**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 ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: |
| Скляров Алексей Викторович |
| (Фамилия, имя, отчество) |

**Цель:** изучить возможности ОССН Astra Linux Special Edition при администрировании локальных учётных записей пользователей и групп с использованием командной строки и графического интерфейса, конфигурирование политики безопасности.

**Задание 1.** Авторизоваться в ОССН в графическом режиме с учётной записью пользователя user (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).

Для выполнения задания от лица администратора нужно изначально создать учетную запись – user. После этого мы сможем зайти за пользователя “user”, как представлено на рисунке 1.

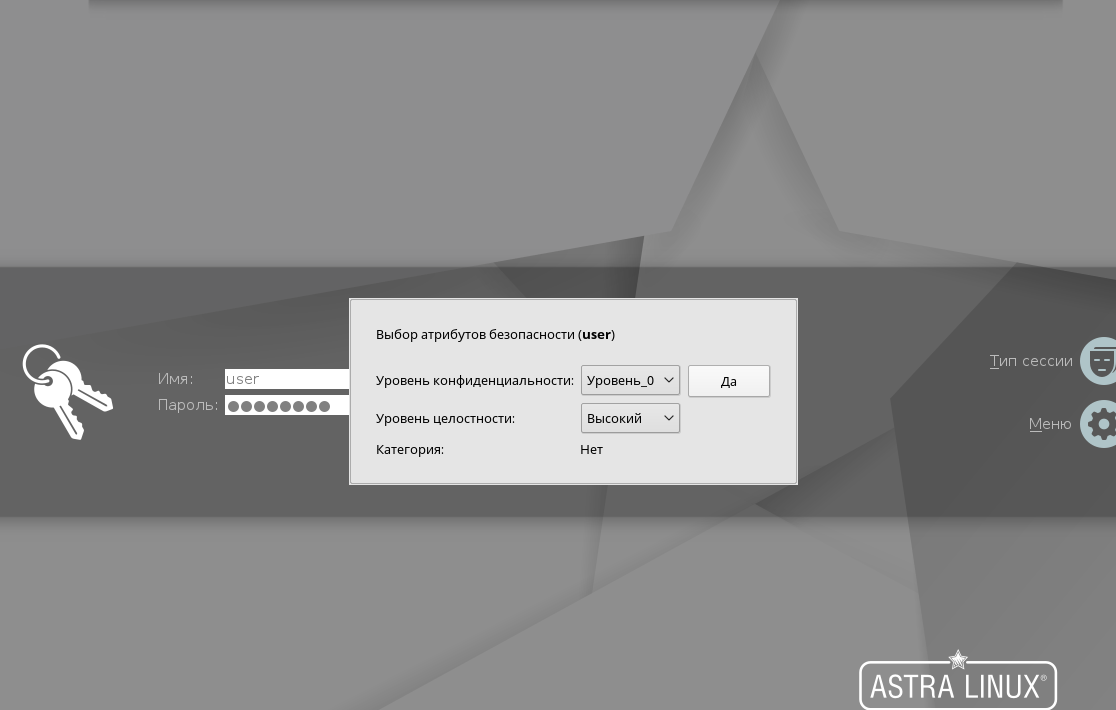


Рисунок 1 – вход в систему от лица user

**Задание 2.** Запустить терминал Fly.

Для запуска можно открыть Пуск и выбрать приложение – Терминал, в итоге у нас откроется такое вот окно, которое представлено на рисунке 2.

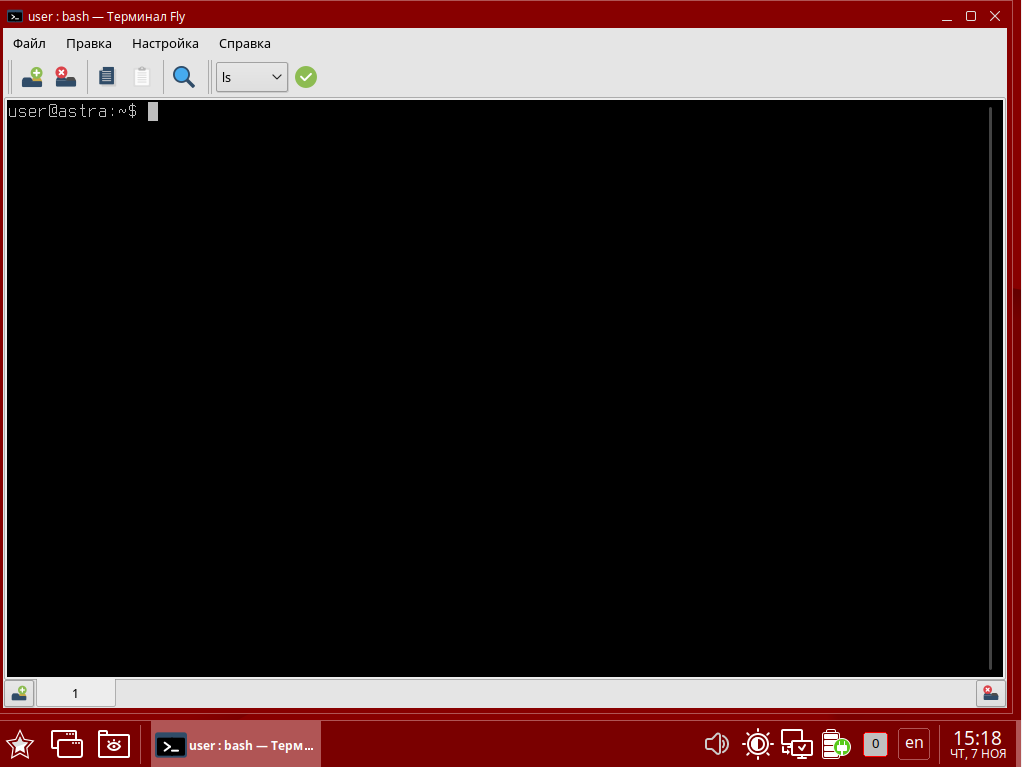


Рисунок 2 – запуск терминала от имени user

**Задание 3.** Определить текущую учётную запись пользователя с использованием команды whoami.

Для выполнения задания нужно просто ввести в терминале команду “whoami”. Результат представлен на рисунке 3.

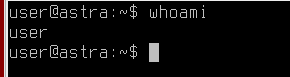


Рисунок 3 – получение информации о текущей сессии пользователя

**Задание 4.** Проверить наличие права доступа на чтение к файлу /etc/passwd и получить следующие данные, выполнив команды cat /etc/passwd или less /etc/passwd.

Для выполнения задания нужно просто вставить команды в терминал, которые предложены по условию задания. В начале проверим доступы к файлу, результат доступа представлен на рисунке 4.

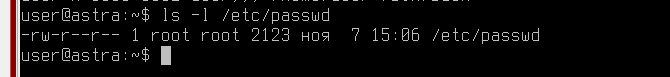


Рисунок 4 – доступы к /etc/passwd

Теперь просмотрим содержимое файла /etc/passwd, используя команду cat. Команда и результат выполнения её представлено на рисунке 5. 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)

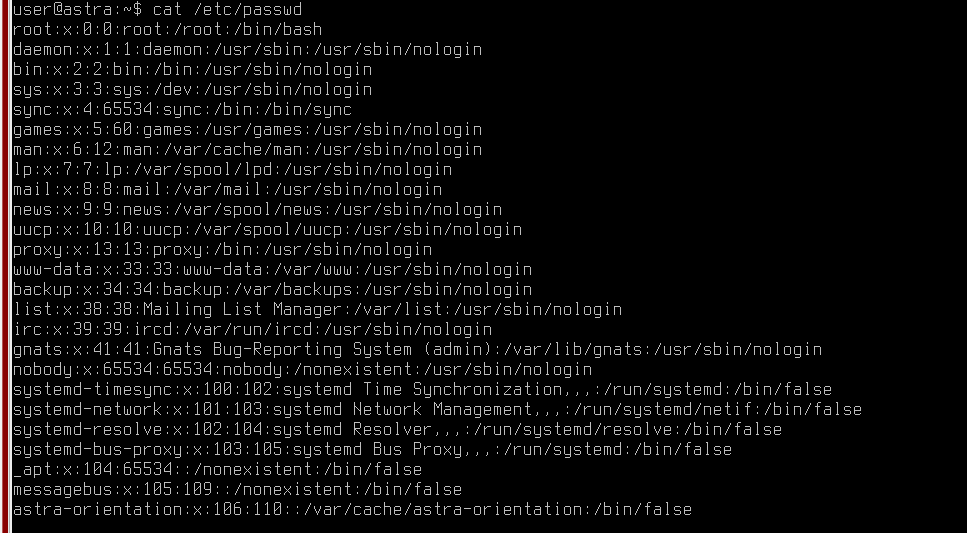


Рисунок 5 – содержимое /etc/passwd

Теперь просмотрим количество параметров учётных записей пользователей. Для выполнения данного пункта нужно использовать команду: “ cat /etc/passwd | head -n 1 | awk -F ':' '{print NF}' ”. Результат представлен на рисунке 6.

Теперь просмотрим количество параметров, совпадающих у всех учётных записей пользователей. Для выполнения данного пункта нужно использовать команду: “ 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}' “. Результат представлен на рисунке 6.

Чтобы узнать текущее число учётных записей пользователей, можно воспользоваться командой: “ cat /etc/passwd | wc -l “. Результат представлен на рисунке 6.

Чтобы узнать количество различных используемых командных интерпретаторов, нужно воспользоваться командой: “ cat /etc/passwd | awk -F ':' '{print $7}' | sort | uniq | wc -l “. Результат выполнения данной команды представлен на рисунке 6.

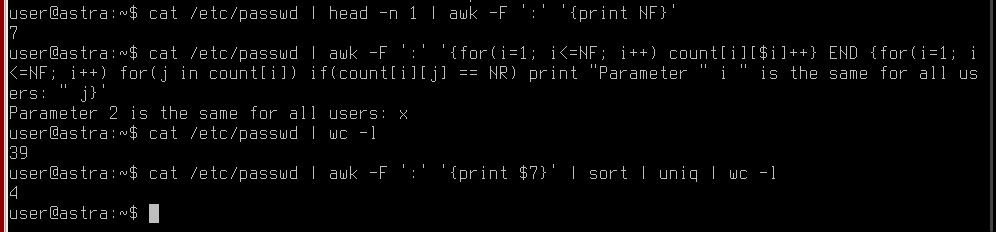


Рисунок 6 – выполнение всех команд для задания 4

**Задание 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), группа и идентификатор текущей учётной записи пользователя, командный интерпретатор по умолчанию для текущей учётной записи пользователя.

Проверим наличие пароля или свёртки пароля. Для этого воспользуемся командой: “ cat /etc/passwd | grep "^$(whoami)" | cut -d : -f 2 “. Результат представлен на рисунке 7.

Теперь узнаем группу и идентификатор текущей учётной записи пользователя. Для этого воспользуемся командой: “ cat /etc/passwd | grep "^$(whoami)" | cut -d : -f 3,4 “. Результат выполнения команды представлен на рисунке 7.

Теперь узнаем командный интерпретатор по умолчанию для текущей учётной записи. пользователя. Для этого нужно выполнить команду: “ cat /etc/passwd | grep "^$(whoami)" | cut -d : -f 7 “. Результат выполнения команды представлен на рисунке 7.

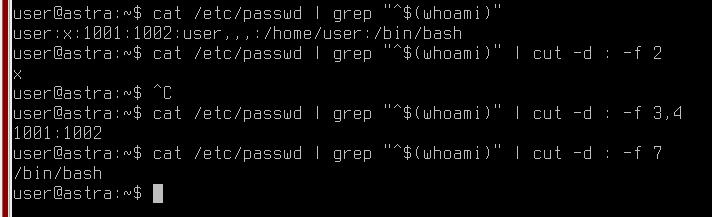


Рисунок 7 – результат выполнения команд

**Задание 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).

Через пуск открываем приложение “Управление политикой безопасности”, выбираем политики учетной записи, а потом выставляем параметр, как представлено на рисунке 8. Нам нужно сделать так, чтобы каждый пользователь мог входить под своим аккаунтом.

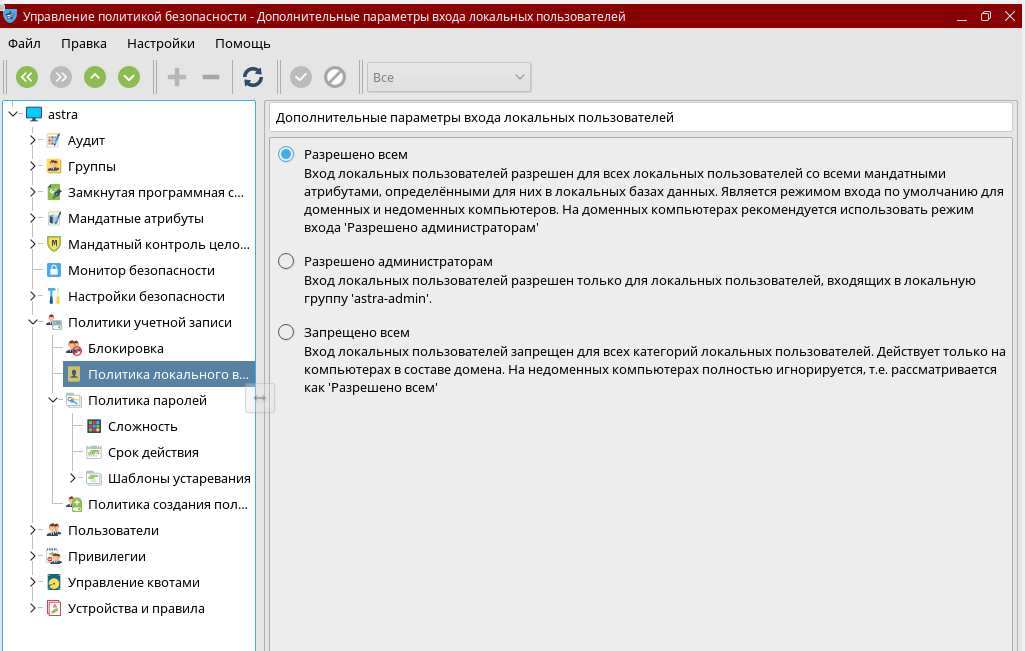


Рисунок 8 – параметры для входа каждого пользователя

Теперь перейдем к политике паролей. Здесь нам нужно выставить параметры согласно заданию. Конфигурация представлена на рисунке 9.

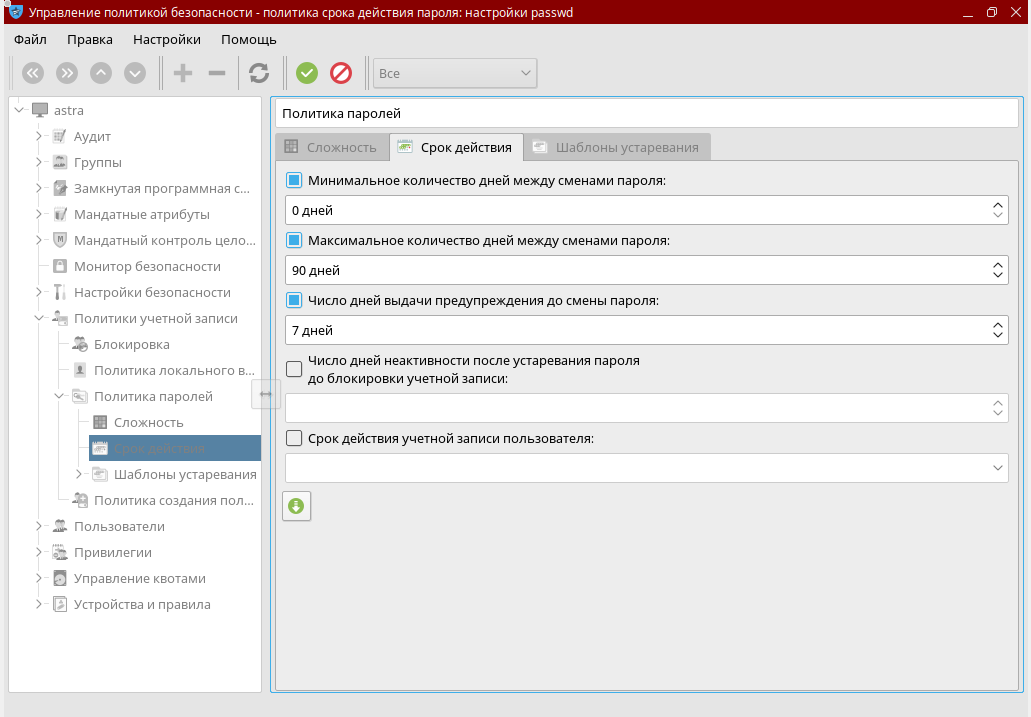


Рисунок 9 – настройка политики паролей

Теперь перейдем к политики сложности паролей. Конфигурация для выполнения задания представлена на рисунке 10.

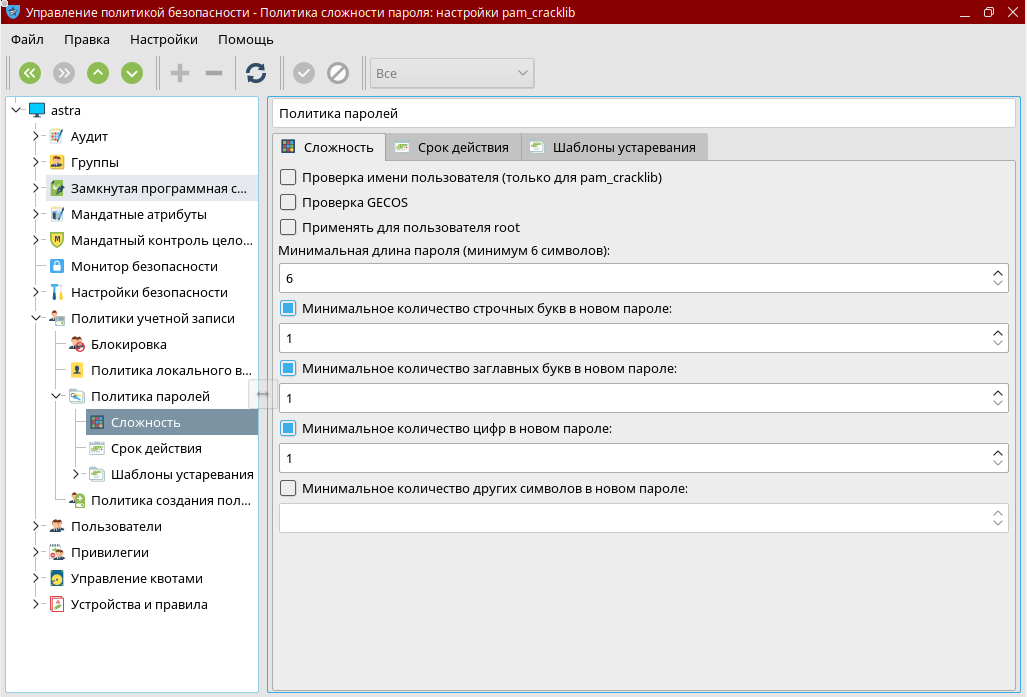


Рисунок 10 – настройка сложности пароля

Теперь перейдем к настройке блокировки при неудачный попытках входа. Результат настройки представлен на рисунке 11.

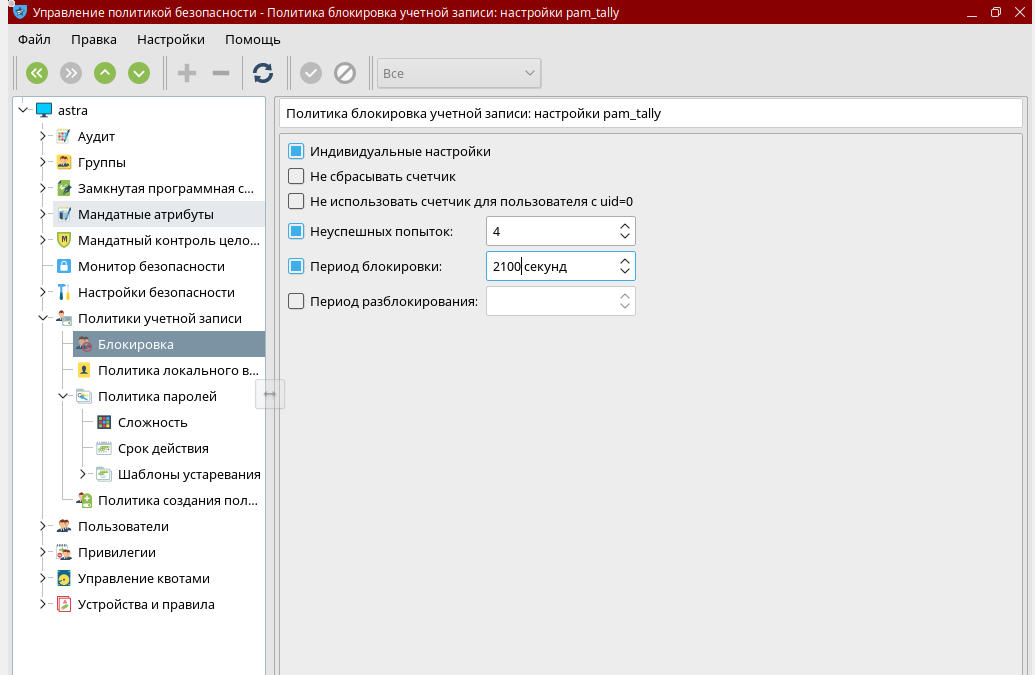


Рисунок 11 – настройка политик блокировки

**Задание 7.** Создать учётную запись пользователя userl (с соответствующим домашним каталогом) с использованием графического интерфейса, установить пароль, соответствующий требованиям политики информационной безопасности.

Для создания пользователя нужно опять-таки открыть приложение “управление политикой безопасности”, после чего заполнить данные, как представлено на рисунке 12.

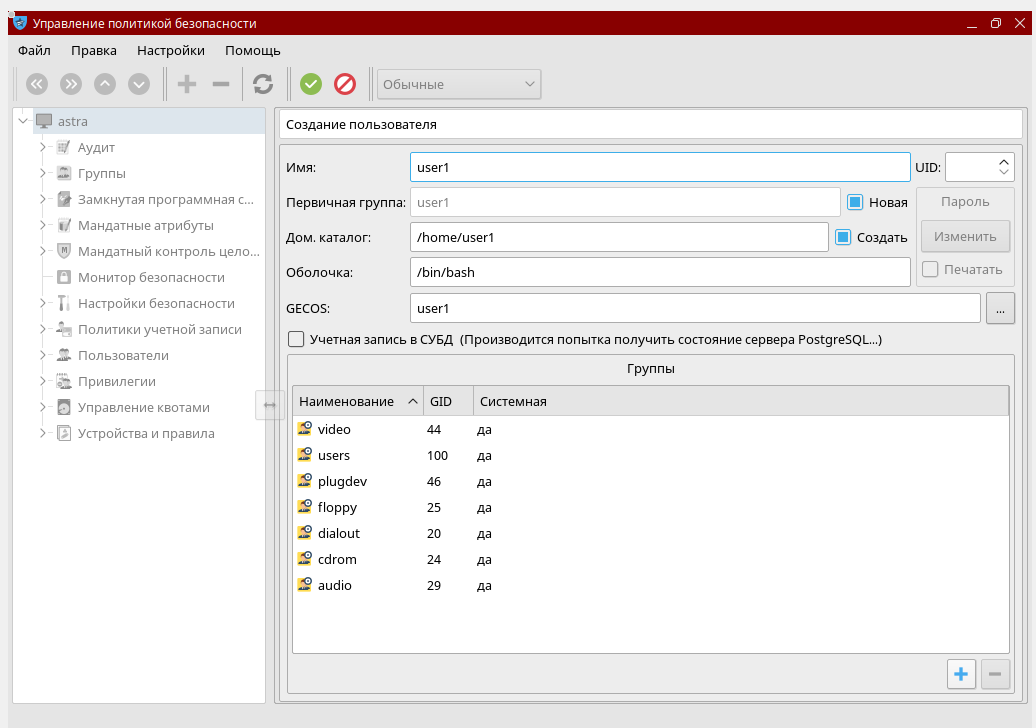


Рисунок 12 – создание пользователя

Теперь также от лица администратора обновим пароль, результат представлен на рисунке 13.

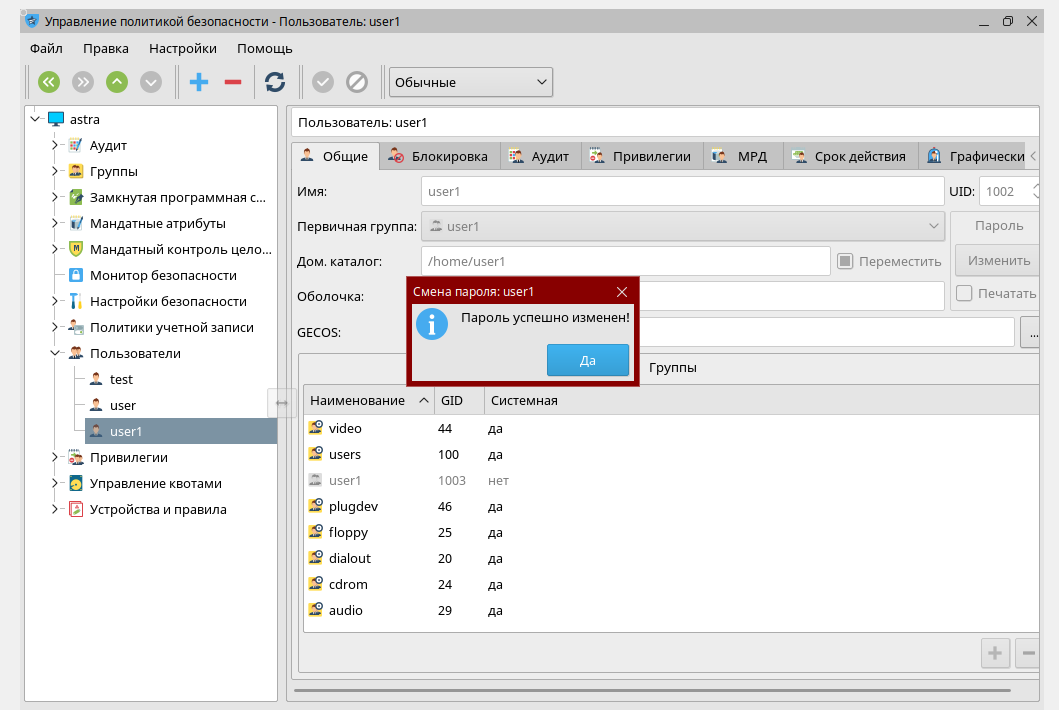


Рисунок 13 – установка пароля для нового пользователя

Теперь с помощью системного журнала определим все записи, которые говорят нам о том, что новый пользователь был создан. Для выполнения этого нужно воспользоваться командой: “ less /var/log/auth.log *“*, результат выполнения команды представлен на рисунке 14.

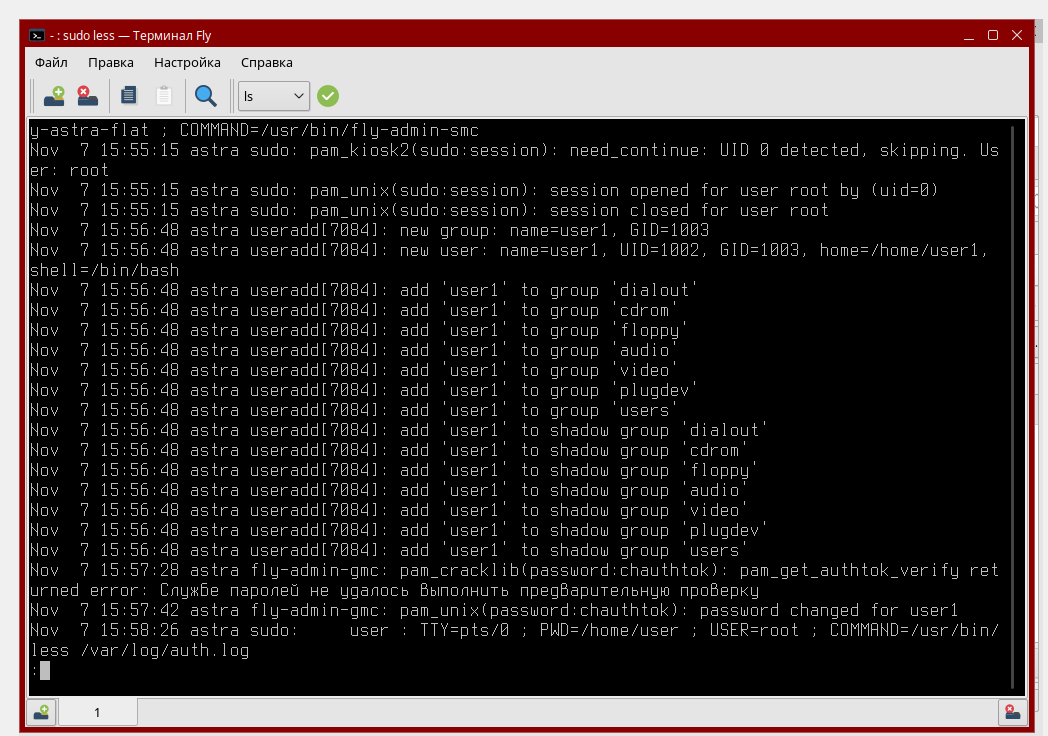


Рисунок 14 – логи о создании нового пользователя

**Задание 8.** Добавить учётную запись пользователя user2 с использованием команды adduser user2, без использования команды sudo, проанализировать и объяснить результат. Установить учётной записи пользователя user2 пароль, соответствующий требованиям политики информационной безопасности. С помощью системного журнала /var/log/auth.log определить все записи, касающиеся рассматриваемого события.

В других дистрибутивах Linux обычно пишется permission denied, в случае Astra Linux пишется, что команда не найдено. Скорее всего это сделано с целью повышения безопасности, но решение сомнительное. Результат выполнения без sudo представлено на рисунке 15.



Рисунок 15 – создание нового пользователя

Теперь попробуем выполнить те же действия с применением команды sudo. Нам нужно установить учётной записи пользователя user2. пароль, соответствующий требованиям политики информационной безопасности. Результат выполнения представлен на рисунке 16.

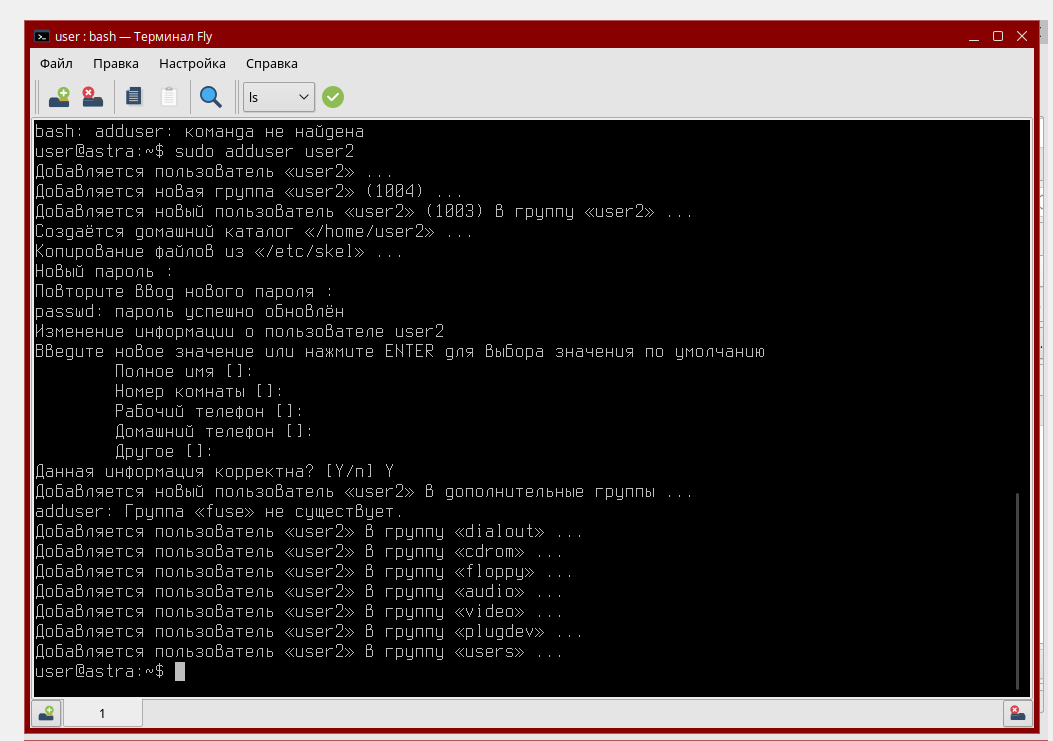


Рисунок 16 – выполнение команды adduser c правами sudo

Теперь с помощью системного журнала просмотрим все логи о создании нового пользователя. Для этого нужно выполнить команду: “ less /var/log/auth.log “. Содержимое журнала и команда представлена на рисунке 17.

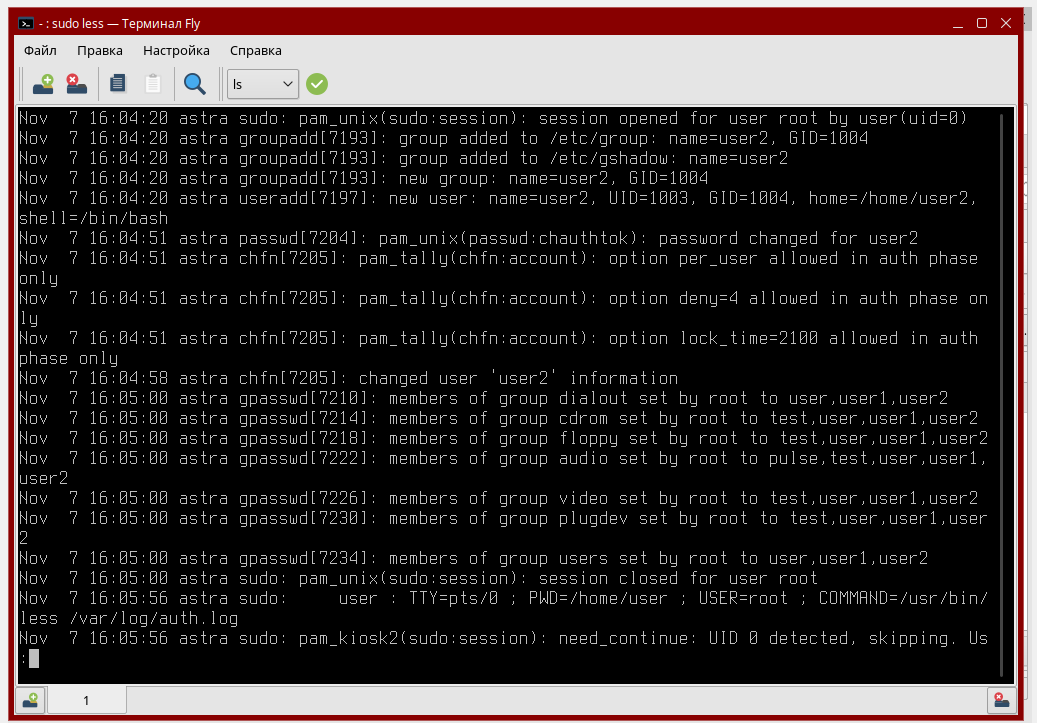


Рисунок 17 – содержимое журнала при создании пользователя с sudo

**Задание 9.** Проанализировать изменения в ОССН, связанные с добавлением новых учётных записей пользователей, для чего определить: домашние каталоги учётных записей пользователей по данным файла; содержимое файла /etc/shadow; алгоритм хеширования пароля, используемый в ОССН; 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 -s /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.

Просмотрим теперь изменения, которые произошли в системе. Самое простое – это посмотреть как поменялись права и записи в файле /etc/passwd. Для просмотра содержимого можно использовать команду: “ Less /etc/passwd; “. В нашем случае вышло то, что представлено на рисунке 18.

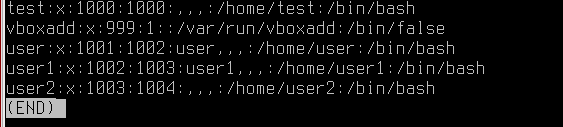


Рисунок 18 – содержимое файла /etc/passwd

Теперь перейдем к просмотру содержимого файла /etc/shadow. Для этого нужно выполнить команду: “less /etc/shadow”. Результат выполнения команды представлен на рисунке 19.

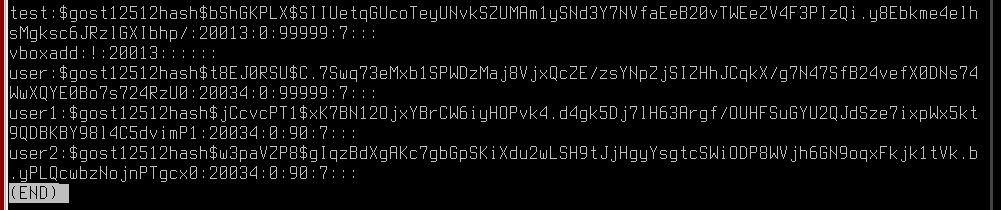


Рисунок 19 – результат просмотра /etc/shadow

Алгоритм хеширования в Astra Linux - 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.

Теперь посмотрим на 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”. Результат выполнения команды представлен на рисунке 20.

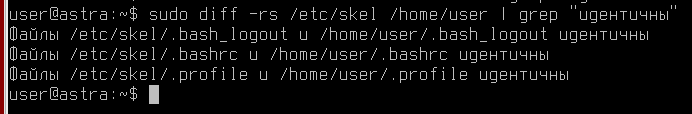


Рисунок 20 – сравнение файлов

Теперь просмотрим новые группы в файле /etc/group, для этого нужно выполнить команду “less /etc/group”. Результат выполнения команды представлен на рисунке 21.

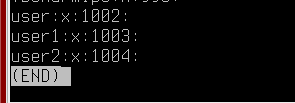


Рисунок 21 – просмотр новых групп

В нашем случае идентификаторы новых учётных записей пользователей и групп в файлах/etc/group и /etc/passwd: user1- 1003, user2 – 1004.

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

Для создания пользователей через графический интерфейс нужно через пуск открыть “Управление политикой безопасности”.

**Задание 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, 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; новые группы в файле /etc/group; идентификаторы новых учётных записей пользователей в файле /etc/passwd; командный интерпретатор по умолчанию для созданных учётных записей пользователей, используя команду: tail -1 /etc/passwd|cut -d: -f7; определить алгоритм свёртки пароля этих учётных записей пользователей по файлу /etc/shadow. С помощью соответствующего системного журнала аудита определить все записи, касающиеся рассматриваемого события.

Если попробовать выполнить без sudo, то выдаст ошибку доступа, как представлено на рисунке 22. Если пробовать с sudo от имени администратора, то все будет работать как часы.

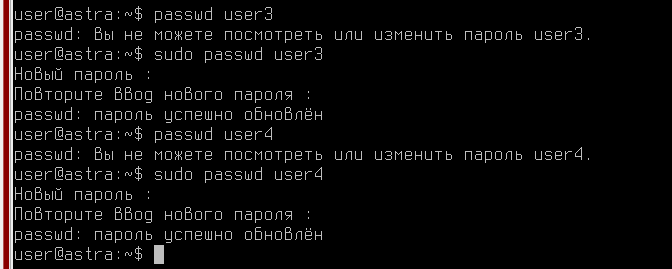


Рисунок 22 – смена паролей для пользователей

Теперь узнаем какие домашние каталоги используются для учётных записей пользователей по файлу /etc/passwd. Для этого нужно выполнить команду: “ less /etc/passwd “. Результат выполнения команды представлен на рисунке 23.

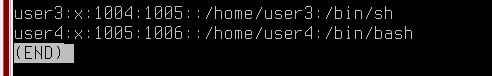


Рисунок 23 – домашние каталоги для учетных записей user3, user4

Теперь просмотрим 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 храниться в файле /etc/passwd, но это не соответсвует современным стандартам безопасности. Видим, что вместо пароля стоит x, значит пароль хранится в файле /etc/shadow. На рисунке 24 как раз представлено то, что пароль не видно.

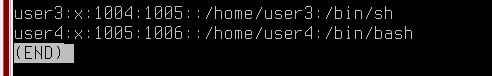


Рисунок 24 – сокрытие пароля пользователя

Теперь просмотрим хэши паролей, которые хранятся в /etc/shadow. Опять-таки в терминале нужно выполнить команду: “less /etc/shadow”. Результат выполнения команды представлен на рисунке 25.

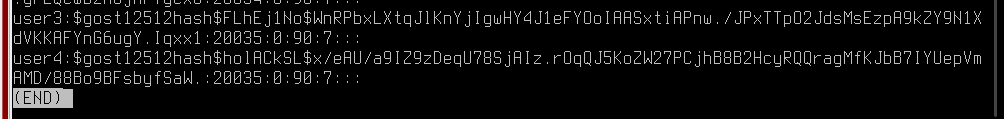


Рисунок 25 – вывод хэшей с /etc/shadow

Теперь просмотрим новые группы в файле /etc/group. Результат выполнения команды представлен на рисунке 26.

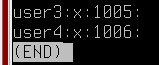


Рисунок 26 – содержимое /etc/group

Идентификаторы новых учётных записей пользователей в файле /etc/passwd: user3 – 1005, user4 -1006.

Теперь просмотрим командный интерпретатор по умолчанию для созданных учётных записей пользователей, используя команду: tail -1 / /passwd|cut -d: -f7. Результат выполнения команды представлен на рисунке 27.

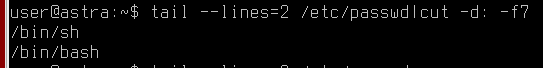


Рисунок 27 – просмотр командных интерпретаторов для новых пользователей

Определим теперь алгоритм свёртки пароля этих учётных записей пользователей по файлу /etc/shadow. Для просмотра нужно использовать команду: “less /etc/shadow”. Результат выполнения команды представлен на рисунке 28.

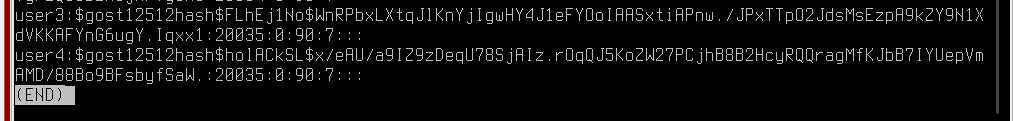


Рисунок 27 – содержимое /etc/shadow

Теперь с помощью соответствующего системного журнала аудита нам нужно определить все записи, касающиеся рассматриваемого события. Для выполнения данного пункта воспользуемся командой: “ less /var/log/auth.log “. В результате получилось то, что представлено на рисунке 28.

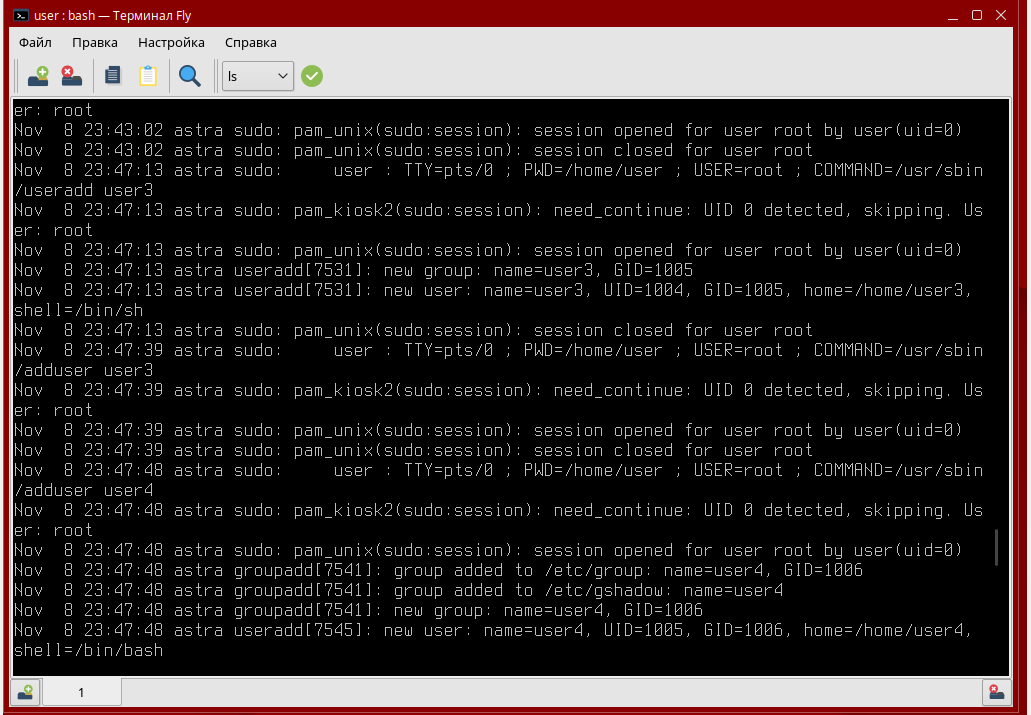


Рисунок 28 – просмотр журнала о создании нового пользователя

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

Через пуск откройте приложение “Политика безопасности”. Блокировка пользователя user1 представлена на рисунке 29.

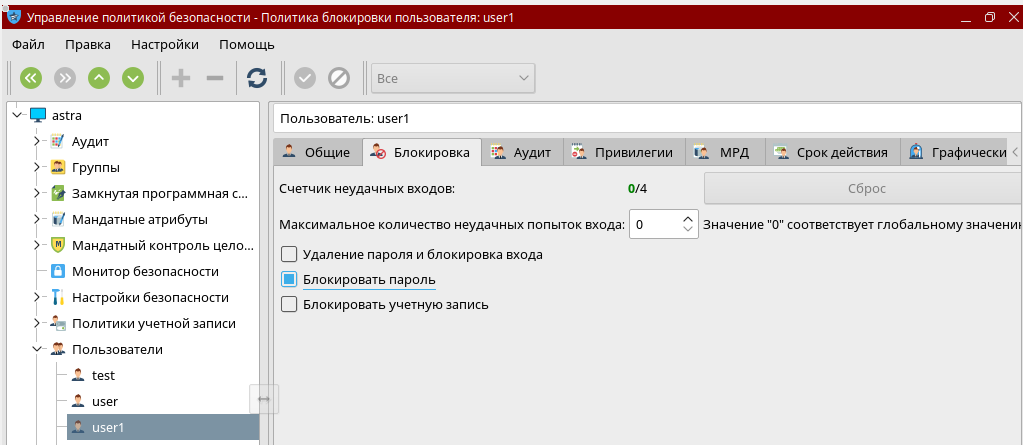


Рисунок 29 – блокировка пользователя user1

Теперь проверим изменения файлов /etc/passwd и /etc/shadow, осуществив следующие действия в терминале. Для начала просмотрим содержимое /etc/passwd, используя команду sudo cat /etc/passwd. В результате произошло то, что представлено на рисунке 30.

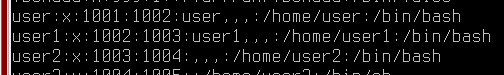


Рисунок 30 – просмотр содержимого /etc/passwd после блокировки пользователя

Теперь просмотрим содержимое /etc/shadow. Для этого воспользуемся командой: “sudo cat /etc/shadow;”. Результат выполнения представлен на рисунке 31.



Рисунок 31 – просмотр /etc/shadow после блокировки пользователя

Теперь проверим функционирование блокировки путём осуществления попытки входа в ОССН в отдельном сеансе от имени учётной записи пользователя user1. Результат представлен на рисунке 32.

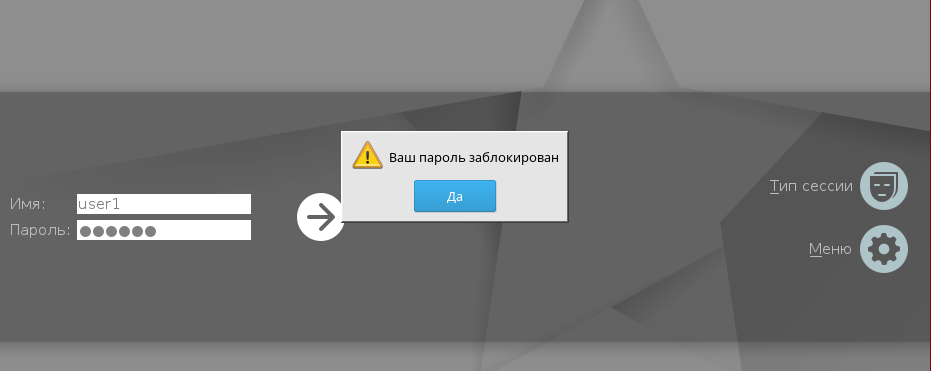


Рисунок 32 – попытка входа за пользователя user1 в ОССН

Теперь нам нужно снять блокировку (выполнить удаление пароля и блокировки входа, задать повторно пароль) и проверить возможность входа в ОССН с учётной записью пользователя user1. От лица администратора открываем “Политику безопасности” и убираем галочку с блокировки пользователя, как представлено на рисунке 33.

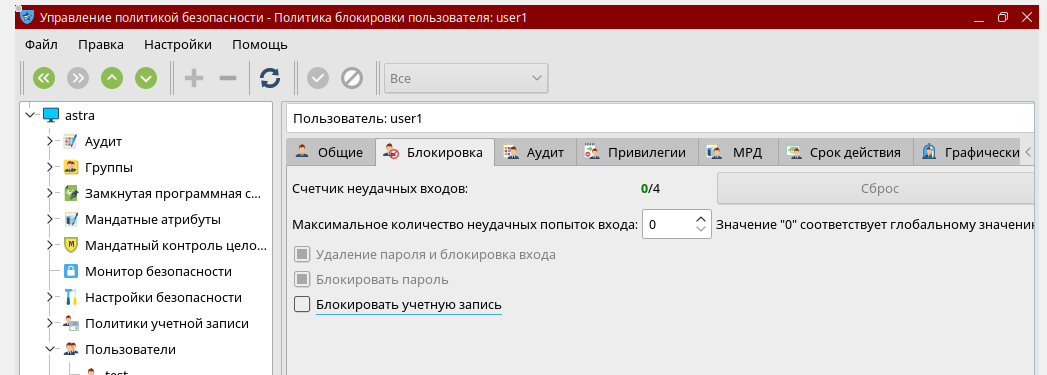


Рисунок 33 – разблокировка пользователя user1

Теперь разблокируем пароль, как представлено на рисунке 34.

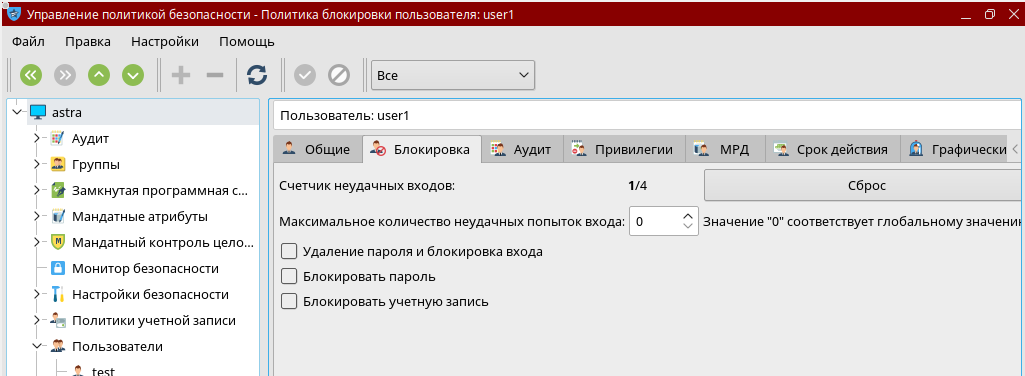


Рисунок 34 – разблокировка пароля

После изменения пароля вход получилось осуществить. Теперь с помощью соответствующего системного журнала аудита нам нужно определить все записи, касающиеся рассматриваемого события. Содержимое журнала после разблокировки пользователя представлено на рисунках 35, 36.

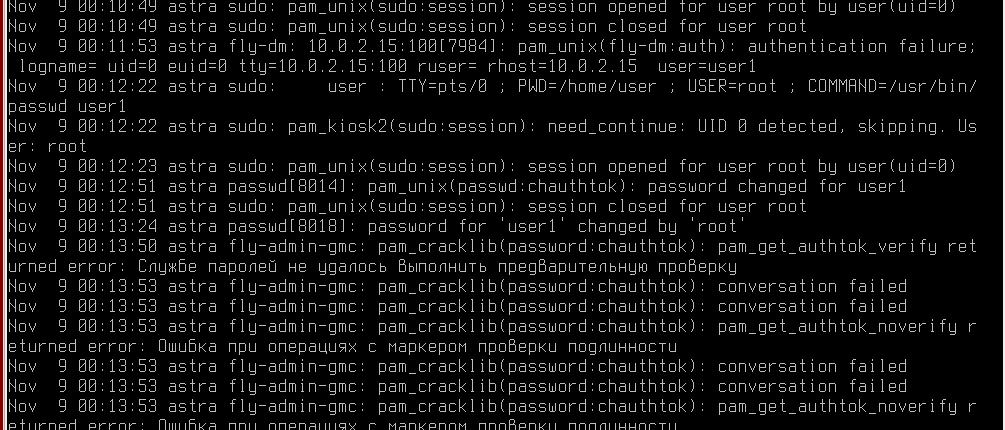


Рисунок 35 – журнал при разблокировке пользователя

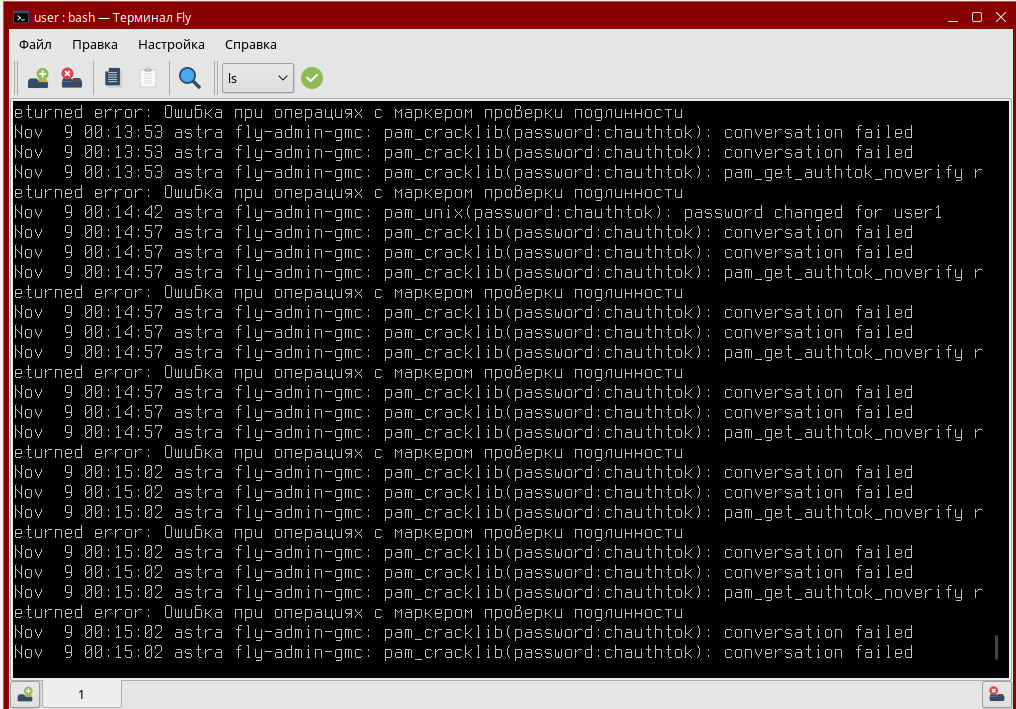


Рисунок 36 – журнал при разблокировке пользователя

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

Теперь перейдем к удалению пользователей. Воспользуемся приложением “Управление политикой безопасности”. Удаление пользователя представлено на рисунке 37.

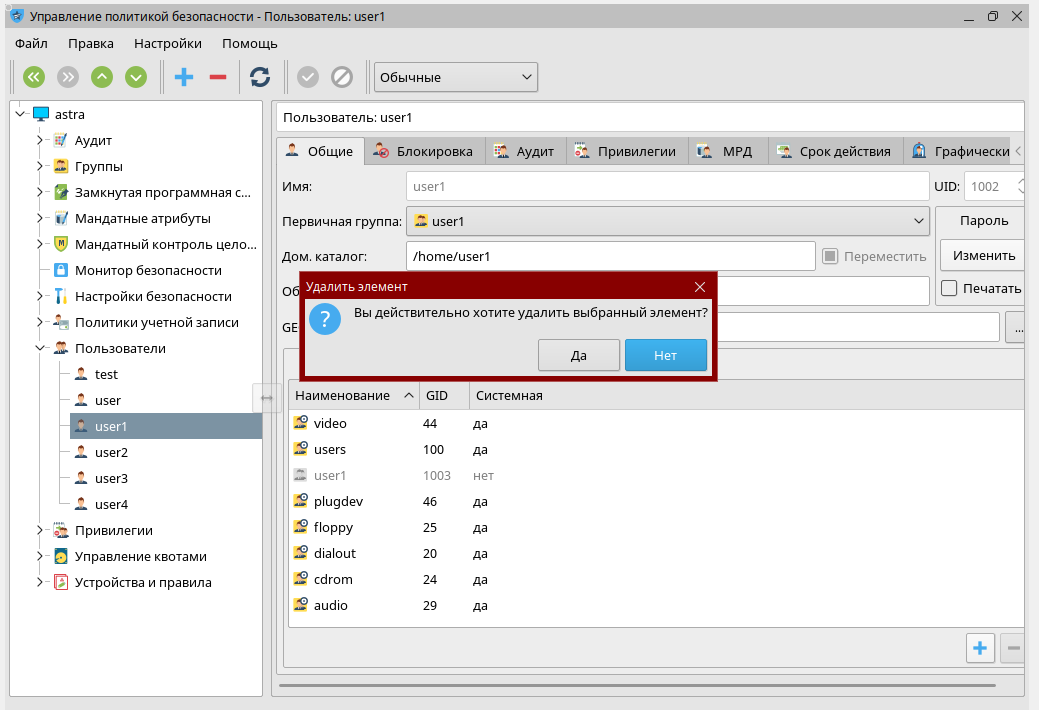


Рисунок 37 – удаление пользователя через графический интерфейс

После удаления пользователя остается его каталог, который потом приходится тоже вручную удалять. Процесс удаления каталога пользователя представлен на рисунке 38.

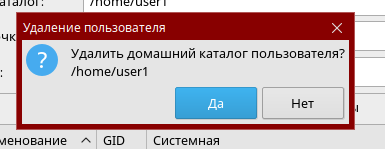


Рисунок 38 – удаление домашнего каталога пользователя

Теперь удалим учётную запись пользователя user2 командой sudo deluser user2. Выполнять данное действие опять-таки нужно от имени нашего user или администратора системы. Результат выполнения команды представлен на рисунке 39.

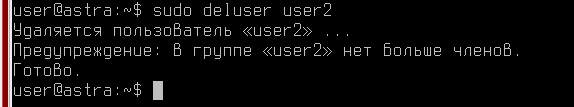


Рисунок 39 – удаление пользователя через терминал

Теперь проверим наличие домашних каталогов учётных записей пользователей user1 и user2. Для этого надо воспользоваться командой “sudo ls /home”. Результат выполнения команды представлено на рисунке 40.

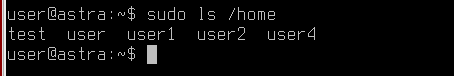


Рисунок 40 – просмотр содержимого домашнего каталога

Теперь поищем нужный параметр, который удаляет также домашние каталоги пользователя. Для этого нужно воспользоваться командой: “man userdel”. Результат выполнения представлен на рисунке 41.

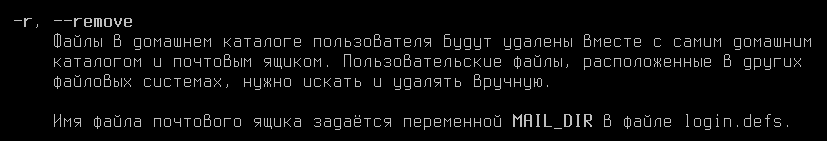


Рисунок 41 – флаг для удаления домашних каталогов пользователя

Теперь удалим 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. Результат выполнения представлено на рисунке 41.

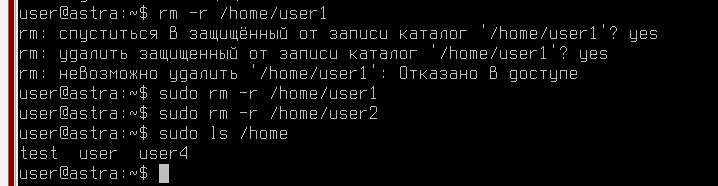


Рисунок 41 – удаление домашних каталогов пользователей

Теперь проверим наличие домашних каталогов учётных записей пользователей user1, user2 в каталоге /home/.pdp. Для выполнения данного пункта воспользуемся командами, которые представлены на рисунке 42. Видим, что такого каталога нет.

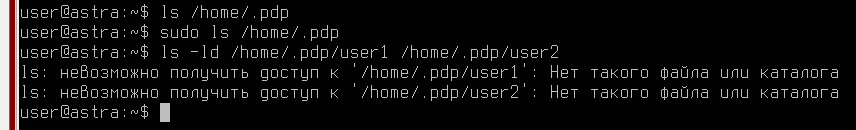


Рисунок 42 – просмотр содержимого каталога /home/.pdp

С помощью соответствующего системного журнала аудита определим все записи, касающиеся рассматриваемого события. Содержимое системных журналов представлено на рисунках 43, 44, 45.



Рисунок 43 – журнал при удалении пользователей

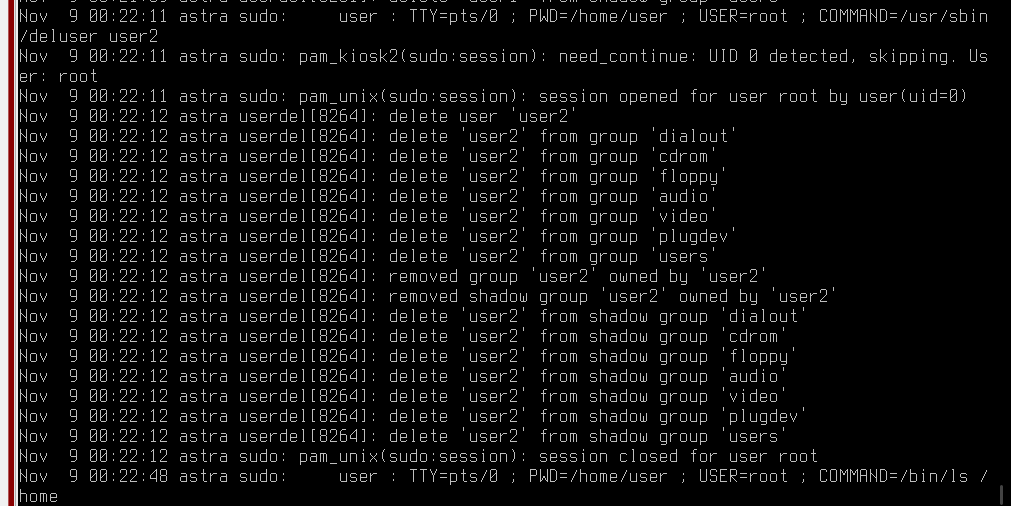


Рисунок 44 – журнал при удалении пользователей

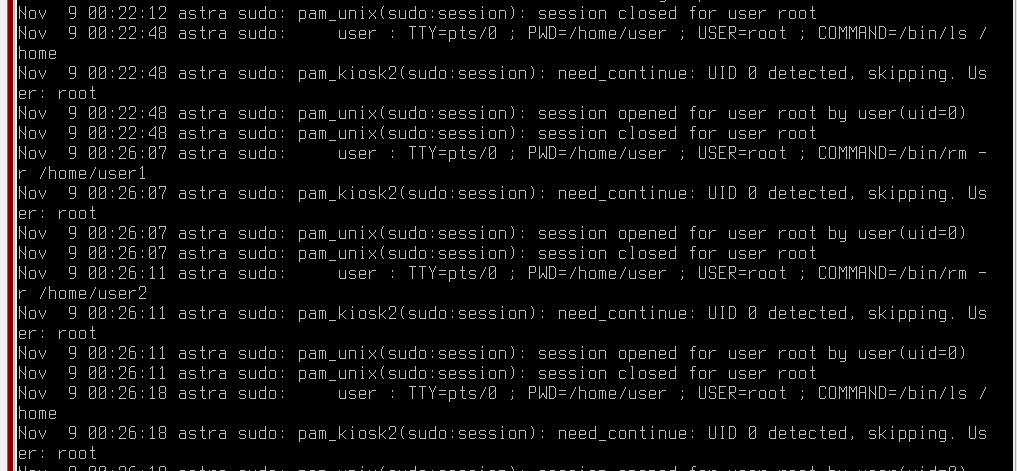


Рисунок 45 – журнал при удалении пользователей

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

Через пуск нужно открыть “политика безопасности”, выбираем Группы, ПКМ и будет кнопка для создания группы. Новая group3 представлена на рисунке 46.

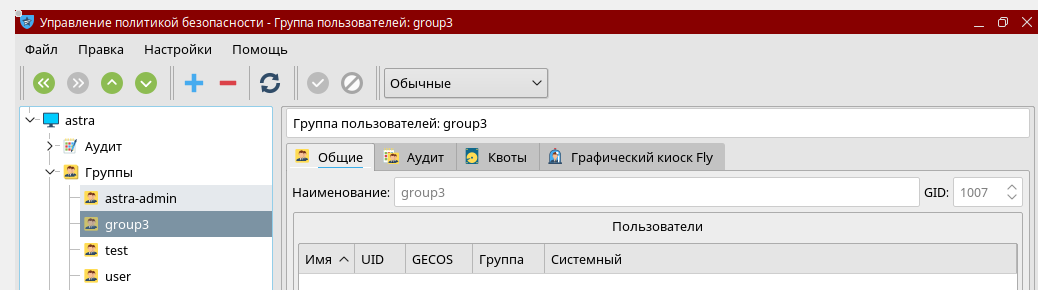


Рисунок 46 – group3 при создании через GUI

Теперь попробуем создать через терминал новую группу – “group4”. В результате получится то, что представлено на рисунке 47.

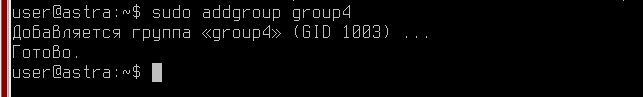


Рисунок 47 – создание новой группы через терминал

**Задание 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".

Для добавления пользователя user3 в группу group3 воспользуемся командой, которая предложена по условию задания. На рисунке 48 представлено выполнение данной команды в терминале.



Рисунок 48 – добавление пользователя в новую группу

Просмотрим теперь через графический интерфейс, что пользователь удачно добавился в новую группу. Результат представлен на рисунке 49.

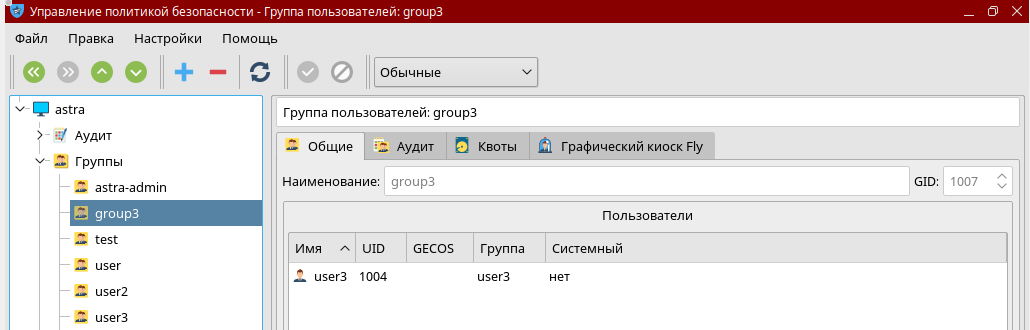


Рисунок 49 – содержимое группы group3

Теперь добавим и во вторичную группу group4 с помощью графической утилиты «Политика безопасности». Добавление пользователя представлено на рисунке 50.

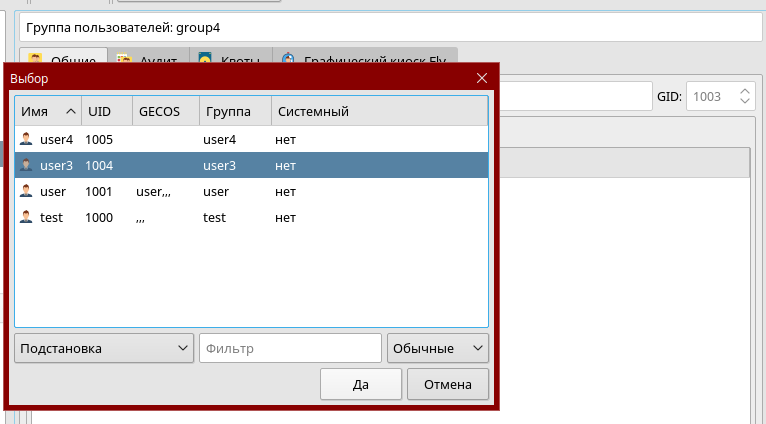


Рисунок 50 – добавление пользователя user3 в group4 через графический интерфейс

В результате содержимое группы получилось таким, как представлено на рисунке 51.

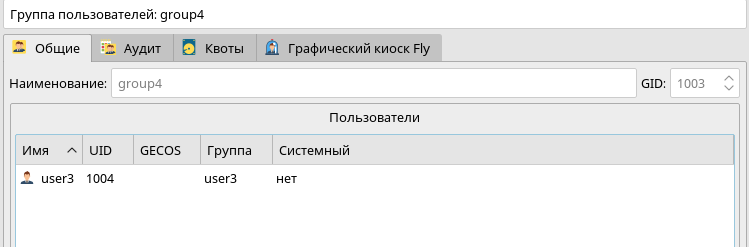


Рисунок 51 – содержимое группы group4

Теперь нам нужно 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". Результат выполнения команд представлено на рисунке 52.

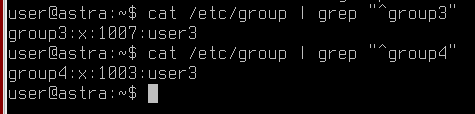


Рисунок 52 – содержимое файла /etc/group

**Задание 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.

Сначала удалим через графическую утилиту. Результат выполнения представлено на рисунке 53.

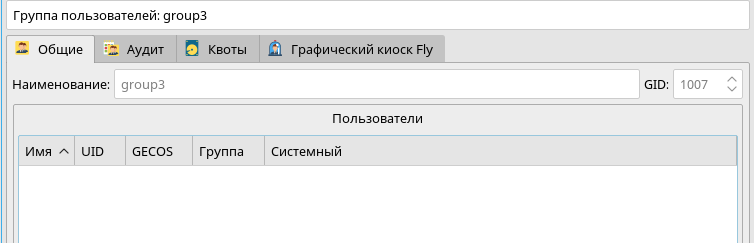


Рисунок 53 – удаление пользователя из группы с помощью графической утилиты

Теперь попробуем удалить, используя командую строку. Команда и результат выполнения представлено на рисунке 54.

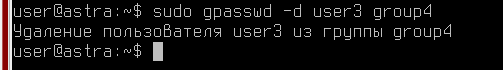


Рисунок 54 – удаление пользователя из группы с помощью командной строки

**Задание 17.** Удалить группу group3 командой sudo delgroup group3 в терминале Fly и группу group4 с помощью графической утилиты «Политика безопасности».

Для удаления группы воспользуемся командой, которая представлена по условию задания. Результат выполнения команды представлено на рисунке 55.

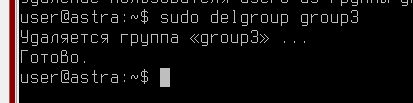


Рисунок 55 – удаление группы через терминал

Теперь удалим группу group4 с помощью графической утилиты «Политика безопасности». Удаление группы с помощью графического интерфейса представлено на рисунке 56.

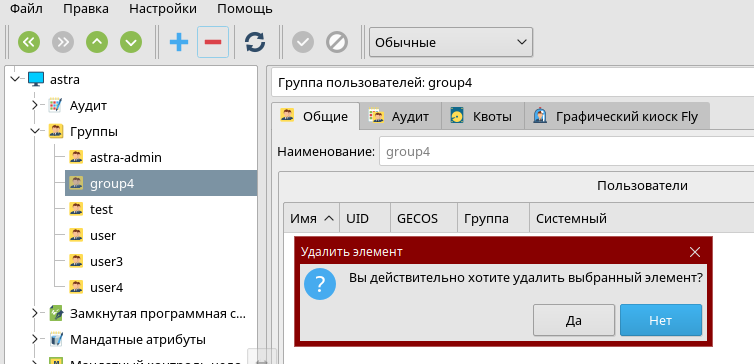


Рисунок 56 – удаление группы через графический интерфейс

**Контрольные вопросы**

1. Что такое идентификационные номера пользователей и групп в ОССН Astra Linux?

Это числовые идентификаторы, которые ядро ОС использует для разграничения прав доступа пользователей и групп к ресурсам (файлам, каталогам, процессам и т.д.).

* **UID (User IDentifier)** — идентификатор пользователя.
  + 0: Зарезервирован для суперпользователя root.
  + 1-999: Системные пользователи и группы (для запуска служб и демонов).
  + 1000+: Обычные пользователи, создаваемые администратором.
* **GID (Group IDentifier)** — идентификатор группы.
  + Имеет аналогичную нумерацию. Каждый пользователь обязательно состоит как минимум в одной **первичной группе**, GID которой указывается в /etc/passwd.

2. Какие файлы ОССН Astra Linux содержат информацию о пользователях и группах системы?

Основные файлы, хранящие информацию о учётных записях, традиционны для Unix-подобных систем:

* **/etc/passwd**: содержит основной список пользователей, их UID, GID и другую информацию (но не пароли).
* **/etc/shadow**: содержит зашифрованные пароли пользователей и информацию об их сроке действия. Доступен только для чтения пользователем root.
* **/etc/group**: содержит список групп и их GID, а также перечень пользователей, входящих в эти группы в качестве дополнительных.
* **/etc/gshadow**: содержит зашифрованные пароли для групп (если используются) и другую служебную информацию.

3. Какие поля содержит каждая строка файла /etc/passwd, кратко охарактеризуйте их?

Каждая строка в /etc/passwd соответствует одному пользователю и содержит семь полей, разделённых двоеточиями (:):

1. **Имя пользователя (логин)**: Уникальное имя для входа в систему.
2. **Пароль (заполнитель)**: Исторически здесь хранился хэш пароля. Теперь почти всегда содержит x, указывая, что реальный пароль находится в /etc/shadow.
3. **UID**: Числовой идентификатор пользователя.
4. **GID**: Числовой идентификатор первичной группы пользователя.
5. **GECOS (или комментарий)**: Дополнительная информация о пользователе (например, полное имя, телефон, номер кабинета).
6. **Домашний каталог**: Полный путь к домашней директории пользователя.
7. **Командная оболочка (shell)**: Интерпретатор команд, который запускается после входа пользователя в систему (например, /bin/bash). Если указан /usr/sbin/nologin, вход в систему запрещён.

**Пример:** johnd:x:1001:1001:John Doe,,,:/home/johnd:/bin/bash

4. В каком файле ОССН Astra Linux хранятся пароли, в каком виде они представлены?

Пароли хранятся в файле **/etc/shadow**. Они представлены в виде **хэшей**, полученных с помощью криптографических алгоритмов.

В Astra Linux по умолчанию используется стойкий алгоритм **SHA-512**. Хэш — это результат одностороннего математического преобразования пароля. Восстановить исходный пароль из хэша практически невозможно. При вводе пароля система хэширует введённую строку и сравнивает полученный хэш с тем, что хранится в файле.

5. Формат записи в файле /etc/shadow, что означает каждое поле?

Каждая строка в /etc/shadow соответствует одному пользователю и содержит девять полей, разделённых двоеточиями (:):

1. **Имя пользователя**: сопоставляется с именем из /etc/passwd.
2. **Пароль (хэш)**: зашифрованный пароль. Если значение “!” или “\*”, учётная запись заблокирована.
3. **Дата последнего изменения пароля**: количество дней, прошедших с 1 января 1970 года (эпоха Unix) до последней смены пароля.
4. **Минимальный срок действия пароля**: минимальное количество дней, которое должно пройти перед возможностью снова сменить пароль.
5. **Максимальный срок действия пароля**: максимальное количество дней, через которое пароль нужно сменить.
6. **Период предупреждения**: за сколько дней до истечения срока действия пароля начать предупреждать пользователя.
7. **Период неактивности**: сколько дней после истечения срока действия пароля учётная запись будет ещё доступна, прежде чем будет заблокирована.
8. **Срок действия учётной записи**: дата (в днях с эпохи Unix), после которой учётная запись будет автоматически заблокирована.
9. **Зарезервированное поле**: не используется.

6. Назовите команды и утилиты, используемые для администрирования параметров учётных записей пользователей.

* **Базовые утилиты командной строки:**
  + useradd, usermod, userdel — для создания, изменения и удаления учётных записей.
  + groupadd, groupmod, groupdel — для управления группами.
  + passwd — для смены пароля пользователя.
  + chage — для управления сроком действия пароля и учётной записи.
* **Графические утилиты (в графической среде Astra Linux):**
  + **Центр управления Astra Linux** → раздел **"Учётные записи"**. Это основной графический инструмент для удобного управления пользователями и группами.
  + **dconf-editor** или настройки в Центре управления — для редактирования политик безопасности.
* **Утилиты для аудита и безопасности:**
  + pam\_tcb — Astra Linux использует альтернативную схему хранения паролей и данных аутентификации (в каталоге /etc/tcb/). Для работы с ней используются свои утилиты (authconfig, passwd и др.), но обычно взаимодействие происходит через стандартные команды и графический интерфейс.

7. Как осуществляется аудит событий в ОССН Astra Linux? Как настроить перечень событий, подлежащих аудиту?

Аудит событий в Astra Linux осуществляется с помощью подсистемы **auditd** (Linux Audit Daemon).

* **Как осуществляется?**
  + Демон auditd работает в фоновом режиме и собирает события аудита на основе заранее заданных правил.
  + Он записывает их в лог-файлы (обычно в /var/log/audit/audit.log).
  + Для просмотра логов используется утилита ausearch.
  + Для генерации отчетов — утилита aureport.
* **Как настроить перечень событий?**  
  Правила аудита задаются в двух основных местах:
  1. **Файл конфигурации /etc/audit/audit.rules**. Сюда правила добавляются вручную или с помощью утилит.
  2. **Графический интерфейс Центр управления Astra Linux** → раздел **"Аудит"**.  
     Через этот раздел можно настроить аудит различных событий:
  + Регистрация в системе (успешные/неуспешные попытки входа).
  + Использование привилегированных команд (sudo, su).
  + Изменение файлов учётных записей (/etc/passwd, /etc/shadow) и прав доступа к ним.
  + Сетевые подключения и многое другое.

8. Какие настройки содержит раздел «Блокировка» в политиках учетной записи?

Раздел "Блокировка" (часто находится в настройках парольной политики) позволяет защититься от подбора паролей brute-force. Он содержит настройки, которые **временно блокируют учётную запись** после нескольких неудачных попыток входа:

* **Включить блокировку**: активирует или деактивирует механизм блокировки.
* **Количество неудачных попыток**: число неправильных вводов пароля подряд, после которого учётная запись блокируется (например, 5 попыток).
* **Время до сброса счётчика неудачных попыток**: время (в секундах/минутах), по истечении которого счётчик неудачных попыток сбрасывается в ноль, если новых ошибок не было (например, 300 секунд).
* **Время блокировки**: Время, на которое блокируется учётная запись после превышения лимита попыток (например, 600 секунд). Может быть установлено как "Навсегда" до разблокировки администратором.

9. Опишите требования, предъявляемые к паролю. Как реализовано конфигурирование этих требований в ОССН Astra Linux?

**Требования к паролю (реализованы через модуль PAM pam\_pwquality):**

* **Минимальная длина** (например, не менее 8 символов).
* **Сложность**: Пароль должен содержать символы из разных категорий:
  + Прописные буквы (A-Z)
  + Строчные буквы (a-z)
  + Цифры (0-9)
  + Специальные символы (например, !, @, #, $)
* **Отличие от старого**: Новый пароль должен отличаться от предыдущего на определенное количество символов.
* **Проверка по словарям**: Запрет на использование простых слов из словаря.
* **Запрет на использование имени пользователя или его вариаций**.

**Конфигурирование требований в Astra Linux:**

Настройка выполняется двумя основными способами:

1. **Через графический интерфейс (Центр управления Astra Linux)**:
   * Необходимо перейти в раздел **"Учётные записи"** -> **"Параметры безопасности"** (или "Политика паролей").
   * В этом разделе можно в удобной форме задать все перечисленные выше требования: минимальную длину, необходимое количество символов каждого типа, историю паролей (сколько раз пароль нельзя повторять) и параметры блокировки.
2. **Через конфигурационные файлы**:
   * Основные настройки сложности пароля хранятся в файле **/etc/security/pwquality.conf**.
   * Настройки истории паролей и других параметров, связанных со старением, находятся в файлах **/etc/pam.d/common-password** и настраиваются через утилиту chage.