МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**ЛАБОРАТОРНАЯ РАБОТА №9**

**Дисциплина: Операционные системы**

**Тема: «БАЗОВЫЙ КОМПЛЕКС СРЕДСТ ЗАЩИТЫ ИНФОРМАЦИИ»**

Работу выполнил:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ахвердян Г.А

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль): Математическое и программное

обеспечение компьютерных технологий

Преподаватель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е. А. Нигодин

Краснодар

2025

**Практические задания:**

**Задание 1.**

1) Войдите в ОС с учетной записью пользователя sa (Уровень\_0, Высокий).

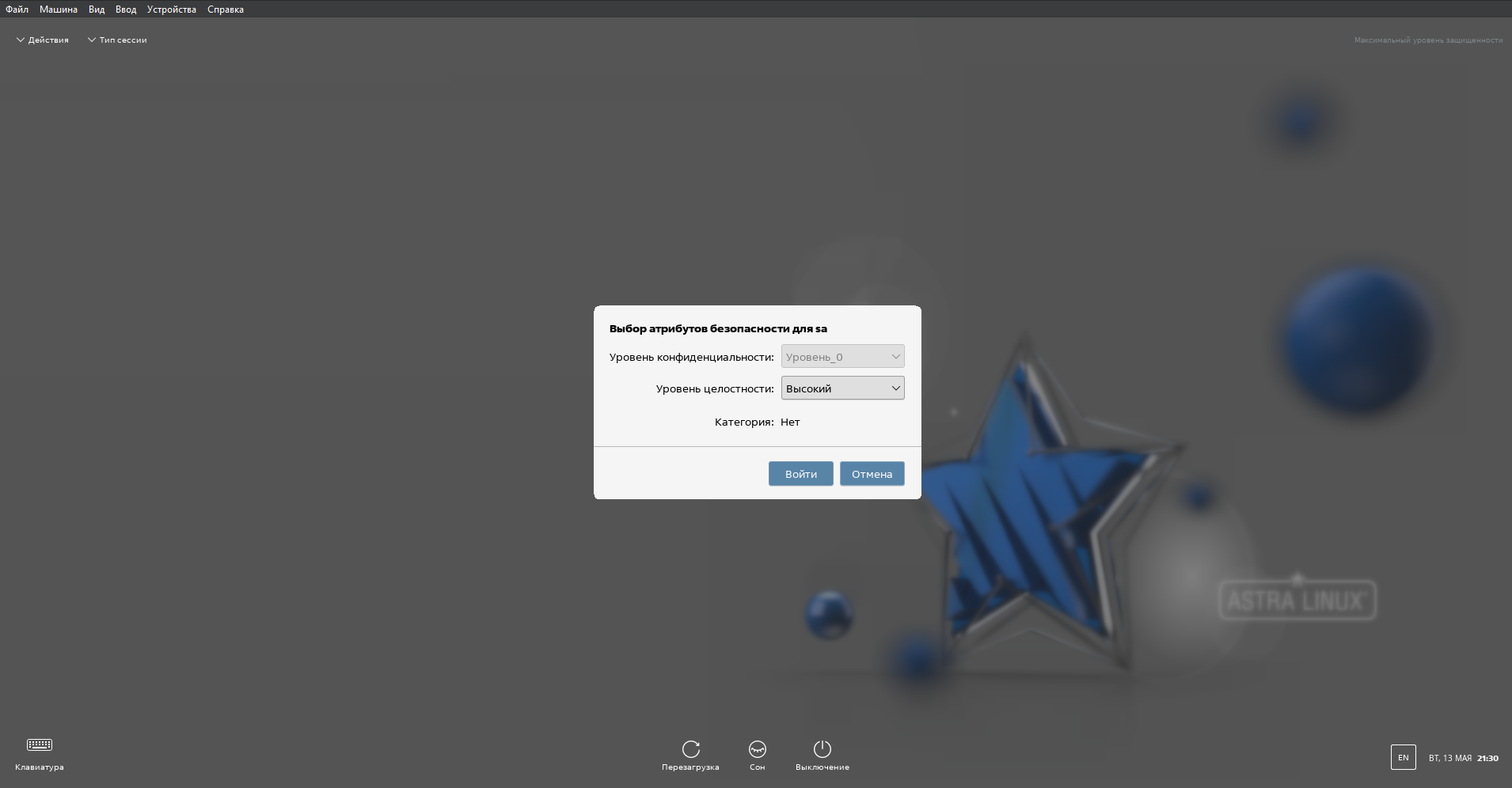
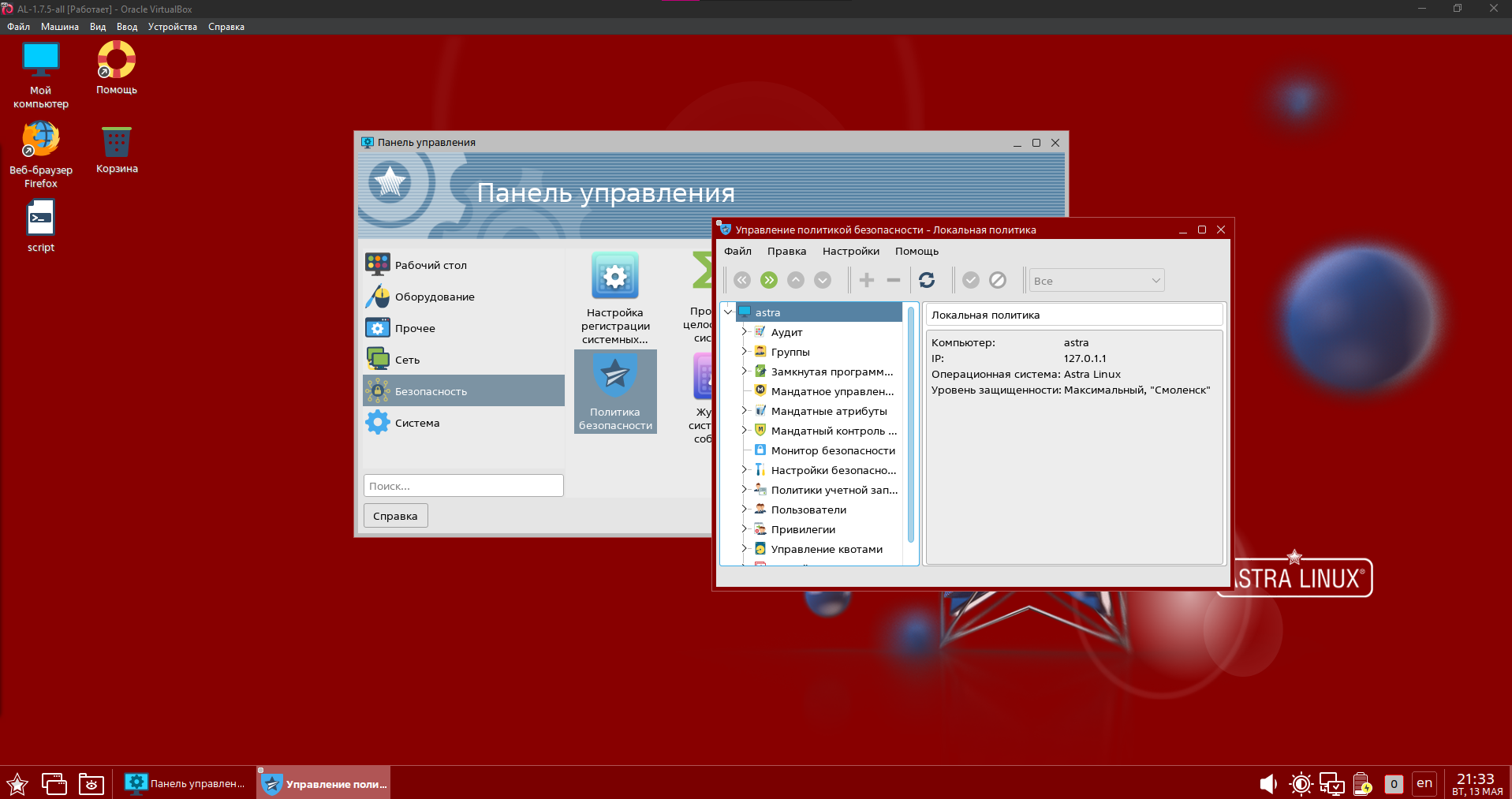
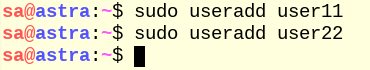
****

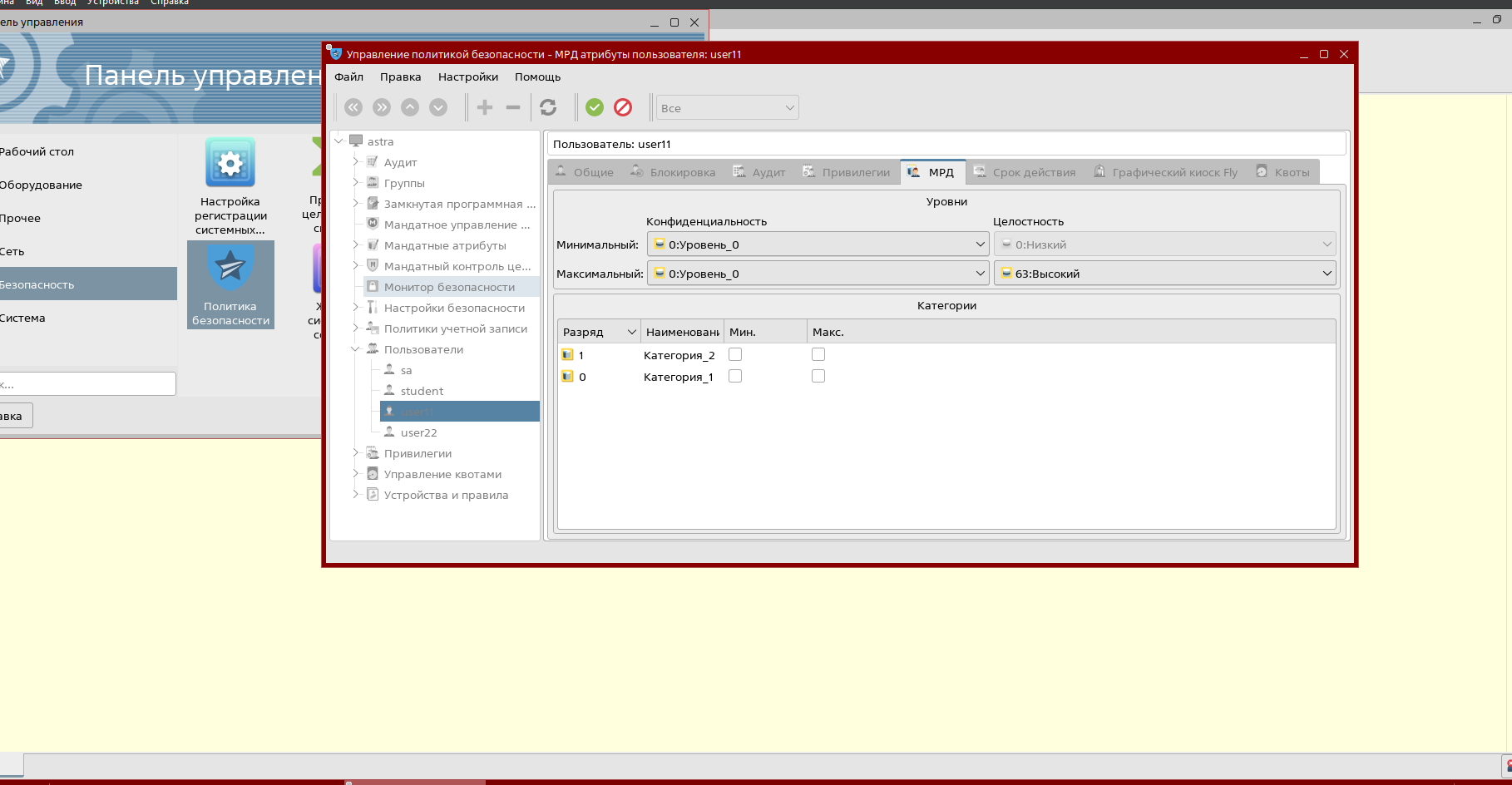
Рисунок 1 – Вход с уровнем 0

2) Запустите графическую утилиту редактирования учетных записей пользователей

  
Рисунок 2 – Графическая утилита

3) Создать 2 пользователя user1, user2. Для созданных учетных записей пользователей задайте максимальный уровень целостности.

****

****

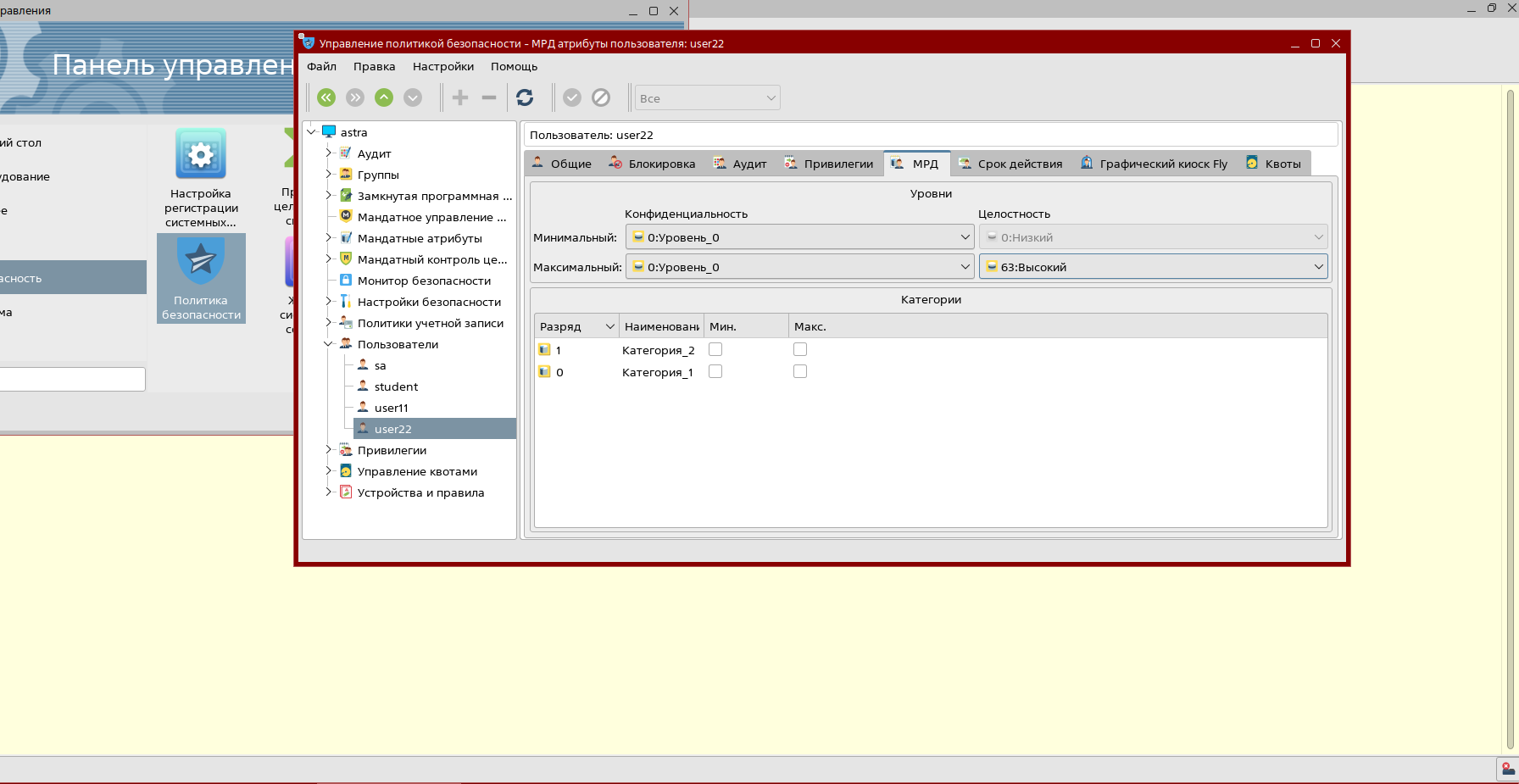
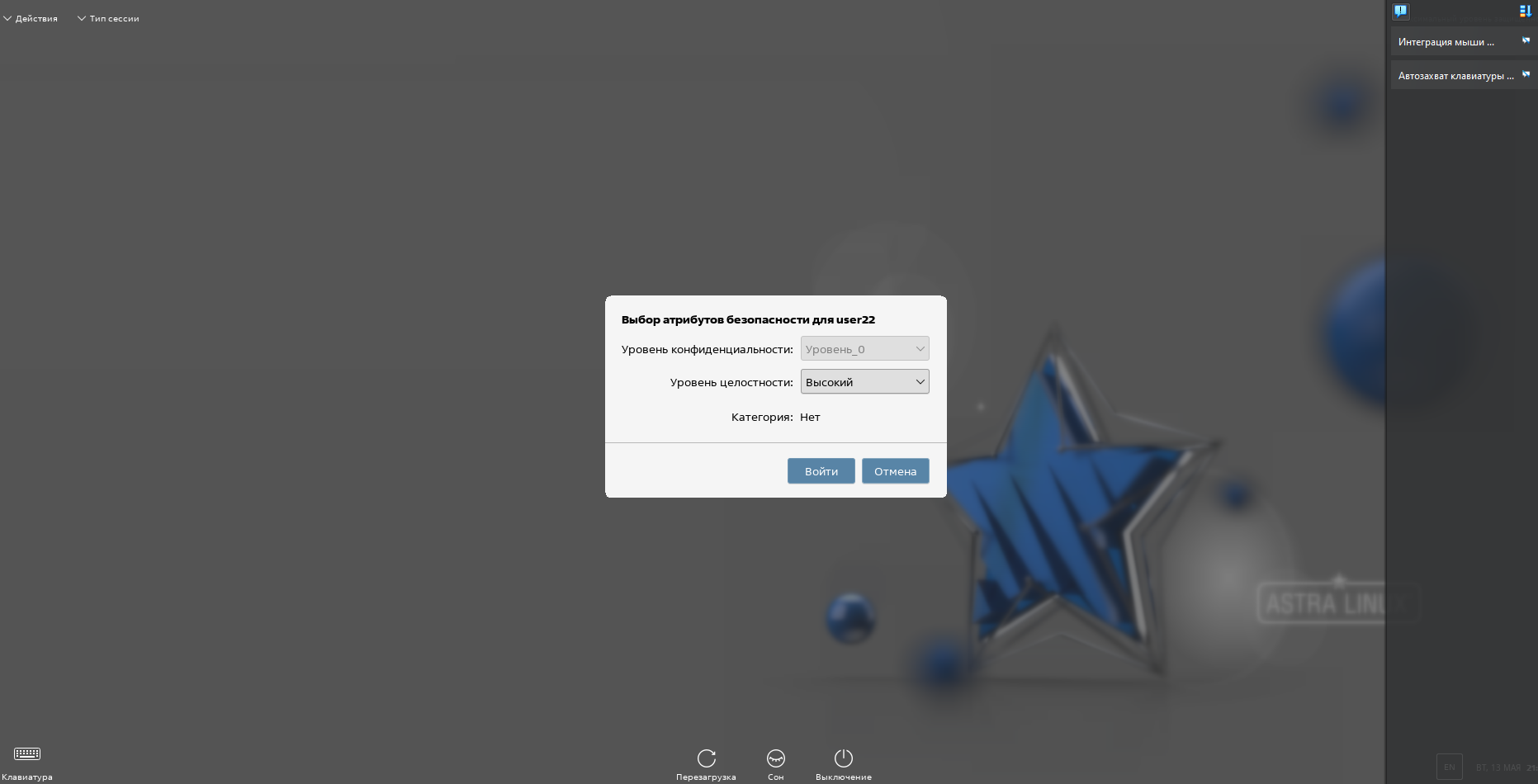
****

Рисунок 3 – Создание учетных пользователей и повышение целостности

4) Войдите в ОС с учетной записью пользователя user2, выбрав уровень доступа Уровень\_0, Высокий.

  
Рисунок 4 – Вход в созданного юзера

5) Создайте в каталоге Документы файл 1.txt, добавив в него любой текст.

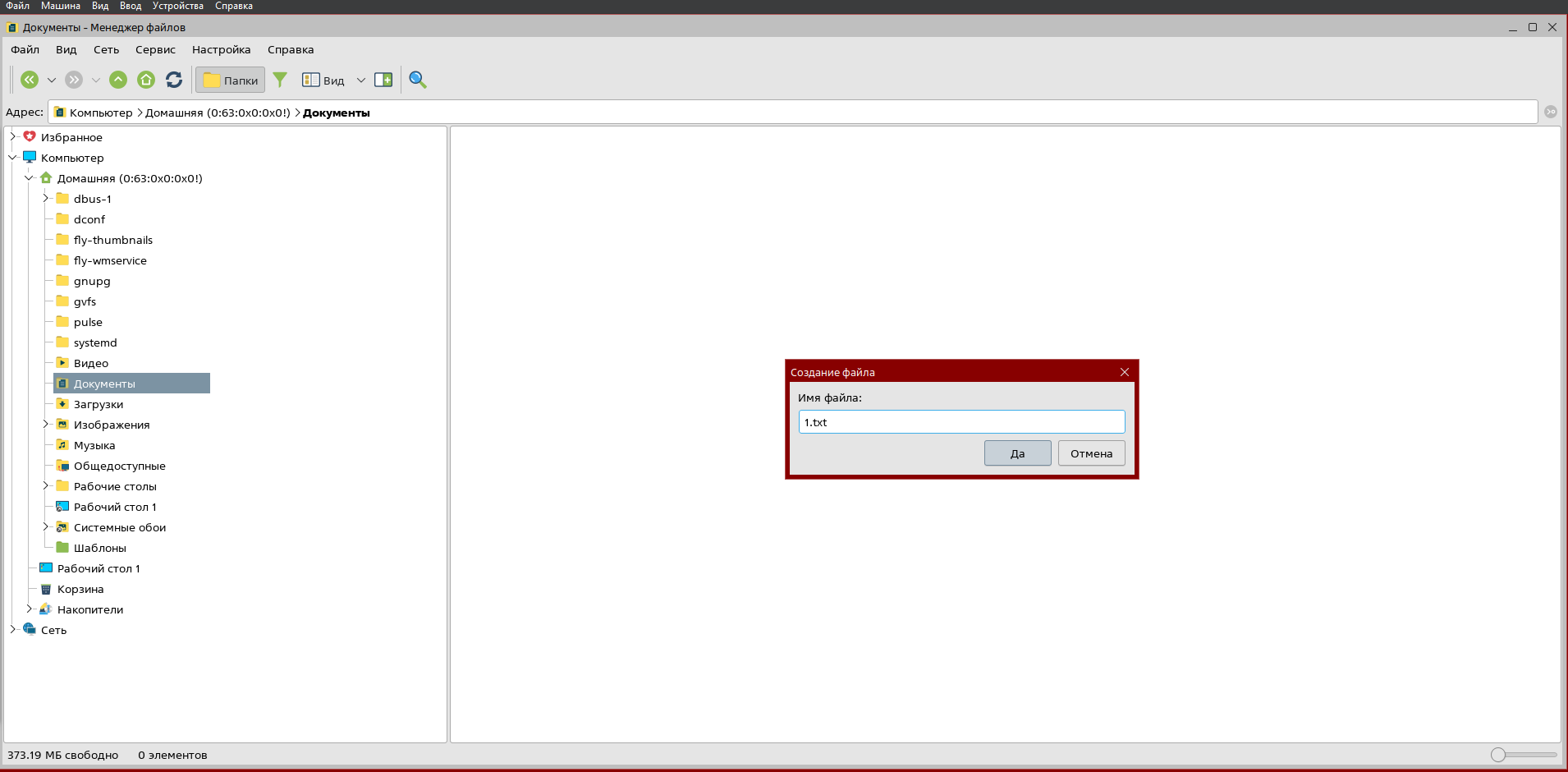
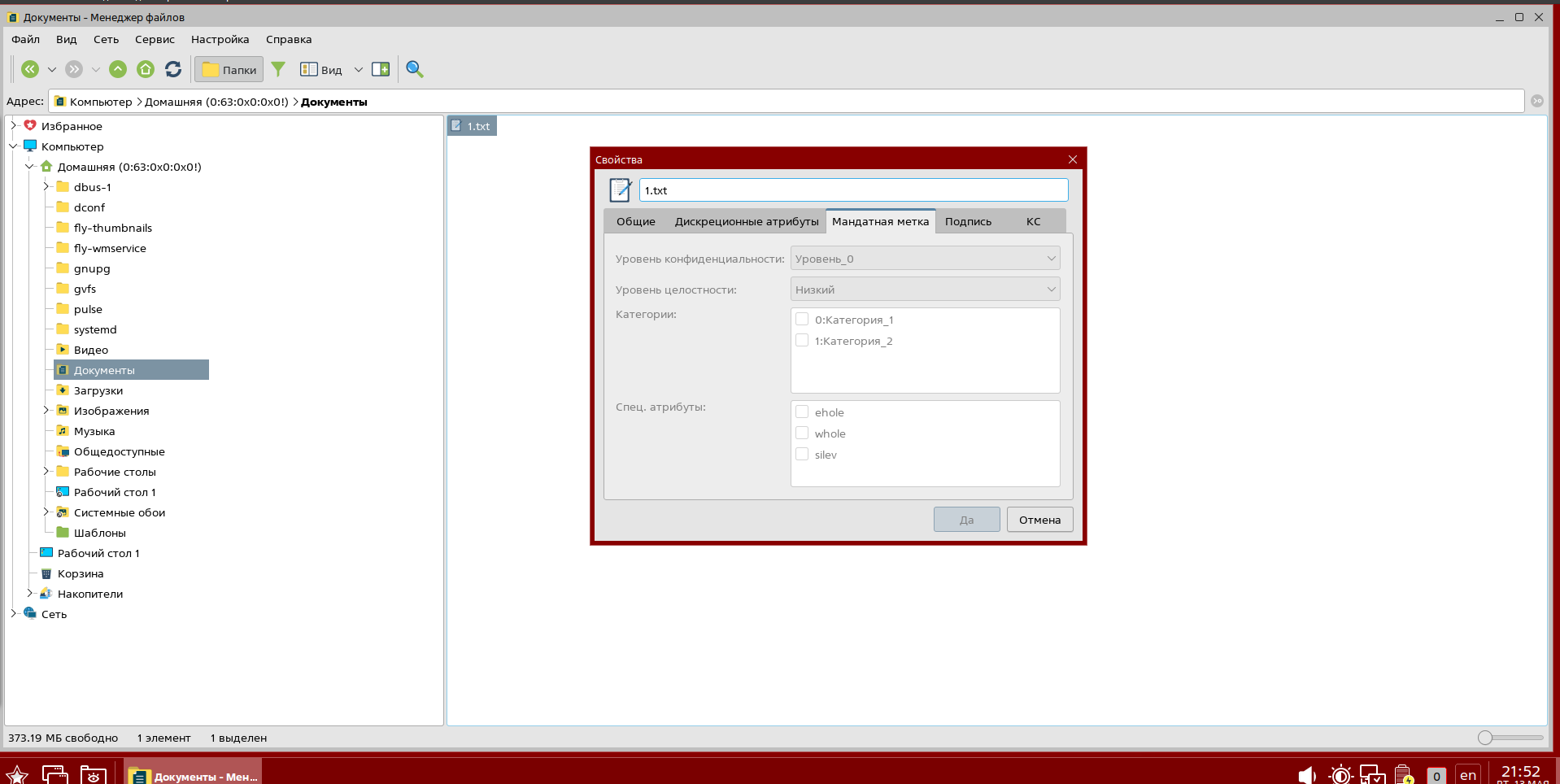
****

Рисунок 5 – Создание текстового документа

6) Просмотрите уровень целостности, указанный в свойствах файла. Каким он оказался?

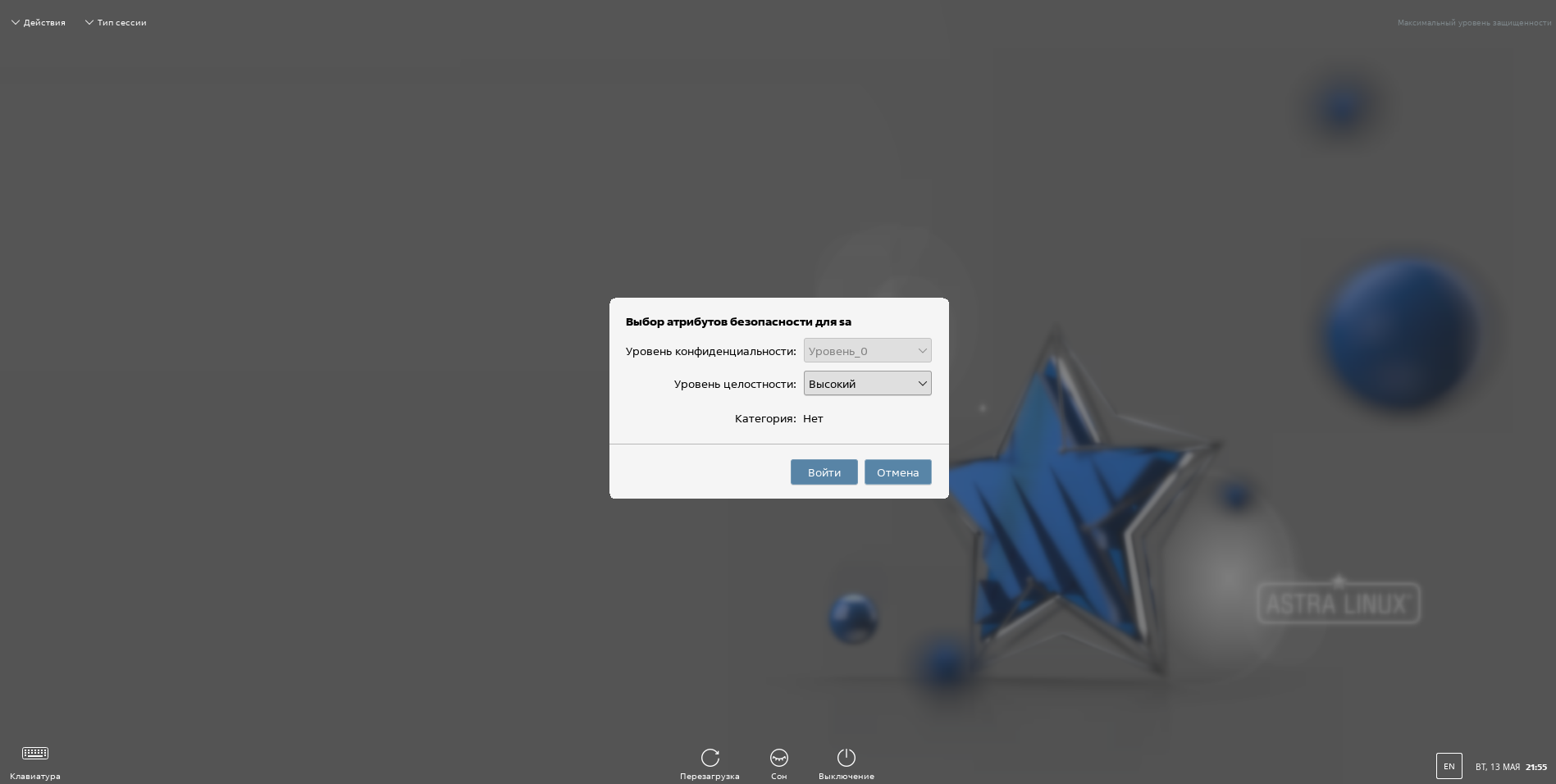
  
Рисунок 6 – Уровень целостности

7) Выйдите из ОС.

****

Рисунок 7 – Вход с уровнем 0

8) Войдите в ОС с учетной записью пользователя sa (Уровень\_0, Высокий).

  
Рисунок 8 – Вход в пользователя sa

9) Проверьте, включен ли режим мандатного контроля целостности. В случае если режим мандатного контроля целостности не включен, включите. После включения режима для вступления изменений в силу требуется перезагрузка.

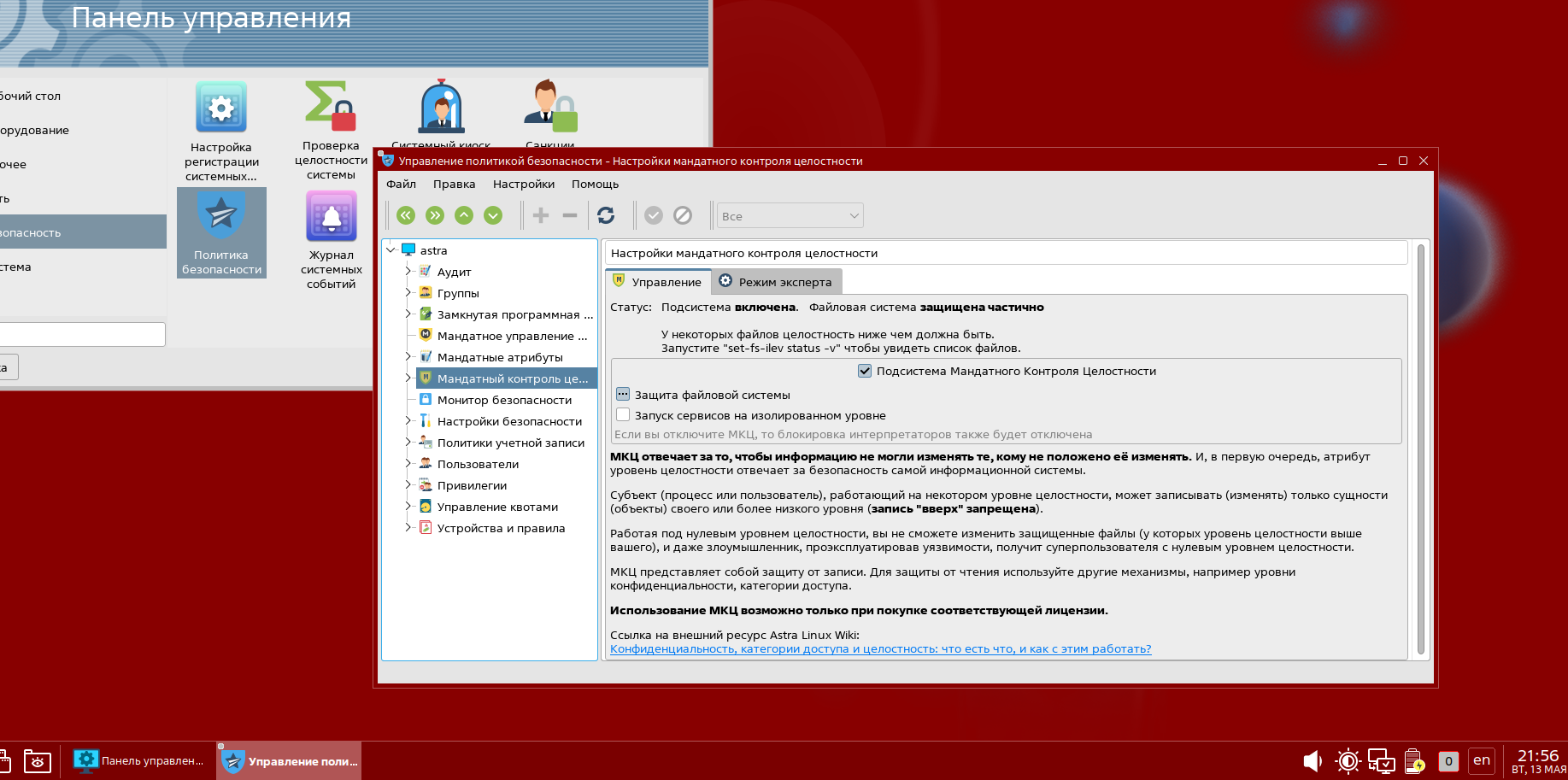
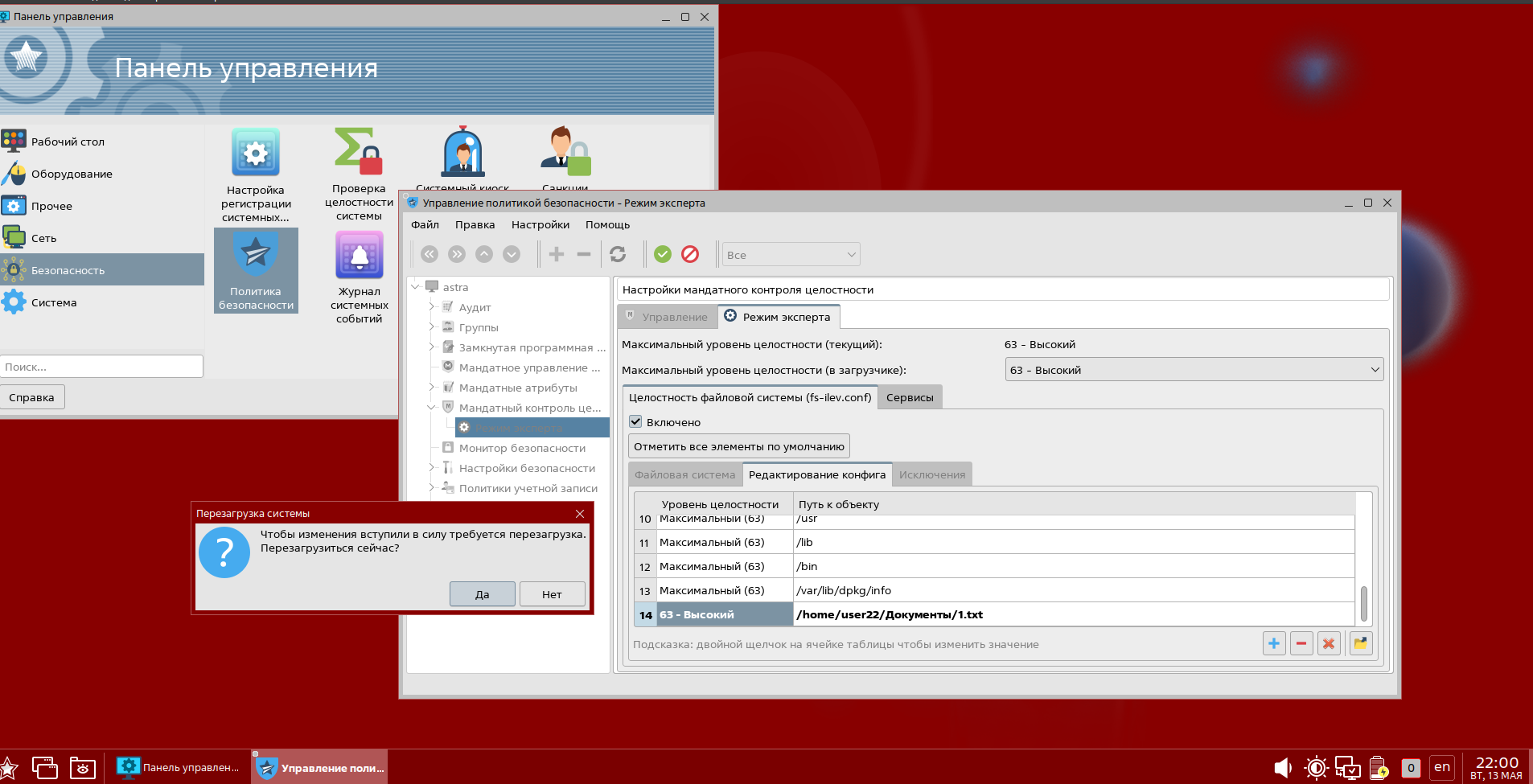
****

Рисунок 9 – Проверка режима мандатного контроля целостности

10) В графической утилите Политика безопасности выберите пункт Мандатный контроль целостности → Режим эксперта → Редактирование конфига добавьте строку, указав файл пользователя user2 Файл 1.txt, и установите для пользователя user2 уровень целостности максимальный. Перезагрузите ОС.

  
Рисунок 10 – Установка максимальной целостности

11) Войдите в ОС с учетной записью пользователя user2, выбрав уровень доступа Уровень\_0, Высокий.

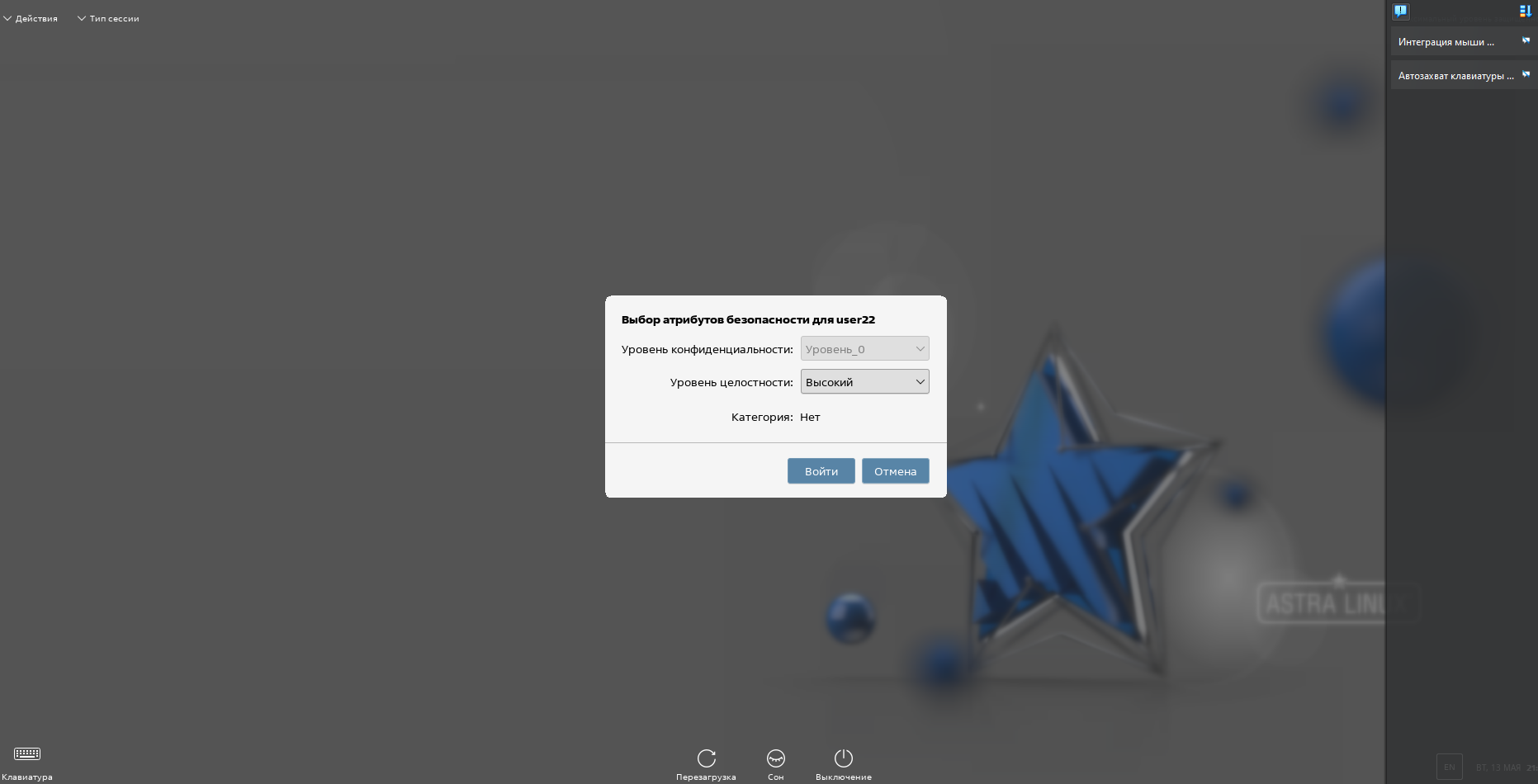
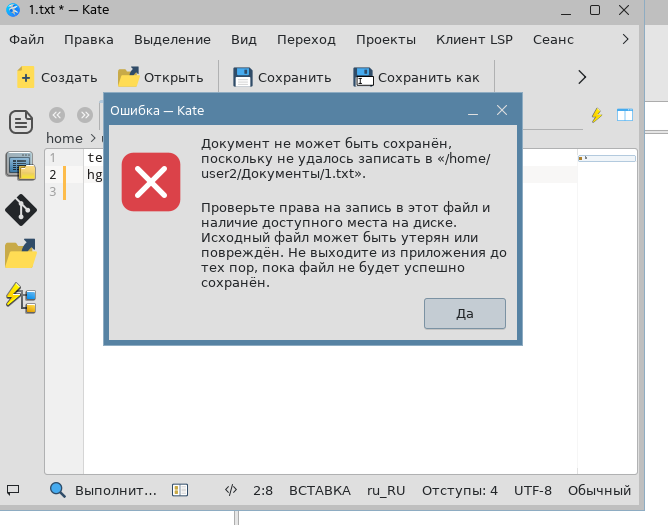


Рисунок 11 – Вход в user22

12) Попробуйте отредактировать файл 1.txt, добавив в него любой текст. Получилось? Почему? Выйдите из ОС.

  
Рисунок 12 – Редактирование файла

**Задание 2.**

1) Зайдите в систему под администратором. Запустите графическую утилиту Мандатное управление доступом с правами root.

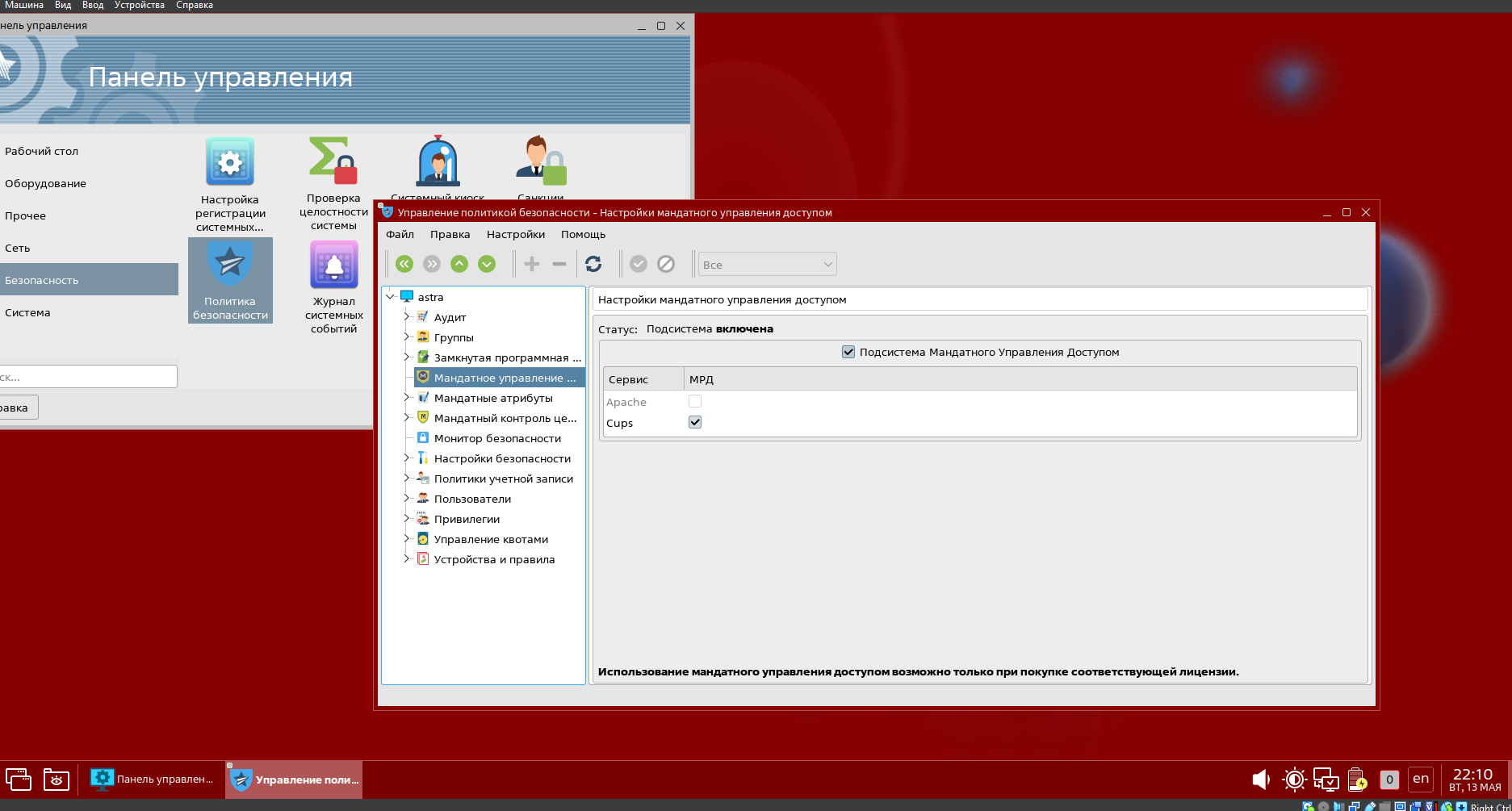


Рисунок 1 – Графическая утилита

2) Переименуйте уровни конфиденциальности:

• 0 - for \_all; • 1 - secret; • 2 - very\_secret; • 3 - very\_important.

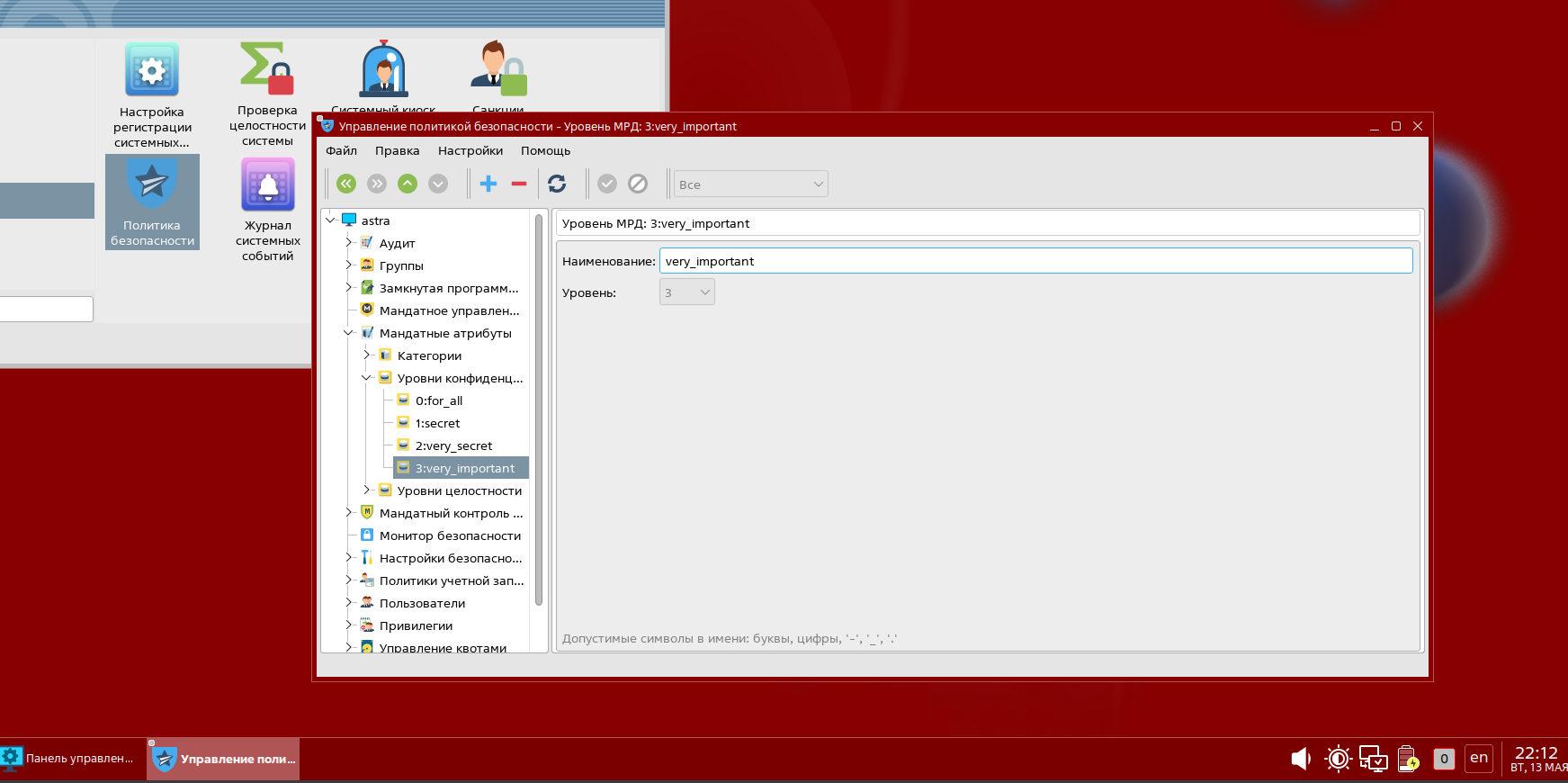


Рисунок 2 – Уровни конфиденциальности

3) Создайте учетную запись для пользователя ivanov:   
• минимальный уровень конфиденциальности - for\_all;   
• максимальный уровень конфиденциальности - very\_secret.

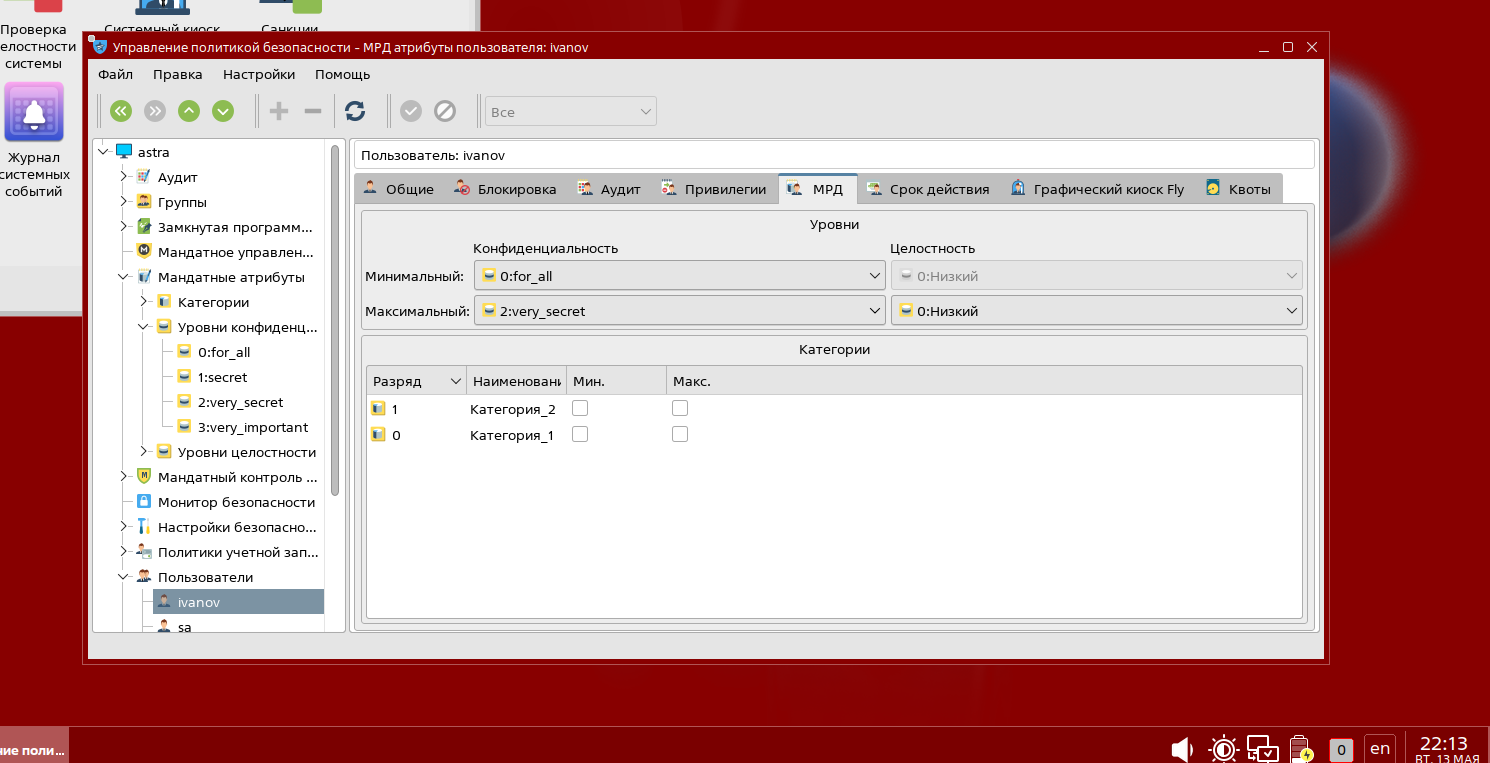


Рисунок 3 – Создание учетной записи

4) Создайте учетную запись для пользователя petrov:   
• минимальный уровень конфиденциальности - for\_all;   
• максимальный уровень конфиденциальности – secret.

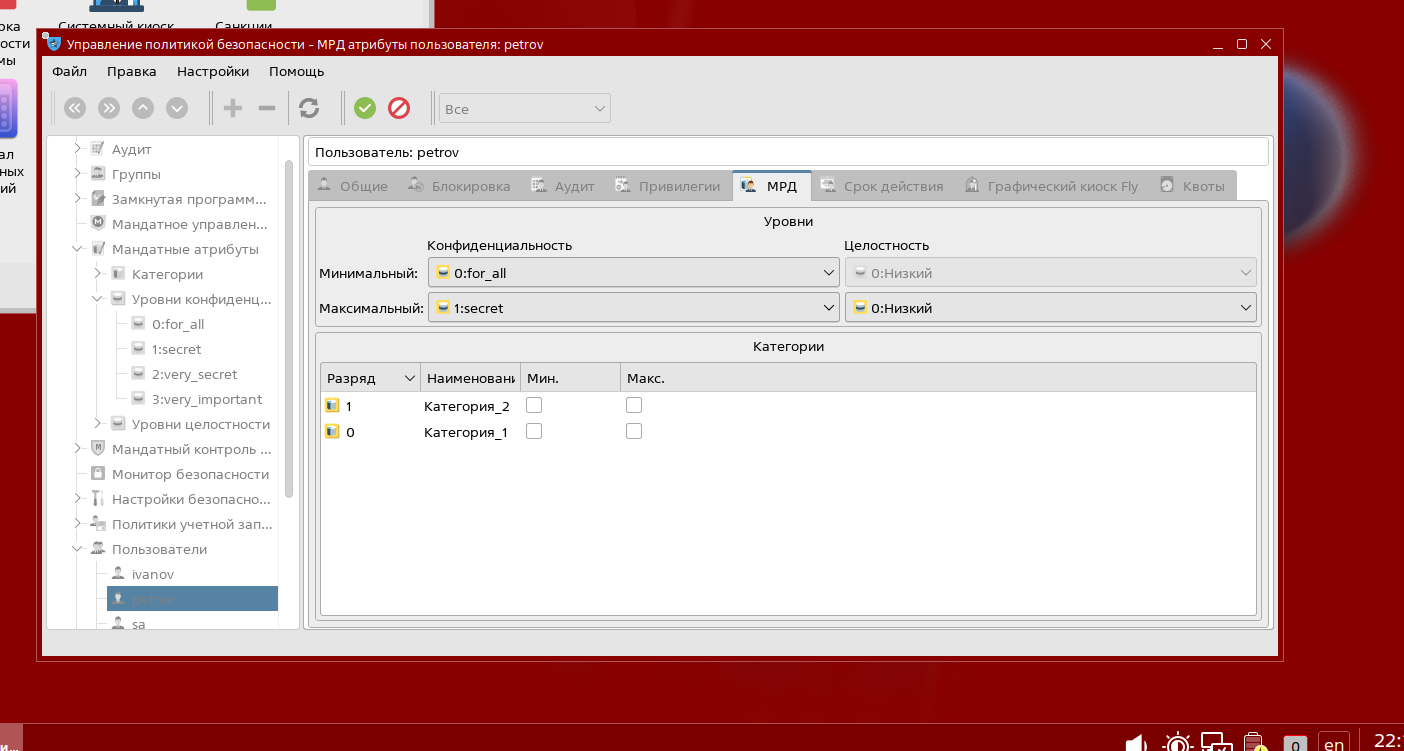


Рисунок 4 – Создание учетной записи

**Задание 3.**

1) Создайте каталог /home/project. Установите на каталог уровень конфиденциальности very\_important и дополнительный атрибут ccnr.

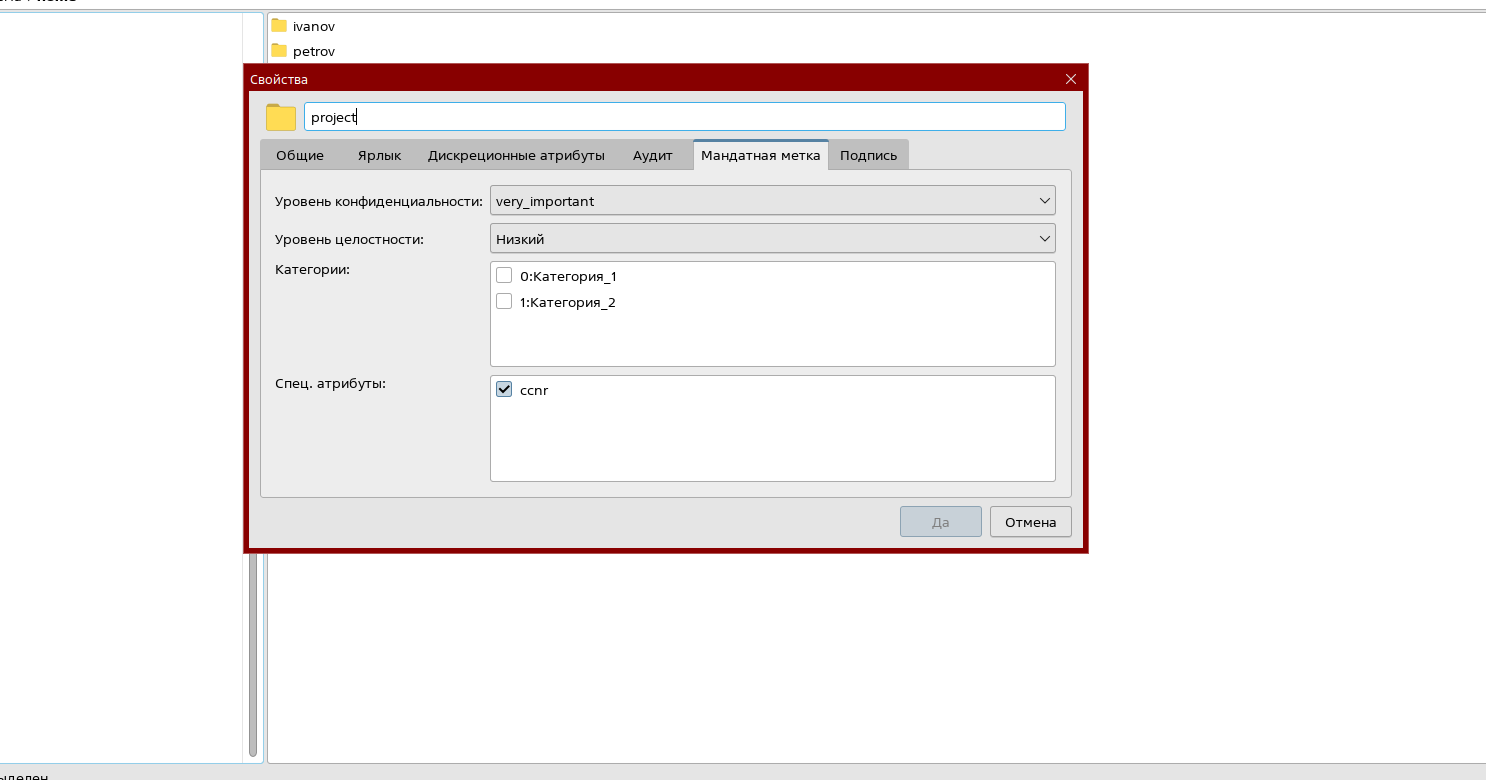


Рисунок 1 – Создание каталога

2) Создайте каталог /home/project/secret. Установите на каталог уровень конфиденциальности secret.

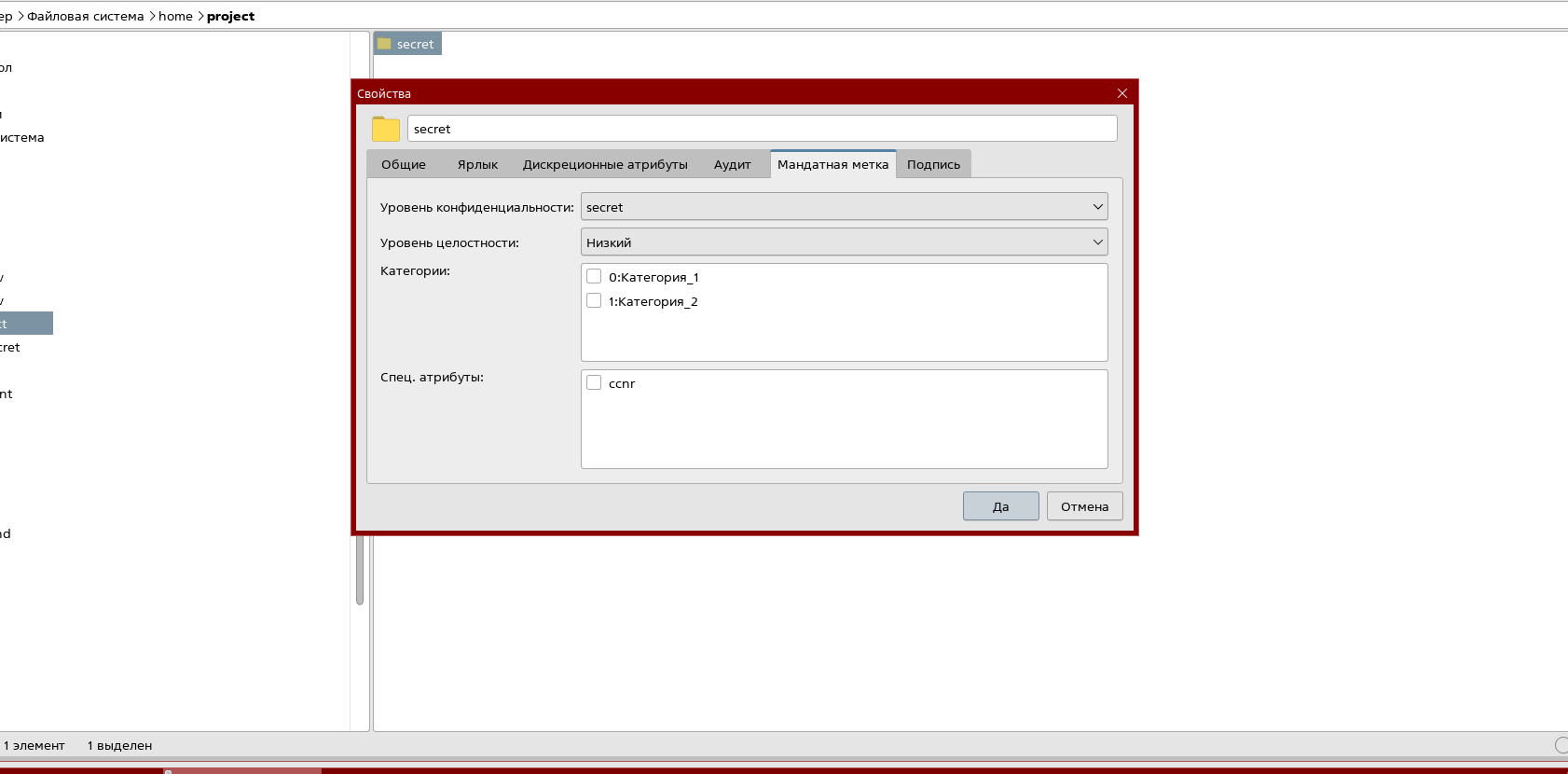


Рисунок 2 – Создание каталога

3) Создайте каталог /home/project/very\_secret. Установите на каталог уровень конфиденциальности very \_secret.

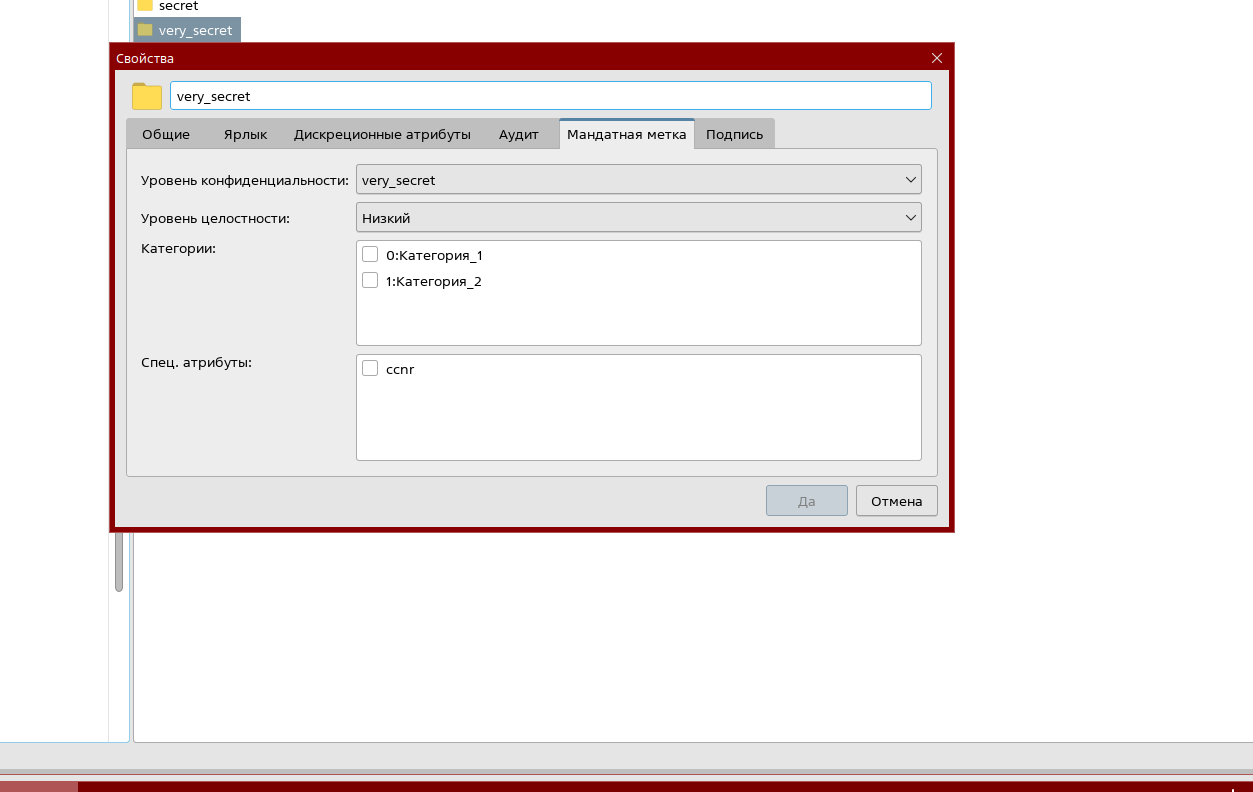


Рисунок 3 – Создание каталога

4) Установите файловые списки управления доступом (ACL) и файловые списки управления доступом по умолчанию (default ACL) на каталоги /home/project, /home/project/secret и /home/project/very\_secret, позволяющие пользователям ivanov и petrov создавать и удалять файлы в этих каталогах и изменять содержимое созданных файлов.

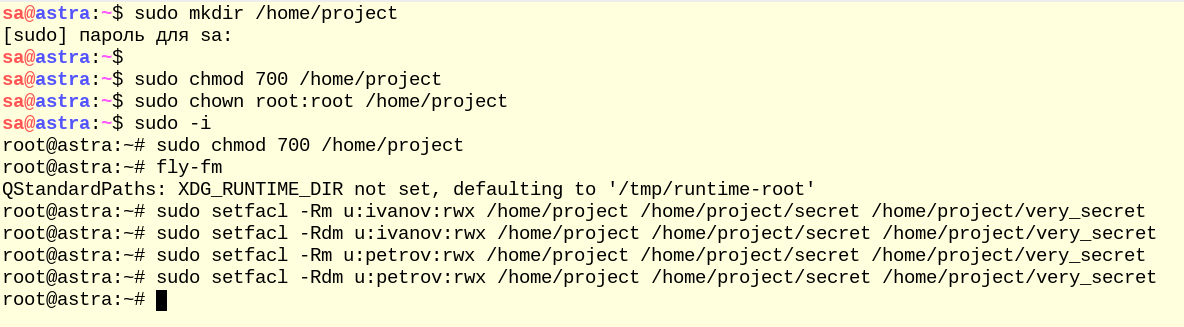


Рисунок 4 – Установка файловых списков

5) Зайдите в систему под учетной записью ivanov с уровнем конфиденциальности secret.



Рисунок 5 – Вход под ivanov

6) Создайте файл file1.txt в каталоге /home/project/secret. В этот файл добавьте строку ivanov. Сохраните файл. Удалось ли создать, изменить и сохранить файл file1.txt?

Пользователь ivanov имеет права на чтение, запись и редактирование файла в папке secret.



Рисунок 6 – Создание файла

7) Виден ли каталог /home/project/very \_secret?

Папку very\_secret мы не можем увидеть из-за разных уровней конфиденциальности

8) Зайдите под учетной записью ivanov в систему с уровнем конфиденциальности very\_secret.

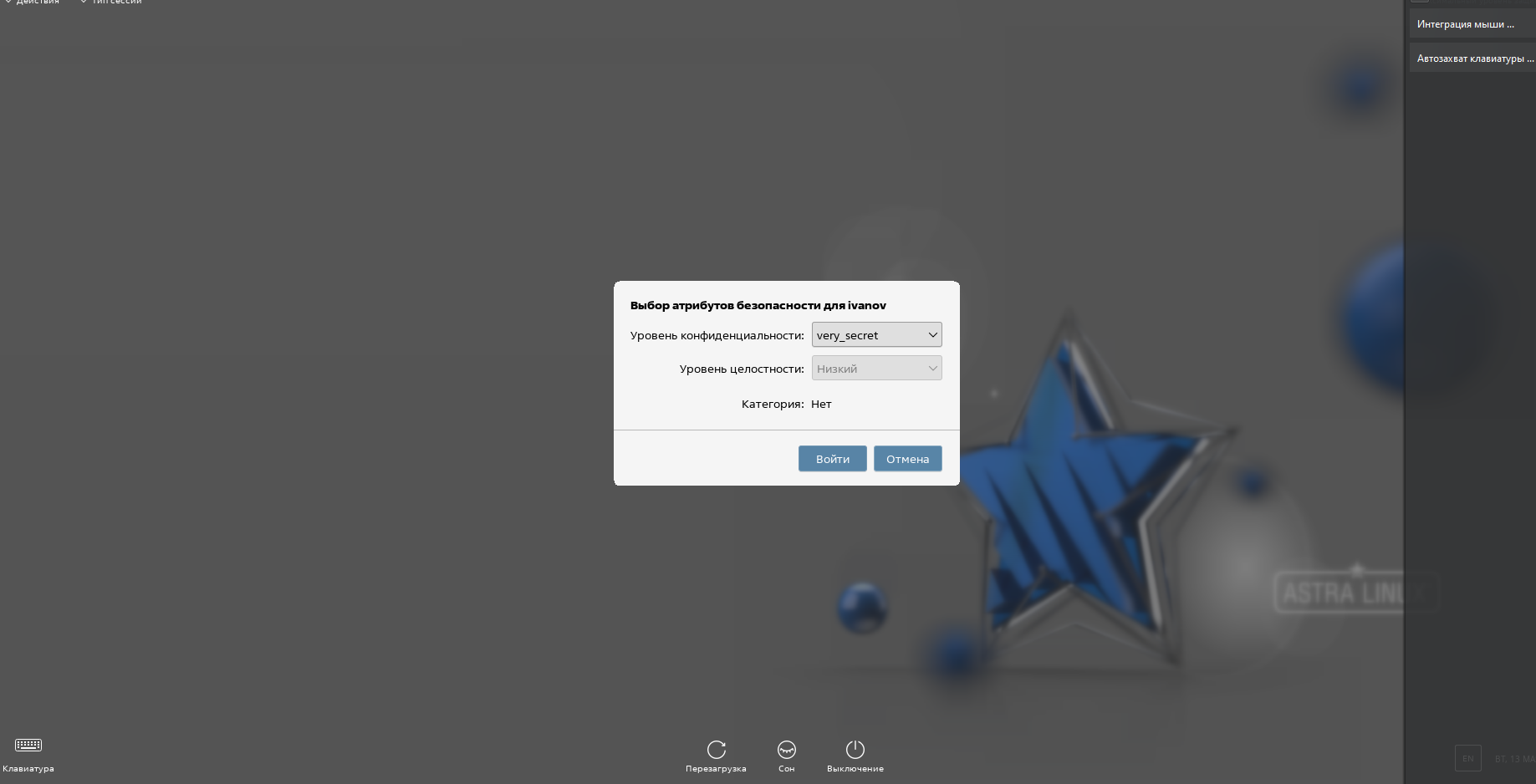


Рисунок 8 – Вход под ivanov

9) Создайте файл file2.txt в каталоге /home/project/very\_secret. В этот файл добавьте строку ivanov. Сохраните файл. Удалось ли создать, изменить и сохранить файл file2.txt?

Данный файл мы можем создать, добавить в него текст, сохранить и отредактировать

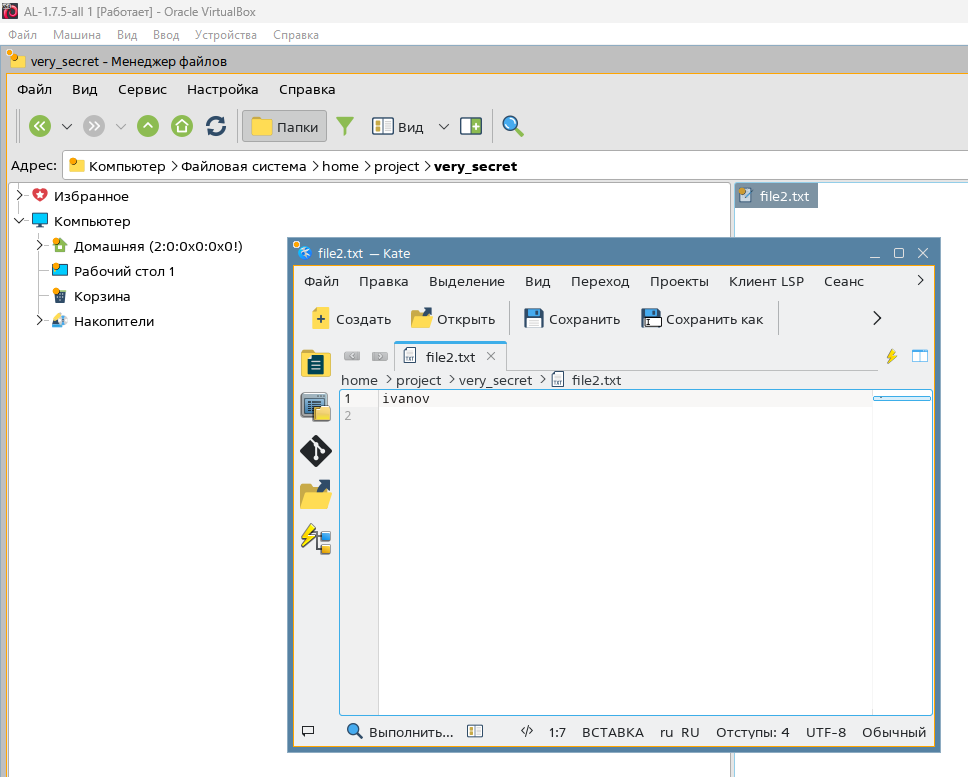
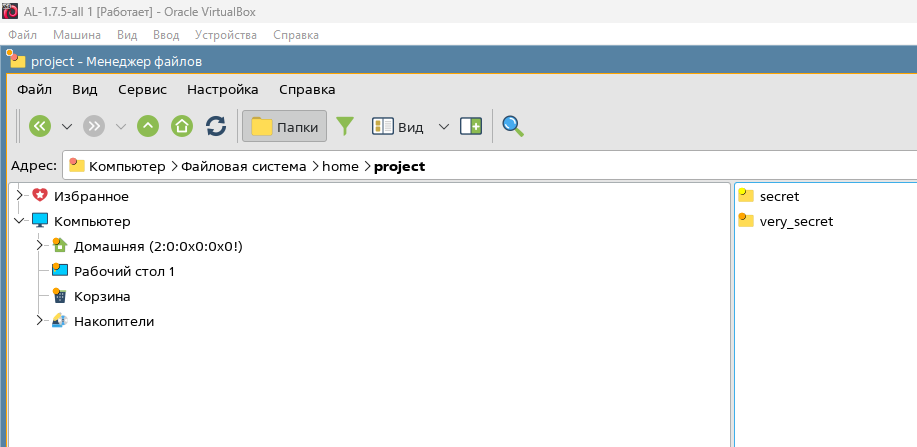


Рисунок 9 – Создание файла

10) Виден ли каталог /home/project/secret?



11) Виден ли файл /home/project/secret/file1.txt?

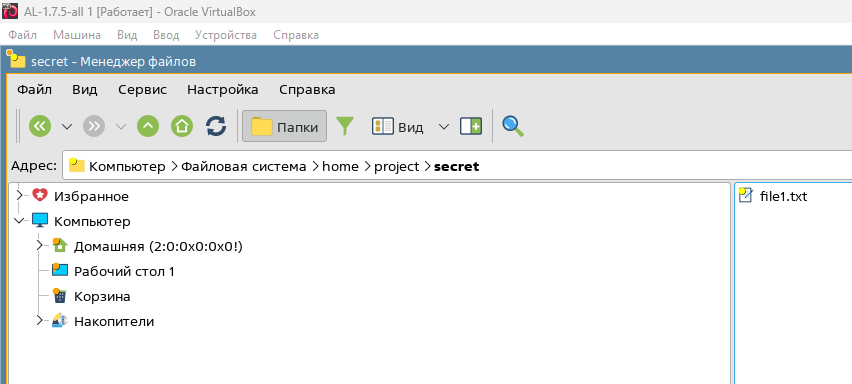


Рисунок 11 – Отображение файла

12) Добавьте в файл /home/project/secret/file1.txt строку ivanov2. Удалось ли изменить содержимое этого файла?

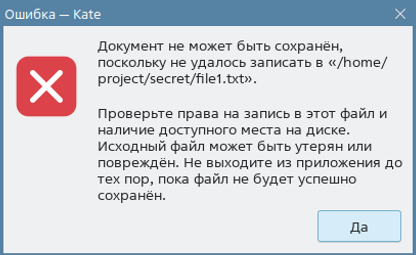


Рисунок 12 – Содержимое файла

13) Зайдите в систему под учетной записью пользователем petrov с уровнем конфиденциальности secret.

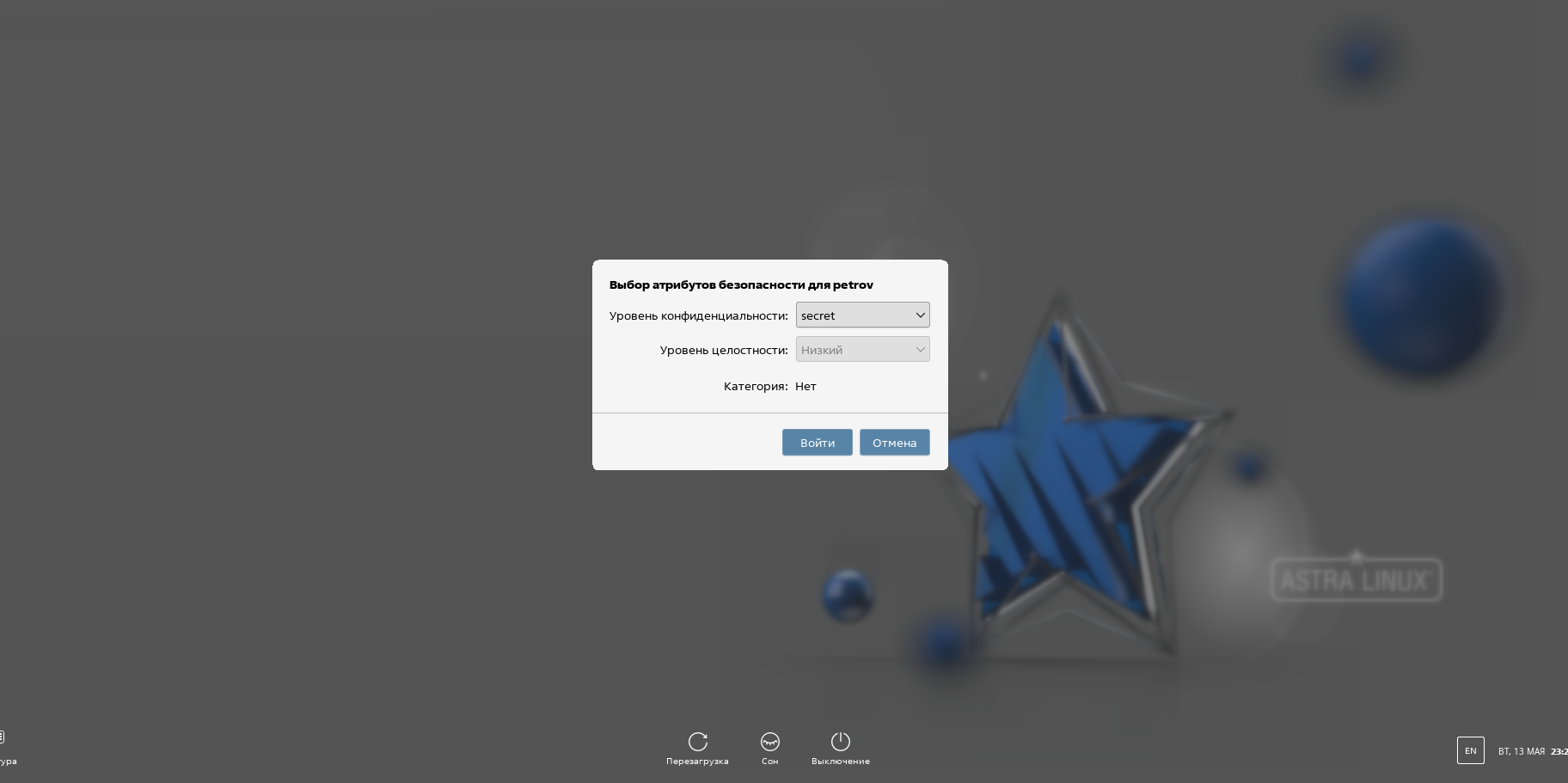


Рисунок 13 – Вход под petrov

14) Добавьте в файл /home/project/secret/file1.txt строку petrov. Удалось ли изменить содержимое этого файла?

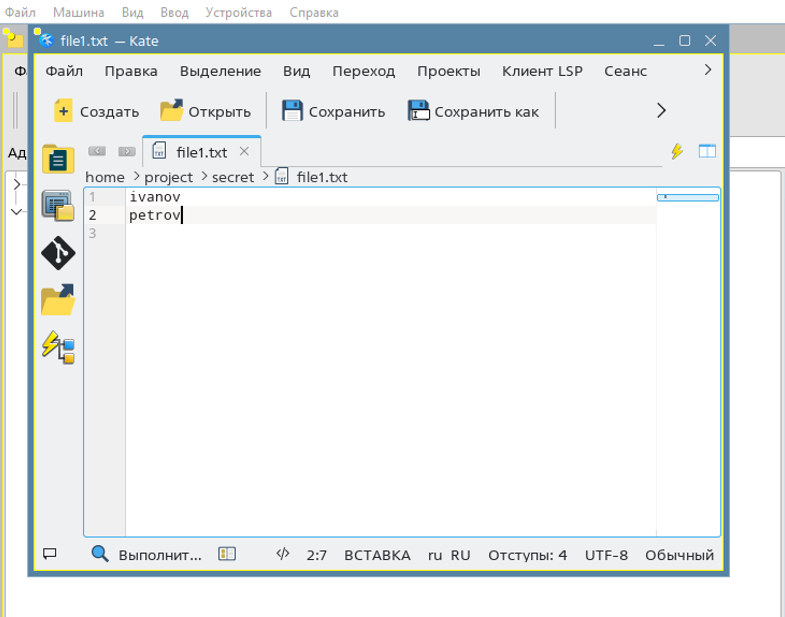


Рисунок 14 – Содержимое файла

15) Можете ли вы прочитать содержимое файла /home/project/very \_secret/fi le2.txt?

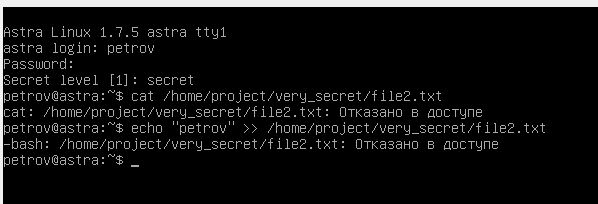


Рисунок 15 – Содержимое файла

**Задание 4.**

1) Создайте пользователей user5, user6 и user7.

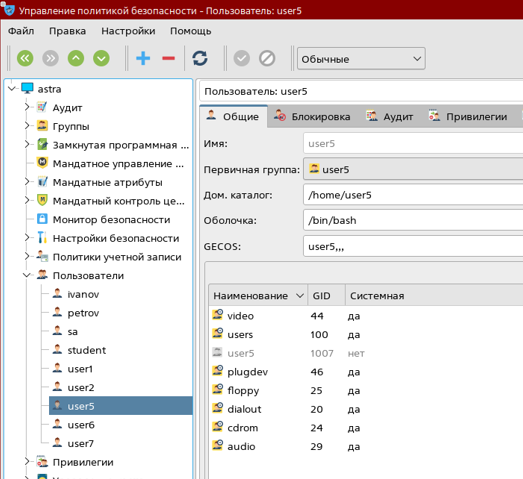


Рисунок 1 – Создание пользователей

2) Настройте графический киоск для пользователя user5, для этого:   
• добавьте запуск следующих приложений: Веб-браузер Firefox, Офис Libreoffice, Почта Thunderblrd;   
• поставьте галочки: Разрешить изменение внешнего вида и Разрешить создание и удаление файлов на рабочем столе;   
• сохраните настройки;

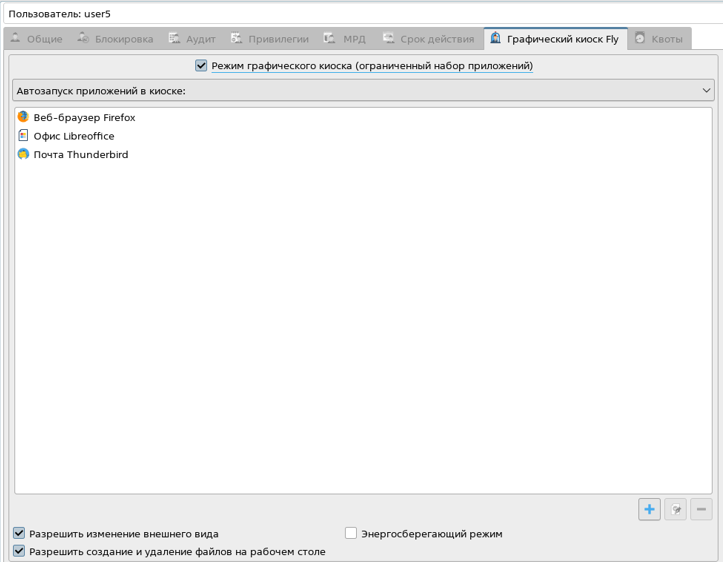


Рисунок 2 – Настройка графического киоска

3) Войдите в ОС под пользователем user5 и протестируйте, какой функционал доступен:   
• открываются ли приложения на Рабочем столе?   
• можете ли вы создать файл или каталог на Рабочем столе?

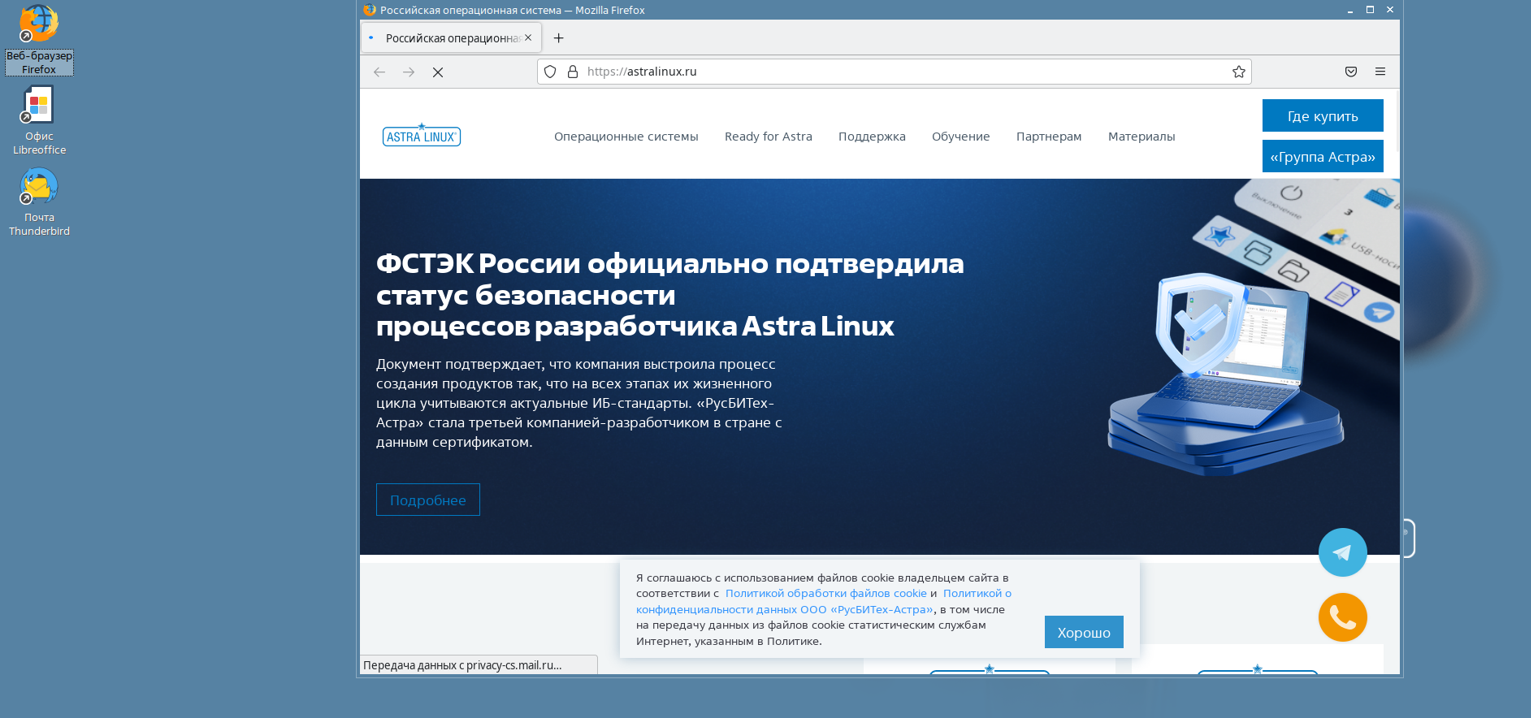


Рисунок 3 – Функционал

4-5) Войдите в ОС под пользователем sa на высоком уровне целостности. Добавьте еще один ярлык на рабочий стол пользователя user5, для этого:   
• выберите меню Пуск → Интернет→Веб-браузер Chromium→ПКМ→Отправить→ Рабочий стол;   
• скопируйте данный ярлык в профиль пользователя киоска user5 таким образом, чтобы у пользователя user5 яр



Рисунок 4 – Ярлык

6) Войдите в ОС под пользователем user5 и убедитесь, что пользователь теперь может запускать веб-браузер Chromium (ярлык появился на рабочем столе).

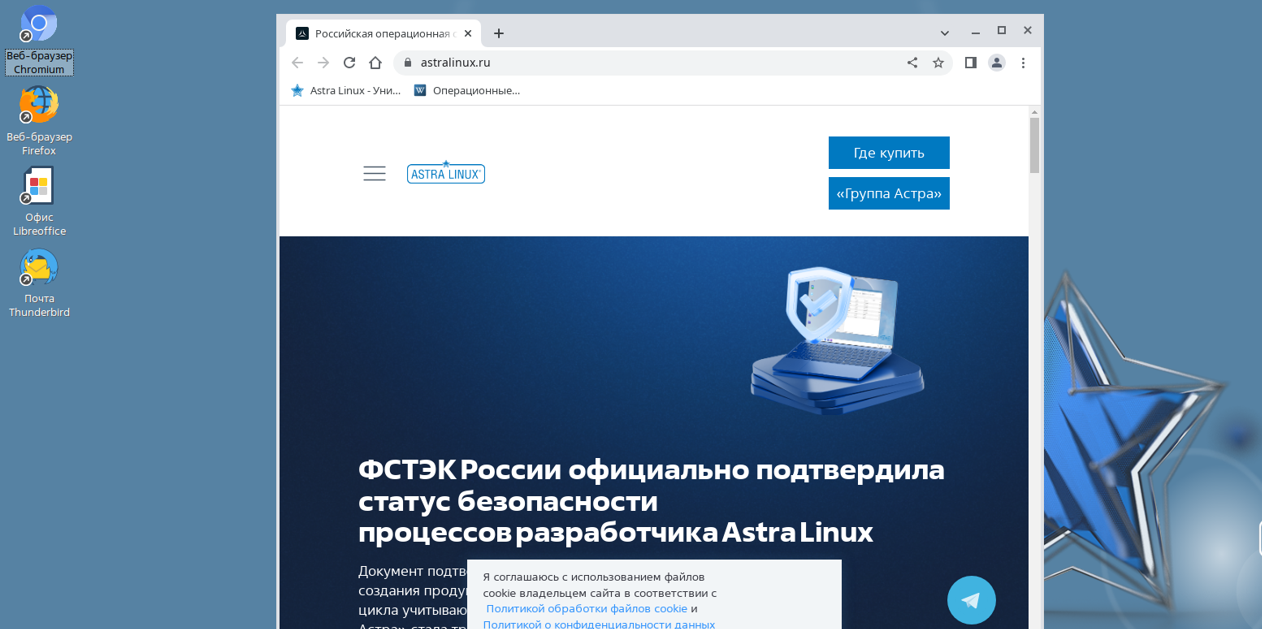


Рисунок 5 – Вход под user5

7) Войдите в ОС под пользователем sa на высоком уровне целостности и по аналогии с предыдущими пунктами задайте для пользователя user6 режим графического киоска с запуском одного приложения. В качестве приложения выберите веб-браузер Chromium.

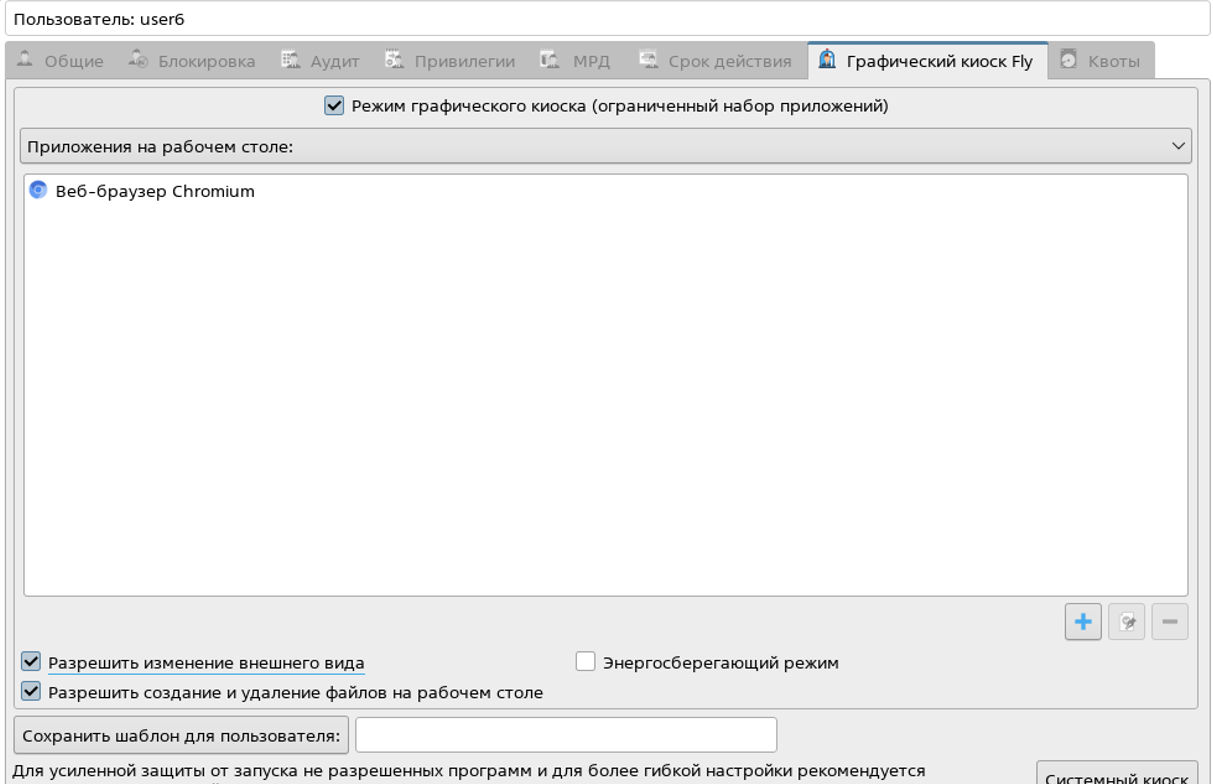


Рисунок 6 – Режим графического киоска с запуском одного приложения

8) После этого войдите в ОС под пользователем user6 и убедитесь, что запускается только одно приложение - веб-браузер Chromium. Закрыв браузер, выйдите из ОС.

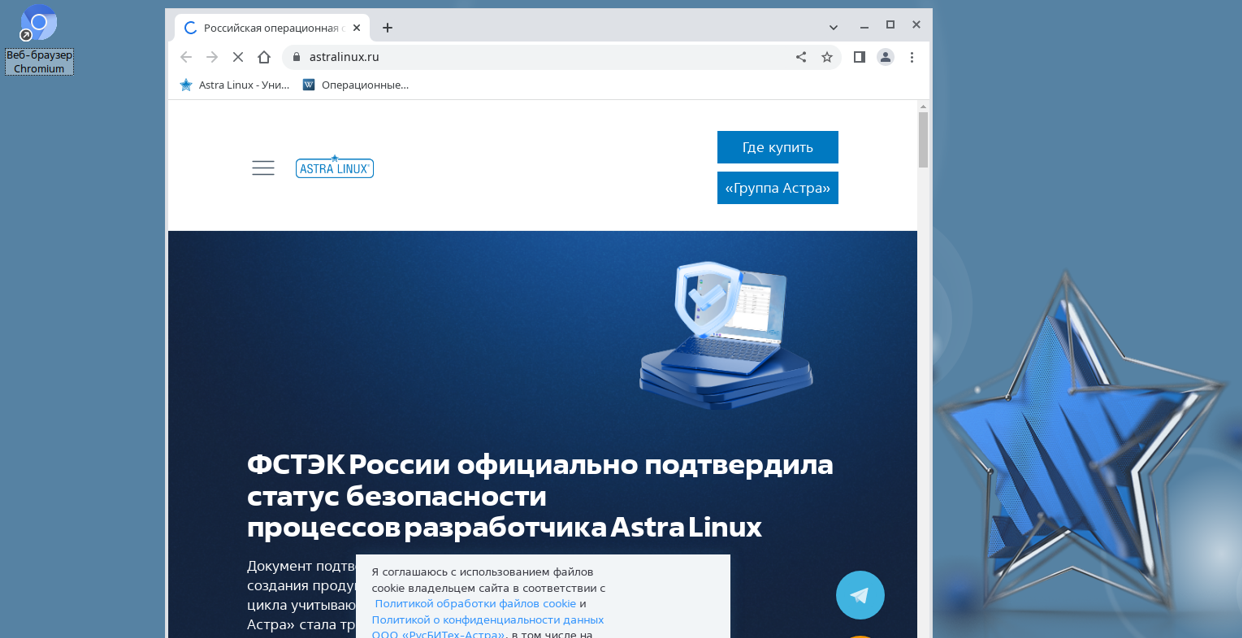


Рисунок 7 – Запуск одного приложения

9-10) Войдите в ОС под пользователем sa на высоком уровне целостности. Настройте работу в системном киоске, для этого:   
• откройте приложение Пуск → Параметры → Панель управления →Безопасность → Системный киоск;   
• на верхней панели инструментов нажмите + и добавьте профиль для нового пользователя user7;   
• выделив пользователя user7 справа в окне Профили, выберите в качестве профиля пользователя everything;   
• после этого включите режим киоска, выбрав в верхнем меню Файл → Включить режим киоска;   
• во всплывающем сообщении Несохраненные изменения нажмите Да.   
• в окне с требованием аутентификации введите пароль пользователя sa и нажмите Да.

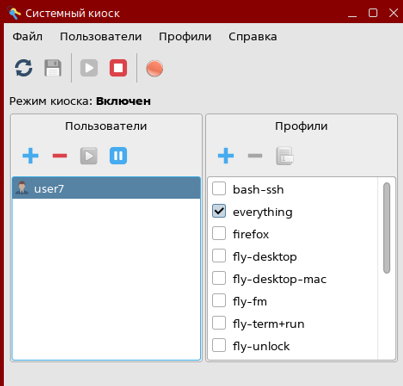


Рисунок 8 – Настройка работы в системном киоске

11) Войдите в ОС под пользователем user7 и убедитесь, что пользователю доступен стандартный функционал системы (откройте браузер, создайте файлы на рабочем столе и в домашнем каталоге, откройте любое доступное приложение из меню Пуск).

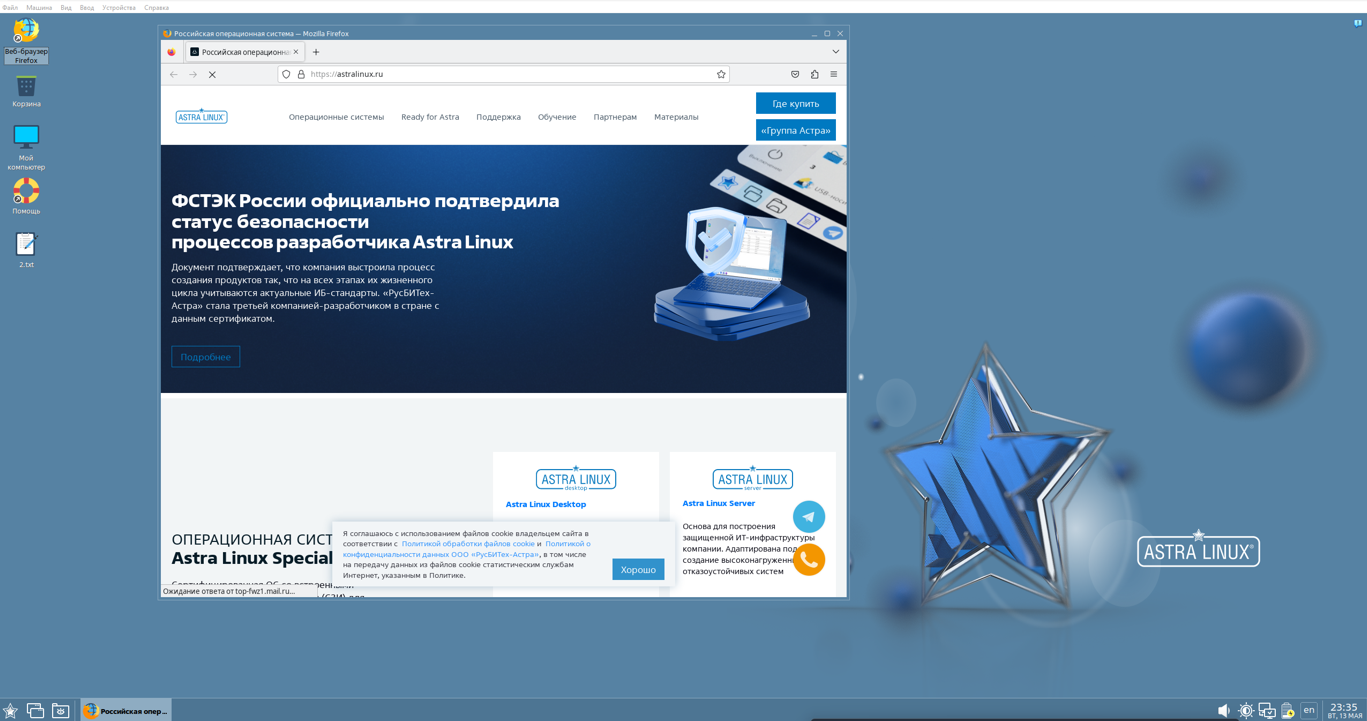


Рисунок 9 – Функционал системы для user7

**Вопросы**

**1)** Что реализуют политики мандатного контроля целостности?- Распределение информации в системе или её компонентах по некоторым явно заданным уровням и назначение прав доступа на основе заданных уровней

**2)** Какой уровень целостности является минимальным?- 0 (нулю)

**3**) Какой уровень целостности присваивается привилегированному пользователю?

- Максимальный, по умолчанию 63

**4)** Для чего предназначен режим графического киоска в Astra Linux? **-** Графический киоск позволяет ограничить запуск программ локальным пользователям. Графический киоск ограничивает доступ на уровне графической среды.

**5)** В какой программе настраивается графический киоск?   
- Графический киоск настраивается в программе управления политикой безопасности и может быть включен для отдельного пользователя и/или для группы пользователей.

**6)** Для чего предназначен системный киоск?

- Это инструмент системы PARSEC для ограничения возможностей, предоставляемых непривилегированным пользователям.

**7)** От чего зависит цветовая индикация интерфейса?- Зависит от уровня конфиденциальности. Цвета зарезервированы за каждым уровнем конфиденциальности. За нулевым уровнем закреплён голубой цвет. За первым – желтый. За вторым уровнем закреплён оранжевый цвет. За третьим — тёмно-розовый. За четвёртым — красный.

**8)** На что влияет установка минимальной категории конфиденциальности пользователя?

- Определяет обязательный набор категорий, которые будут активны при входе пользователя

**9)** На каком уровне защищённости доступно редактирование мандатных атрибутов?  
- На уровне защищенности **"**Смоленск**"** (максимальный уровень в PARSEC).

**10)** Как изменить мандатные атрибуты объекта?  
- Устанавливает максимальное количество процессов для текущего пользователя

**11)** Что может сделать субъект имеющий первый уровень конфиденциальности с объектом, имеющим второй уровень?  
- Читать или изменять объект уровня 2. Увидеть объект в списке файлов (если не включены специальные атрибуты).

**Вывод**

В данной лабораторной работе я познакомимся с подсистемой безопасности PARSEC.