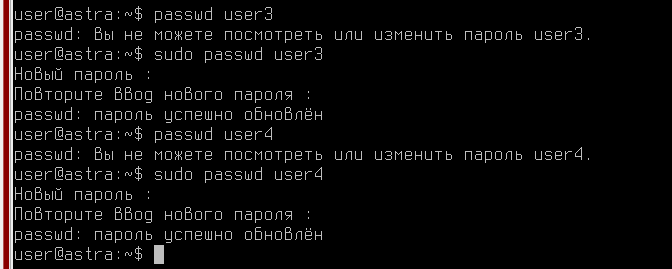
10. Создать учётные записи пользователей user3, user4 любым возможным способом (с помощью графического интерфейса или команды adduser).

11. Задать пароли для учётных записей пользователей user3 и user4,

соответствующие требованию политики безопасности, с использованием команд passwd user3 без использования команды sudo, проанализировать и объяснить результат.

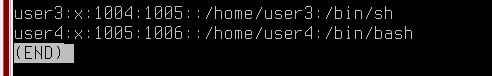
Выполнить те же действия с применением команды sudo,

sudo



после чего определить: домашние каталоги учётных записей пользователей по файлу

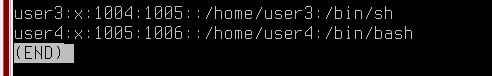
/etc/passwd;



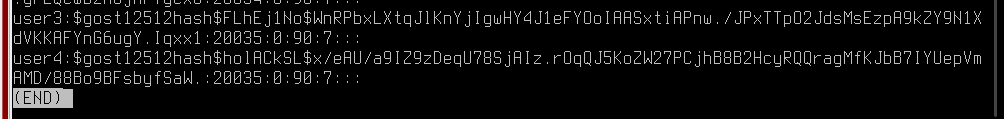
- наличие свёрток паролей учётный записей пользователей по файлам /etc/passwd и /etc/shadow;

В Linux-системах хеши паролей пользователей (иногда называемые "свёртками") хранятся в файле /etc/shadow, а файл /etc/passwd содержит только общую информацию о пользователях без паролей.

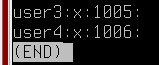
пароль может хранится в файле /etc/passwd, но это не соответсвует современным стандартам безопасности. Видим что вместо пароля стоит x, значит пароль хранится в файле /etc/shadow



хэши паролей хранятся в /etc/shadow



- новые группы в файле /etc/group



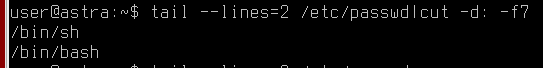
- идентификаторы новых учётных записей пользователей в файле /etc/passwd;

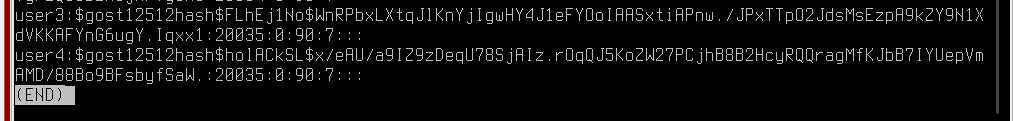
user3 – 1004

user4 -1005

- командный интерпретатор по умолчанию для созданных учётных записей пользователей, используя команду:

tail -1 / /passwd|cut -d: -f7

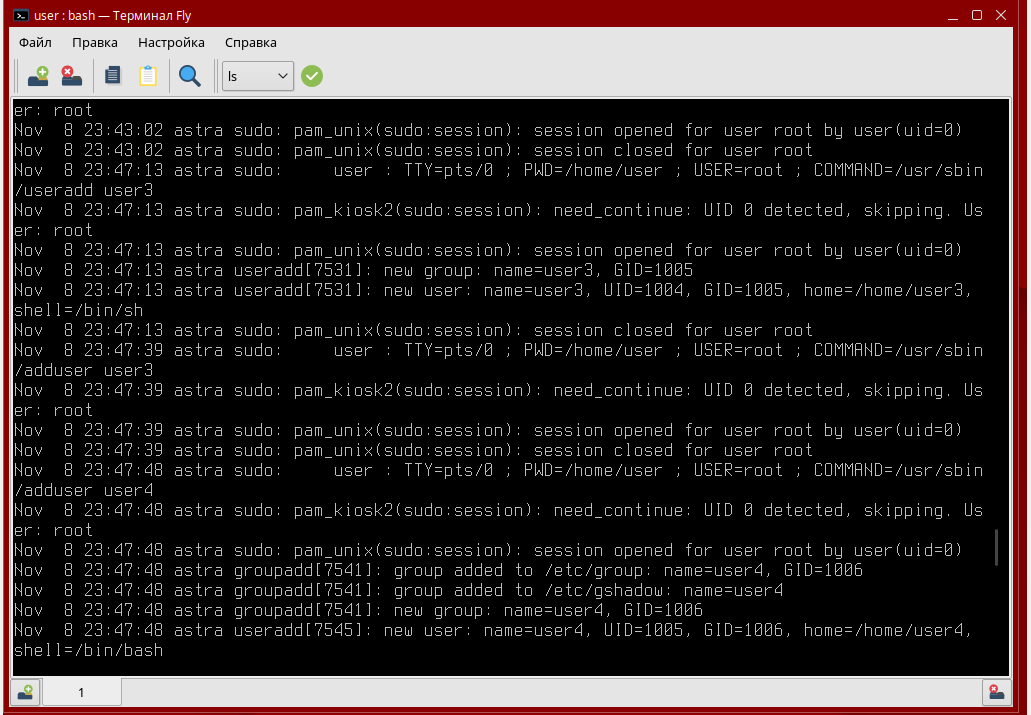
- определить алгоритм свёртки пароля этих учётных записей пользователей по файлу /etc/shadow.



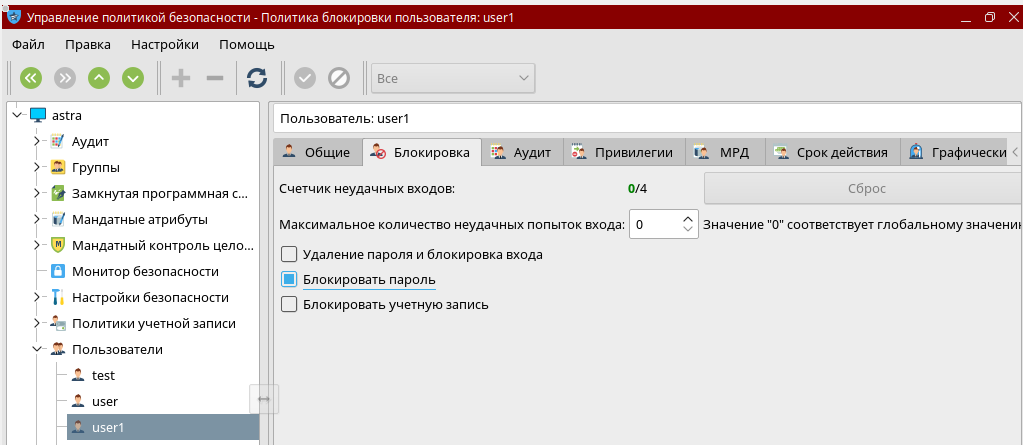
Алгоритм хеширования gost12512hash — это вариант хеширования, основанный на российском криптографическом стандарте ГОСТ Р 34.12-2015, который определяет алгоритм шифрования и хеширования. ГОСТ Р 34.12-2015 описывает алгоритмы на основе блочного шифрования, такие как **СТРИБУТ** (Стандартный Резервный Инструмент для Блочных Удвоенных Таблиц) и **КУЗНЕЧИК**. Алгоритм хеширования на основе ГОСТ-34.12 может называться **ГОСТ-3411-2012** и является частью семейства хеш-функций с высокой степенью безопасности.

С помощью соответствующего системного журнала аудита определить все

записи, касающиеся рассматриваемого события.



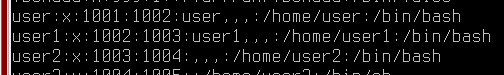
12. С использованием графической утилиты «Политика безопасности» заблокировать пароль учётной записи пользователя user1.



Проверить изменения

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

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

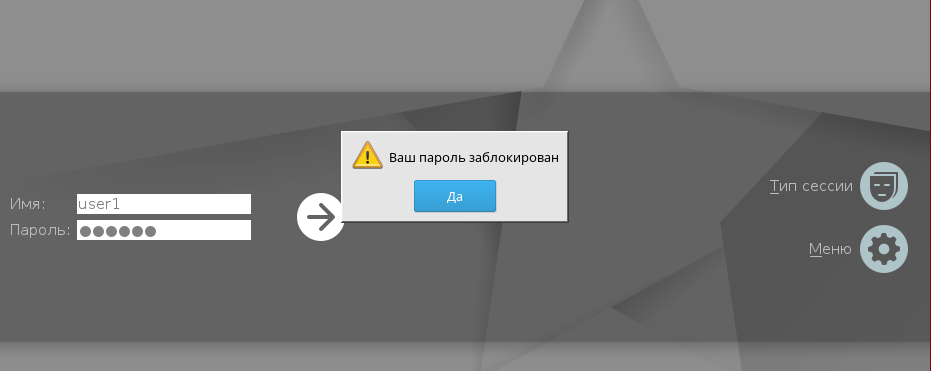


и sudo cat /etc/shadow;

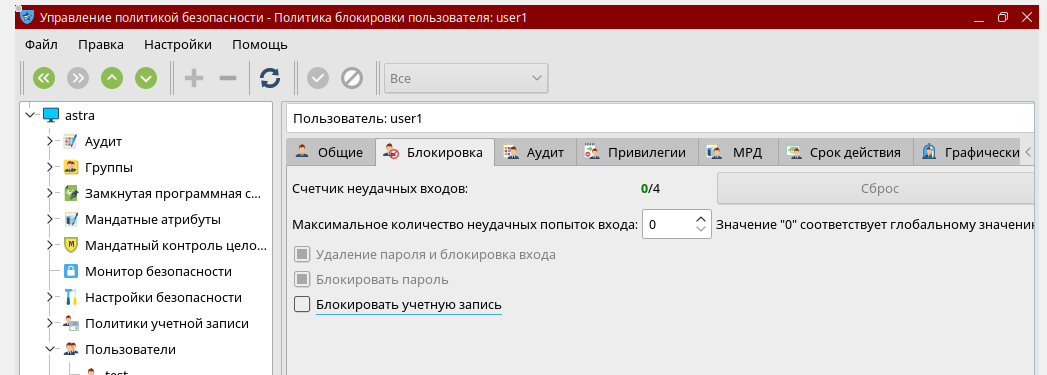


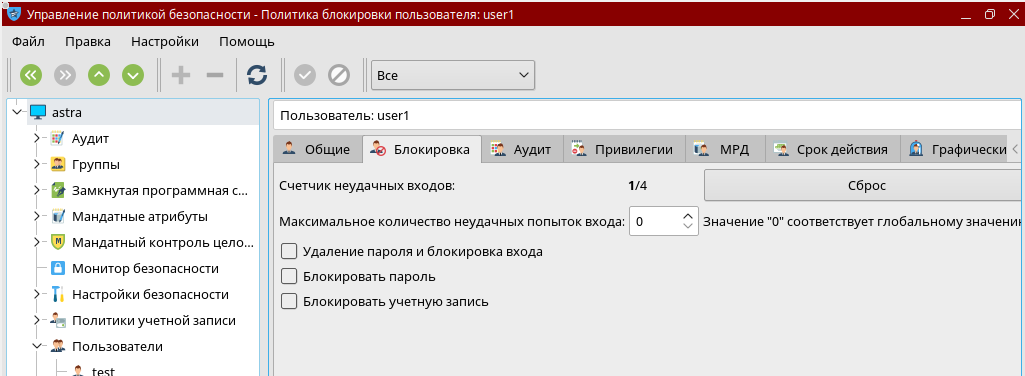
- проверить наличие блокировки учётной записи пользователя по файлу /etc/shadow (должен быть установлен знак «!» в начале свёртки пароля);

- проверить функционирование блокировки путём осуществления попытки входа в ОССН в отдельном сеансе от имени учётной записи пользователя user1;



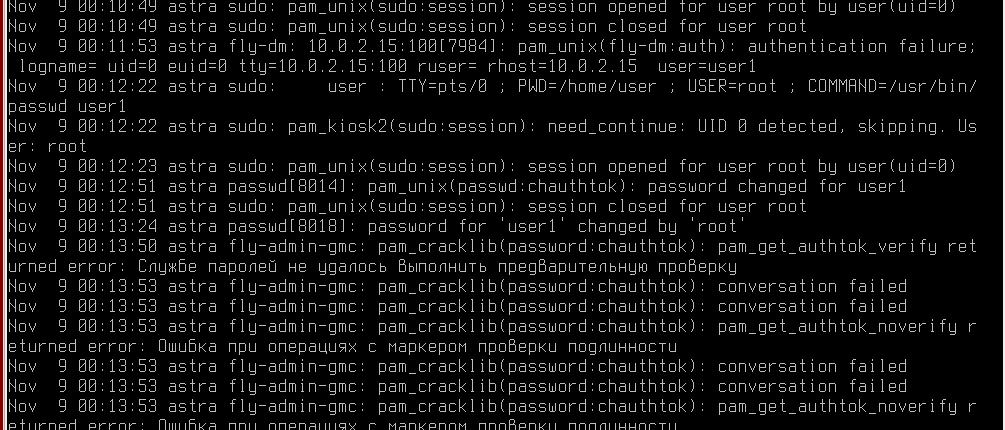
- снять блокировку (выполнить удаление пароля и блокировки входа, задать повторно пароль) и проверить возможность входа в ОССН с учётной записью пользователя user1. после изменения пароля

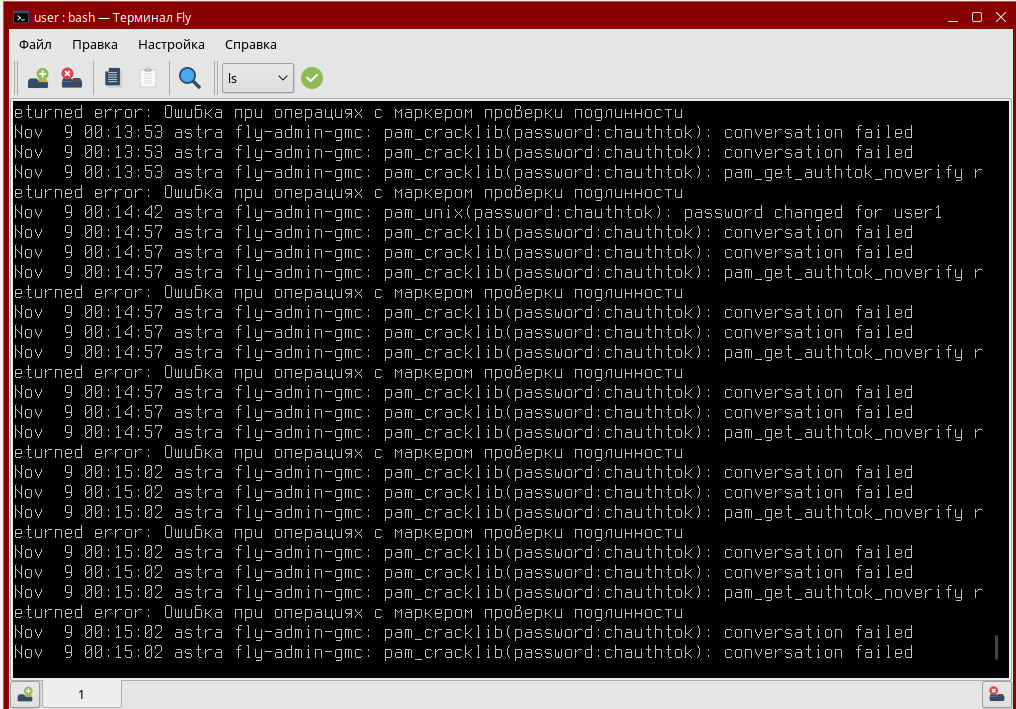




вход получилось осуществить

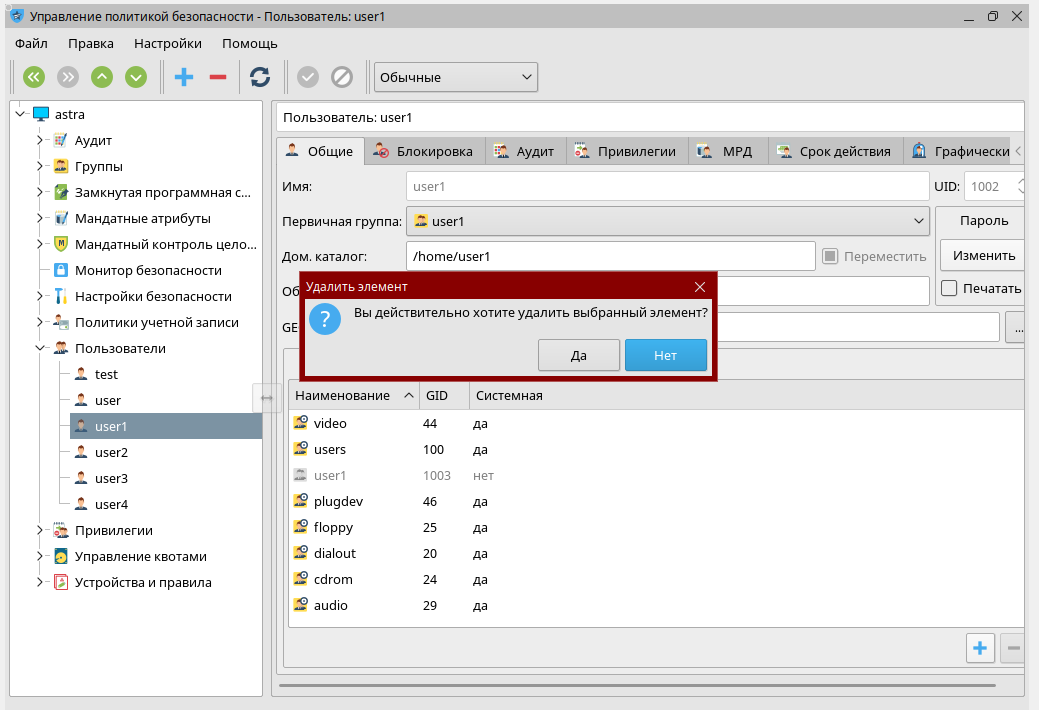
С помощью соответствующего системного журнала аудита определить все записи, касающиеся рассматриваемого события.

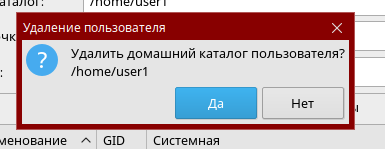




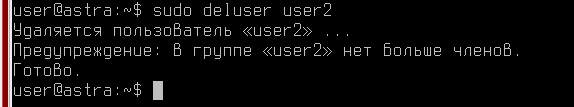
13. Выполнить удаление учётных записей пользователей:

- удалить учётную запись пользователя user1 с использованием графической утилиты «Политика безопасности»;

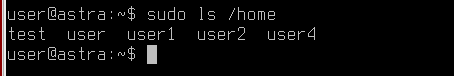




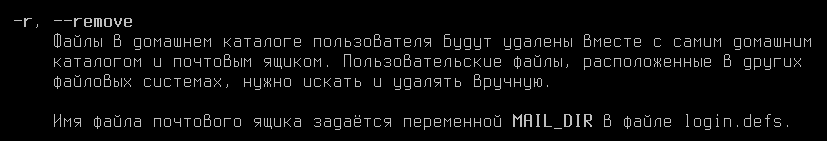
- удалить учётную запись пользователя user2 командой sudo deluser user2;



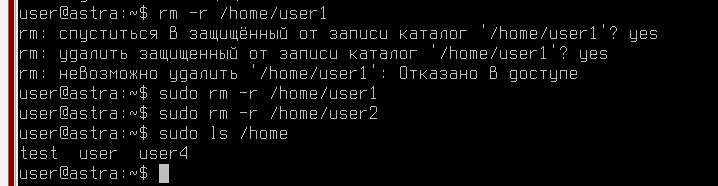
- проверить наличие домашних каталогов учётных записей пользователей user1 и user2, после чего с использованием справочной информации по команде userdel определить её параметры, позволяющие удалять содержимое домашнего каталога учётной записи пользователя;

каталоги остались  


Нужный параметр находим при помощи справки по команде (вызывается при помощи man userdel).

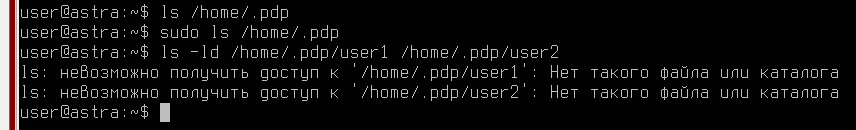


- удалить домашние каталоги учётных записей пользователей user1 и user2 непосредственно командами rm -r /home/userone и rm –r /home/usertwo, осуществив попытки удаления без использования и с использованием команды sudo;



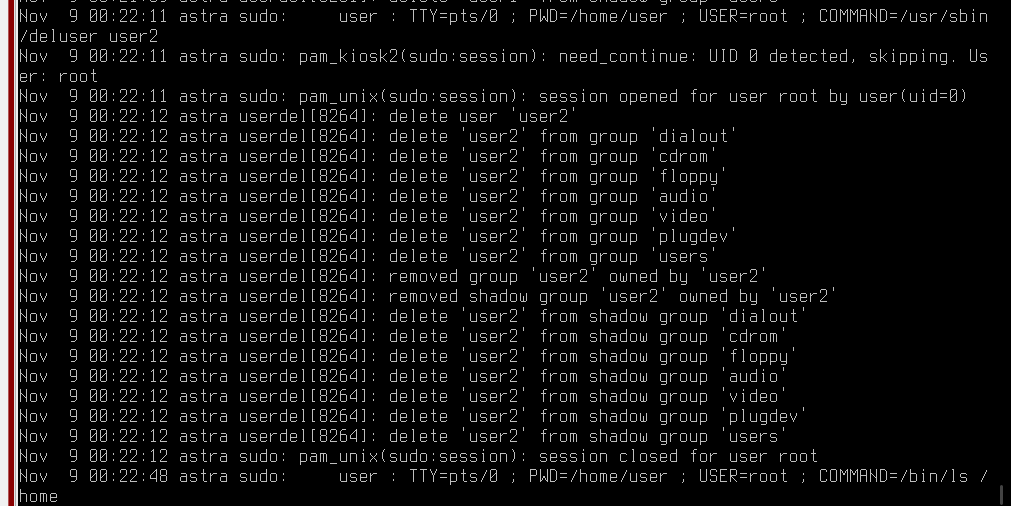
- проверить наличие домашних каталогов учётных записей пользователей user1, user2 в каталоге /home/.pdp.

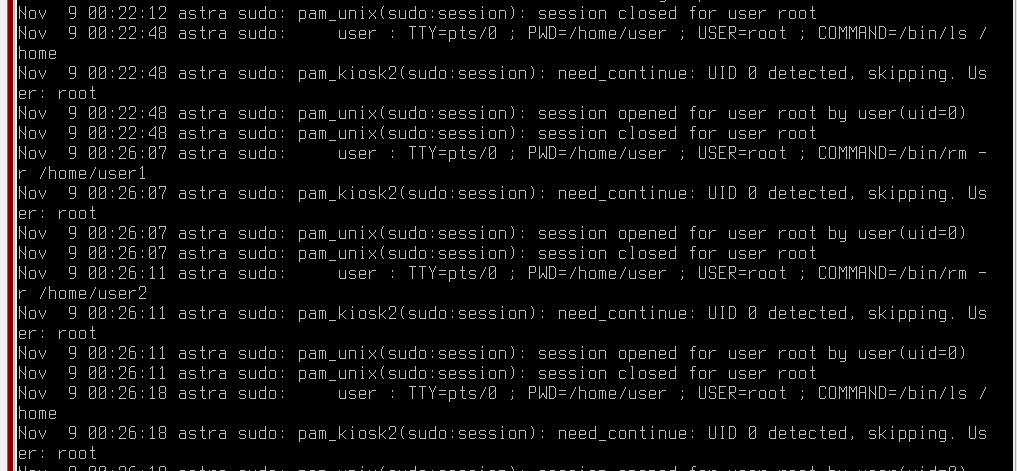
такого каталога нет



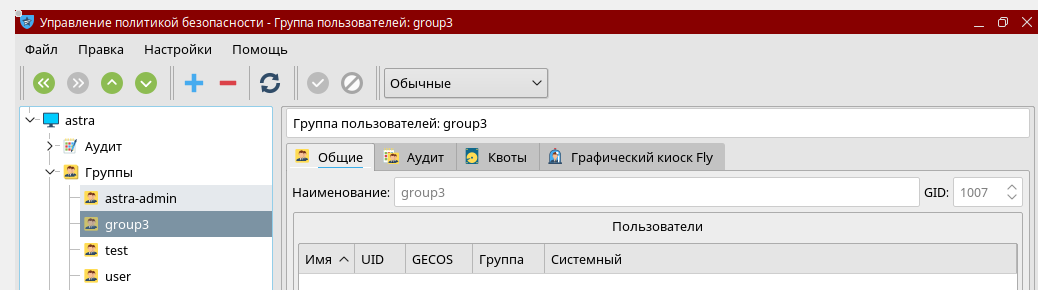
С помощью соответствующего системного журнала аудита определить все записи, касающиеся рассматриваемого события.

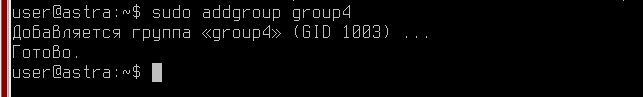






14. Создать новые группу group3 (с использованием графической утилиты «Политика безопасности») и группу group4 (командой sudo addgroup group4, выполненной в терминале Fly).

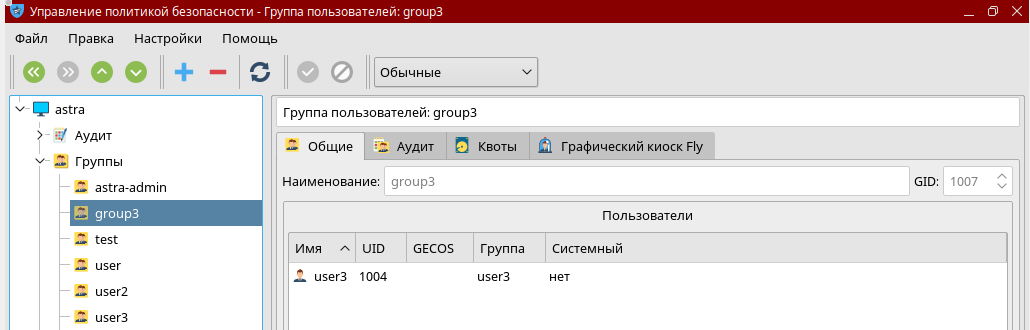




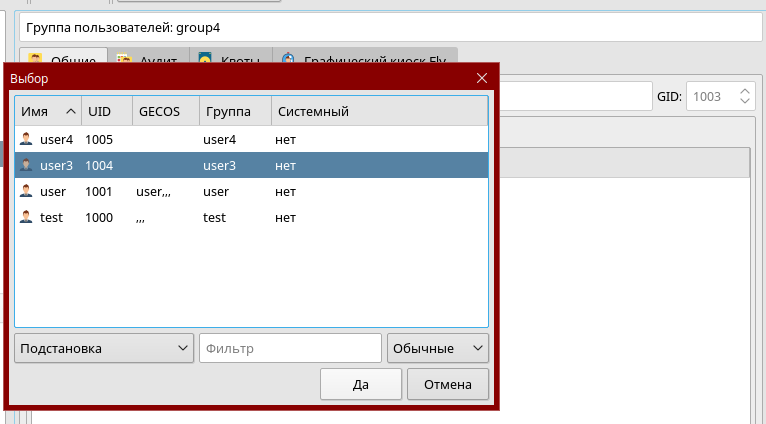
15. Добавить учётную запись пользователя user3 во вторичную группу

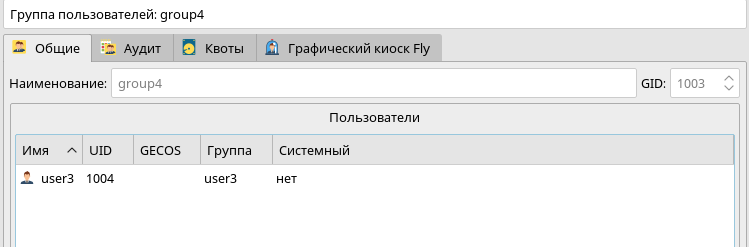
group3 командой usermod -a -G group3 user3



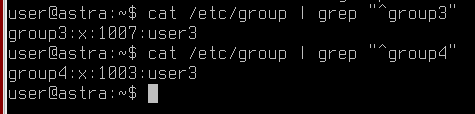


и во вторичную группу group4 с помощью графической утилиты «Политика безопасности».

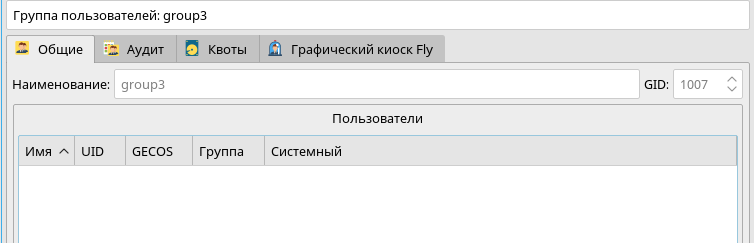




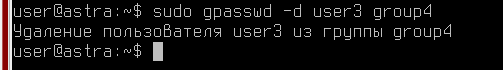
Проверить включение учётной записи пользователя user3 в группы group3 и group4 путем просмотра содержимого файла /etc/group командами cat /etc/group | grep "^group3" и cat /etc/group | grep "^group4".



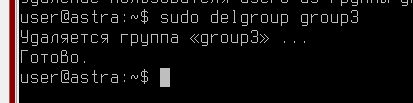
16. Выполнить удаление учётной записи пользователя user3 из группы group3 с использованием графической утилиты «Политика безопасности»



и из группы group4 командой gpasswd -d user3 group4.



17. Удалить группу group3 командой sudo delgroup group3 в терминале Fly



и группу group4 с помощью графической утилиты «Политика безопасности».

