МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)**

Факультет компьютерных технологий и прикладной математики
Кафедра информационных технологий

ОТЧЕТ О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ №7 «БАЗОВЫЙ КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ»

по дисциплине
«ОПЕРАЦИОННЫЕ СИСТЕМЫ»

Выполнила,
студентка группы МО32 _____С.Н. Чупрова
(подпись, дата)

Направление подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем
Курс 3

Отчет принял,
преподаватель кафедры ИТ, доцент _____А.А. Полупанов
(подпись, дата)

Краснодар
2025

Задание 1.

1. Войдите в ОС с учетной записью пользователя sa (Уровень_0, Высокий).

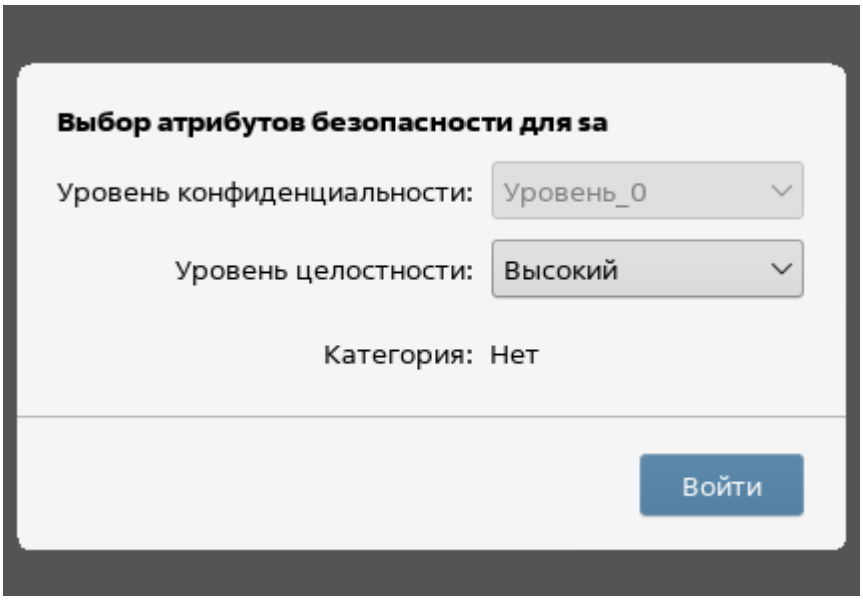

Рисунок 1 – Вход в ОС с учетной записью sa

2. Запустите графическую утилиту редактирования учетных записей пользователей.

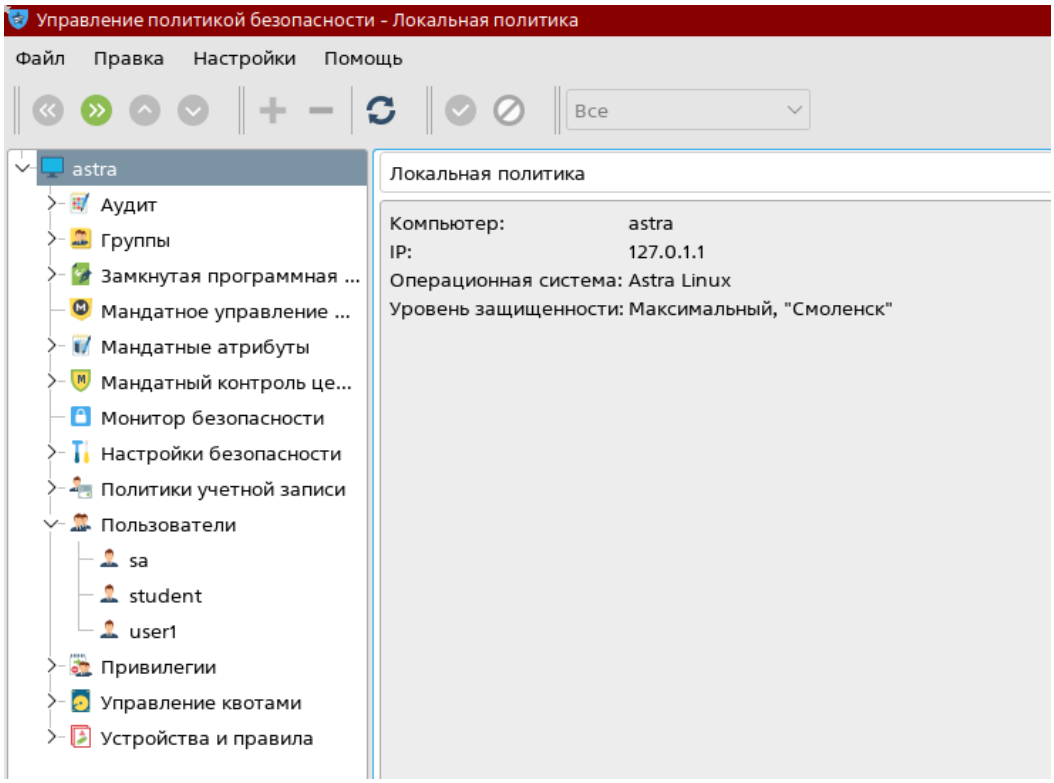

Рисунок 2 – Графическая утилита редактирования учетных записей

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

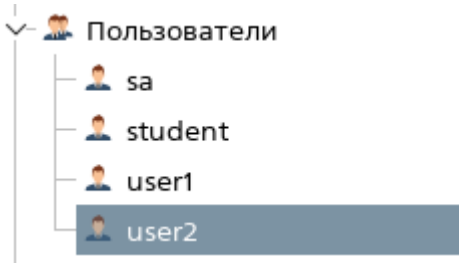

Рисунок 3 – Новые пользователи

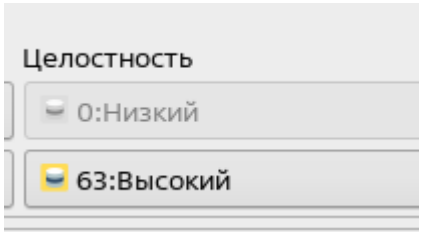

Рисунок 4 – Уровень целостности пользователей user1, user2

4. Войдите в ОС с учетной записью пользователя user2, выбрав уровень доступа Уровень_0, Высокий.

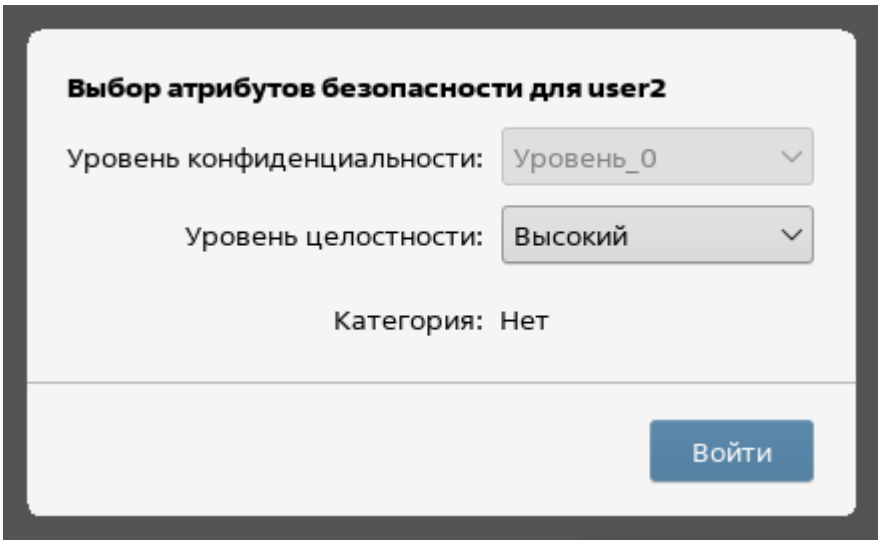

Рисунок 5 – Вход в ОС с учетной записью пользователя user2

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

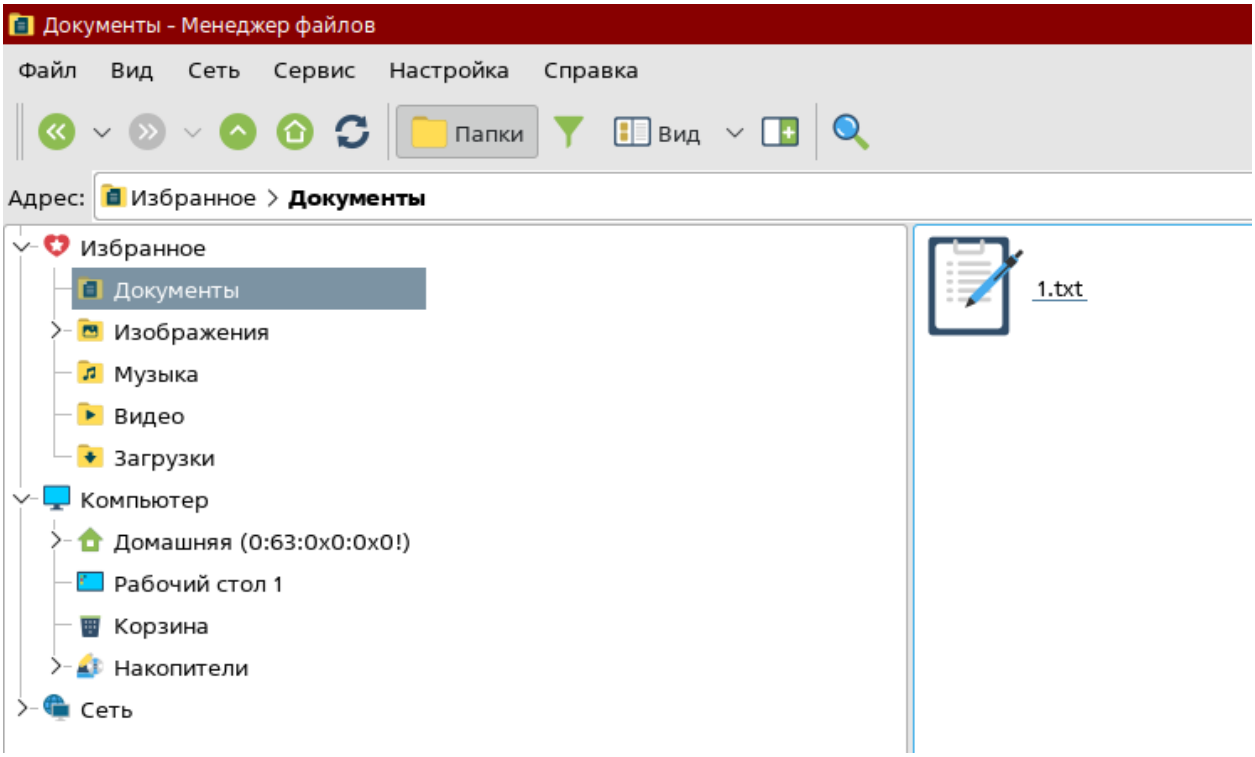

Рисунок 6 – Созданный файл 1.txt

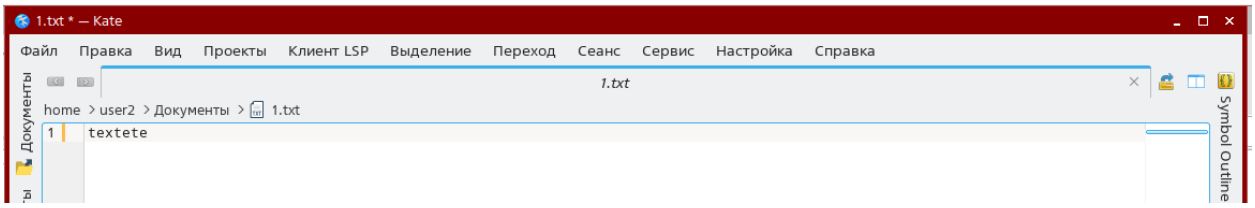

Рисунок 7 – Текст файла

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

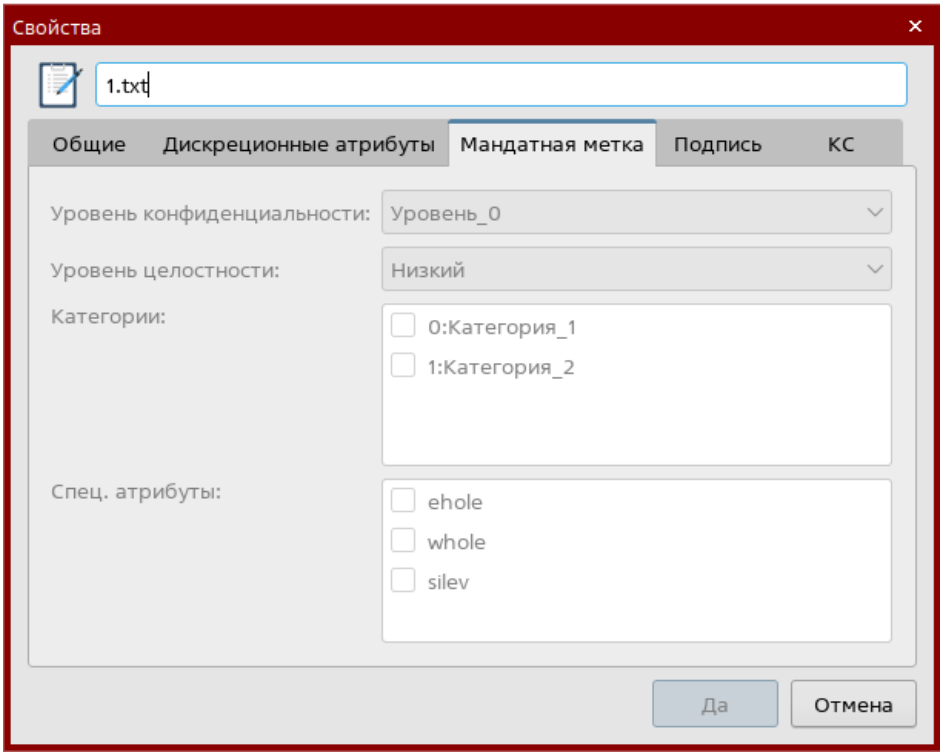

Рисунок 8 – Уровень целостности файла

7. Выйдите из ОС.

8. Войдите в ОС с учетной записью пользователя sa (Уровень_0, Высокий).

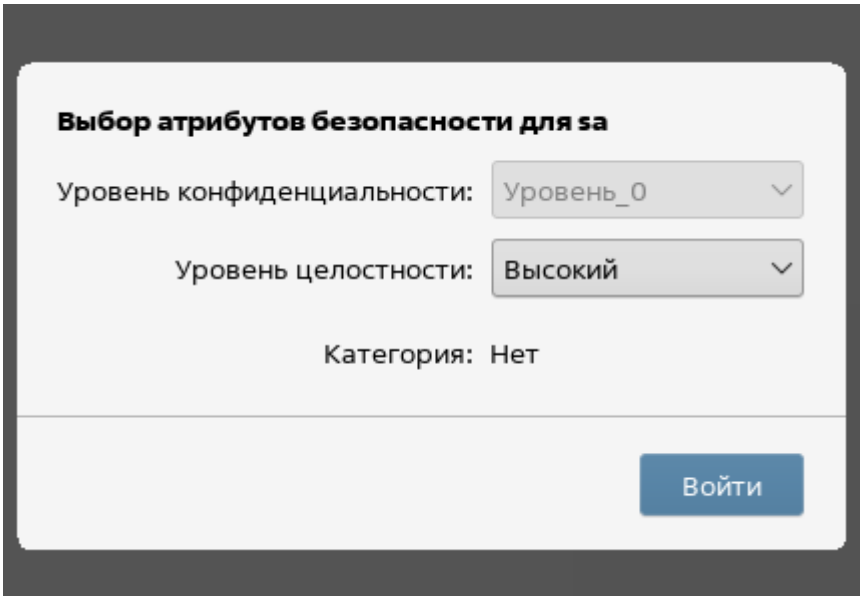

Рисунок 9 – Повторный вход в ОС с записью пользователя sa

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.

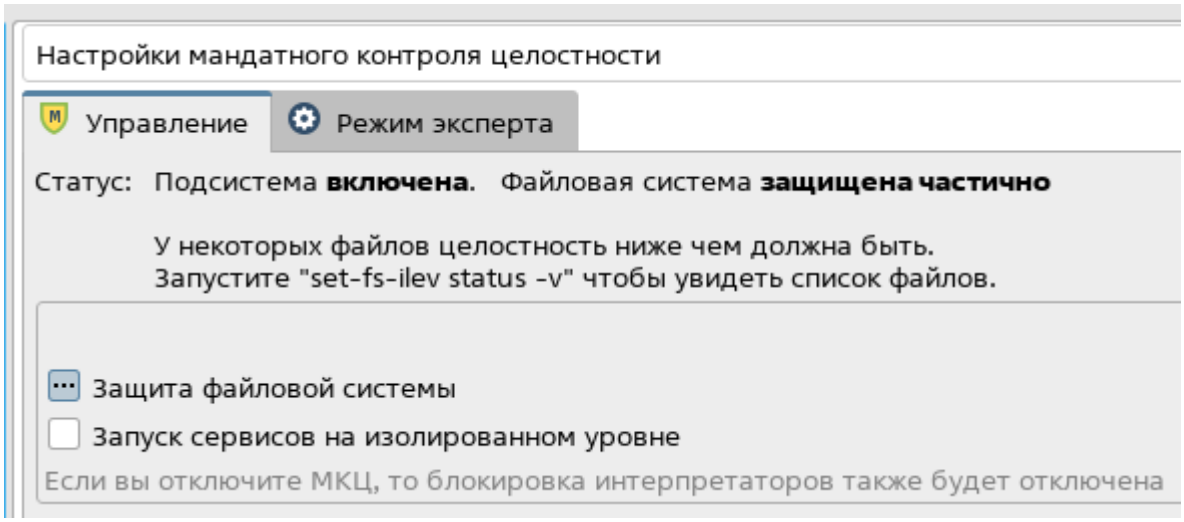

Рисунок 10 – Статус режима мандатного контроля

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 11 – Изменение уровня целостности пользователя user2

11. Войдите в ОС с учетной записью пользователя user2, выбрав уровень доступа Уровень_0, Высокий.

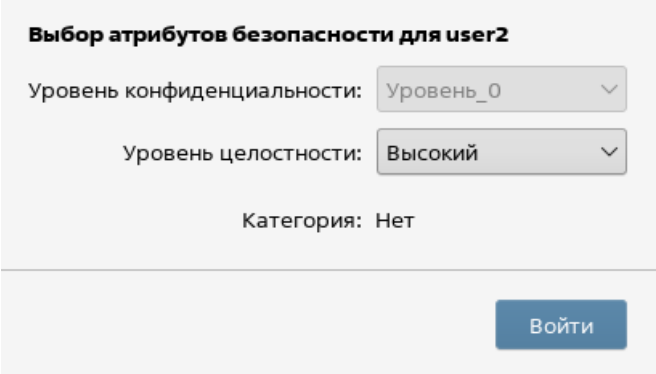

Рисунок 12 – Повторный вход в ОС с записью пользователя user2

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

Файл был успешно изменен, так как пользователь имеет максимальный уровень целостности. Субъект с определенным уровнем целостности может получить доступ на запись к сущности, если его уровень целостности не ниже уровня целостности сущности

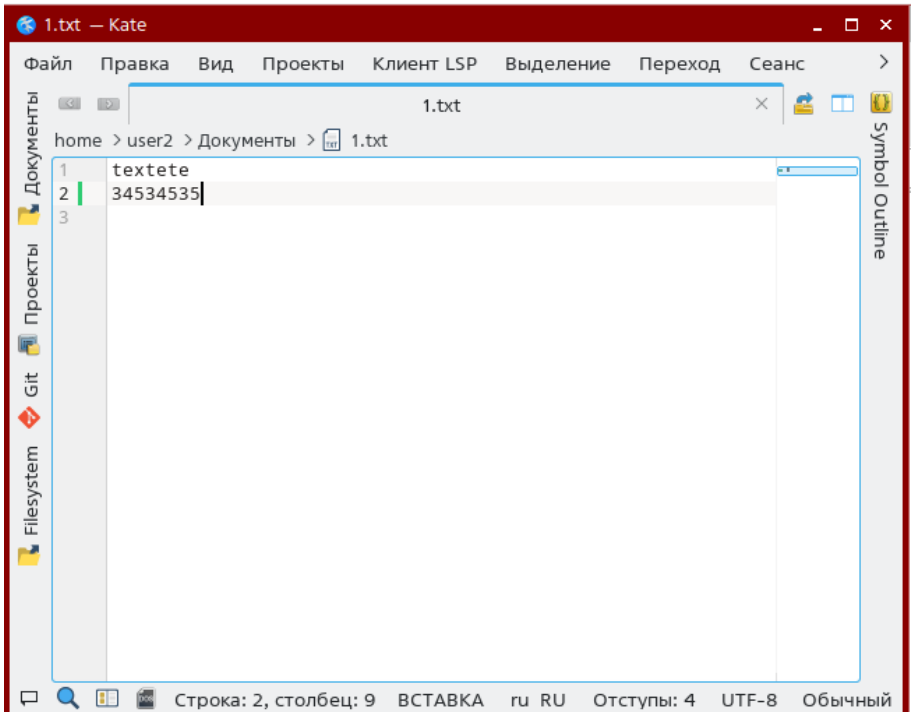

Рисунок 13 – Внесенные в файл изменения

Задание 2.

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

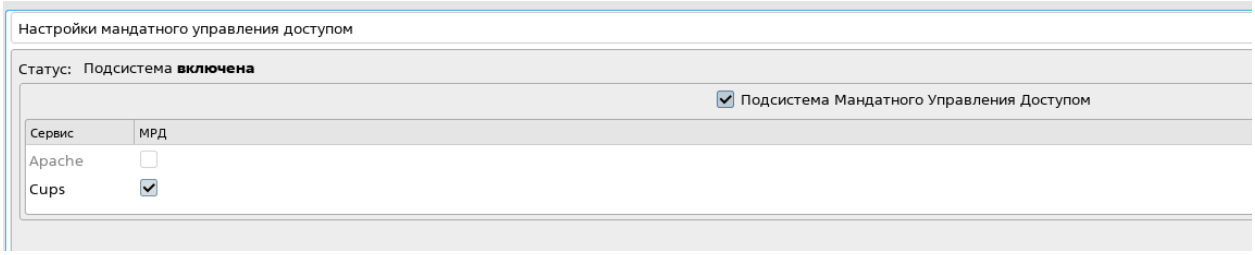

Рисунок 14 – Графическая утилита Мандатное управление доступом

2. Переименуйте уровни конфиденциальности:

- 0 - for _all;
- 1 - secret;
- 2 - very_secret;
- 3 - very_important.

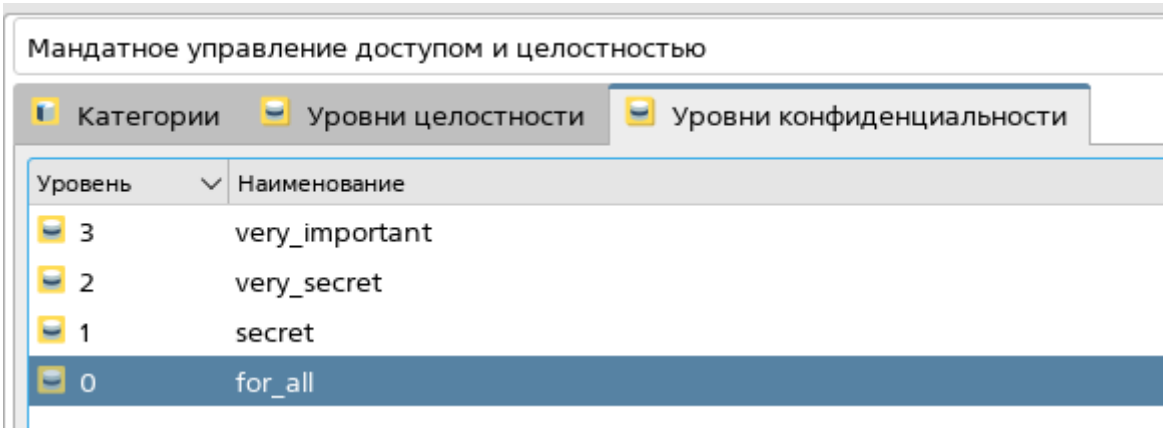

Рисунок 15 – Переименованные уровни конфиденциальности

3. Создайте учетную запись для пользователя ivanov:

• минимальный уровень конфиденциальности - for_all;

• максимальный уровень конфиденциальности - very_secret.

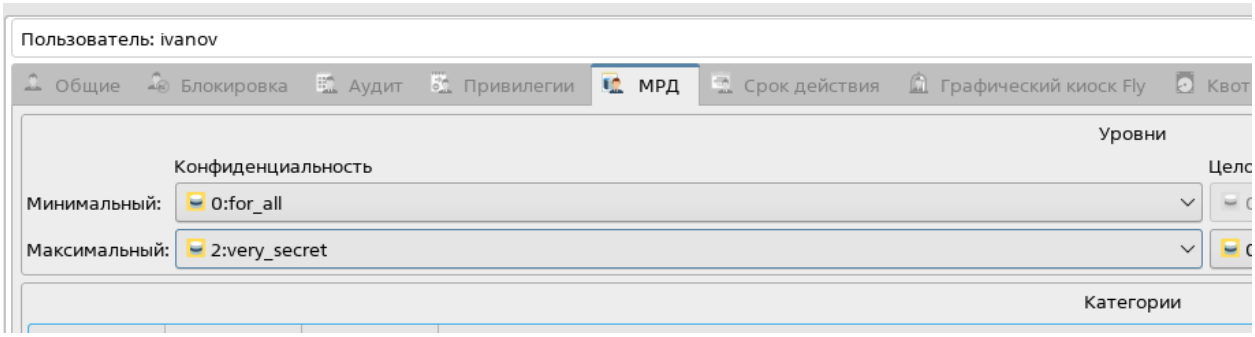

Рисунок 16 – Учетная запись пользователя ivanov

4. Создайте учетную запись для пользователя petrov:

• минимальный уровень конфиденциальности - for_all;

• максимальный уровень конфиденциальности – secret.

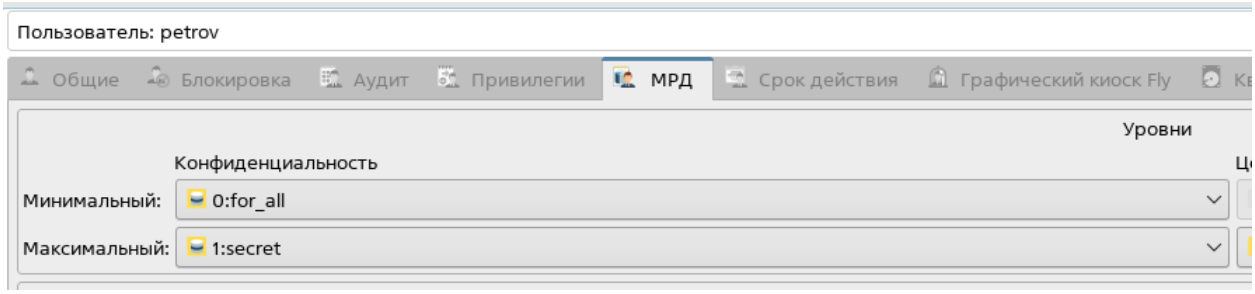

Рисунок 17 – Учетная запись пользователя petrov

Задание 3.

1. Создайте каталог /home/project. Установите на каталог уровень конфиденциальности very_important и дополнительный атрибут ccnr.

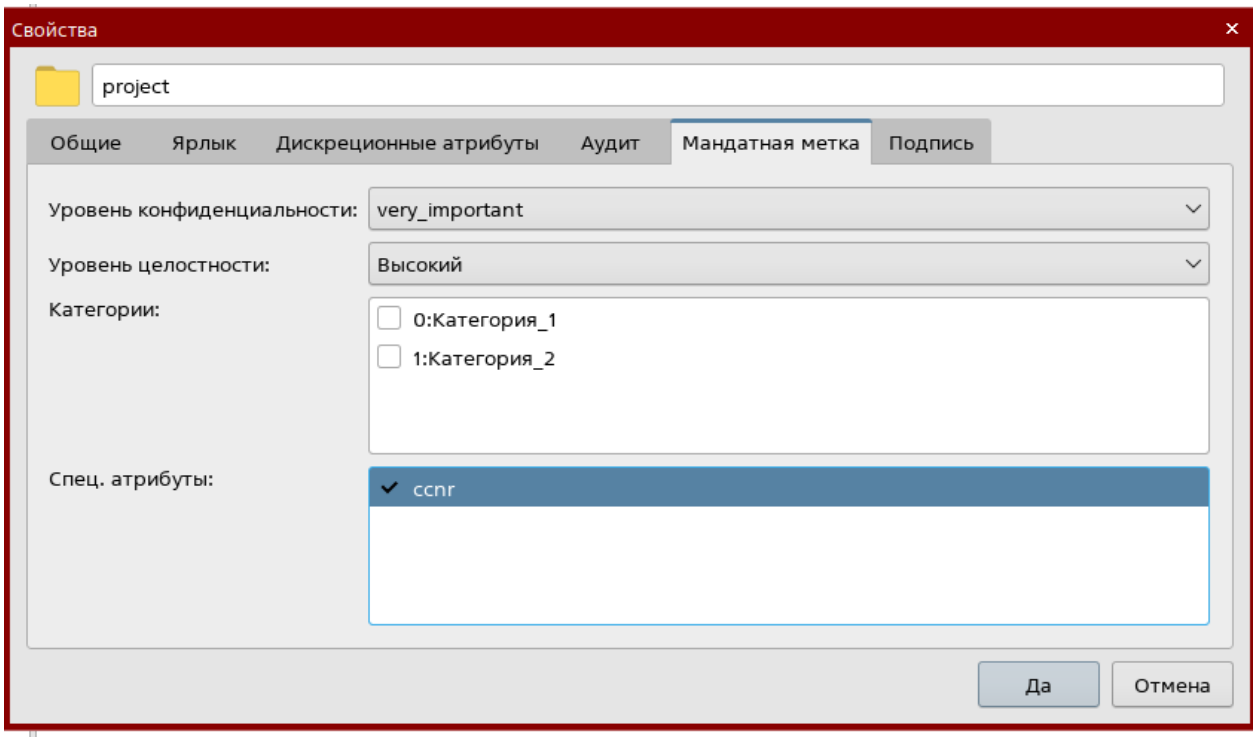

Рисунок 18 – Мандатные метки каталога project

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

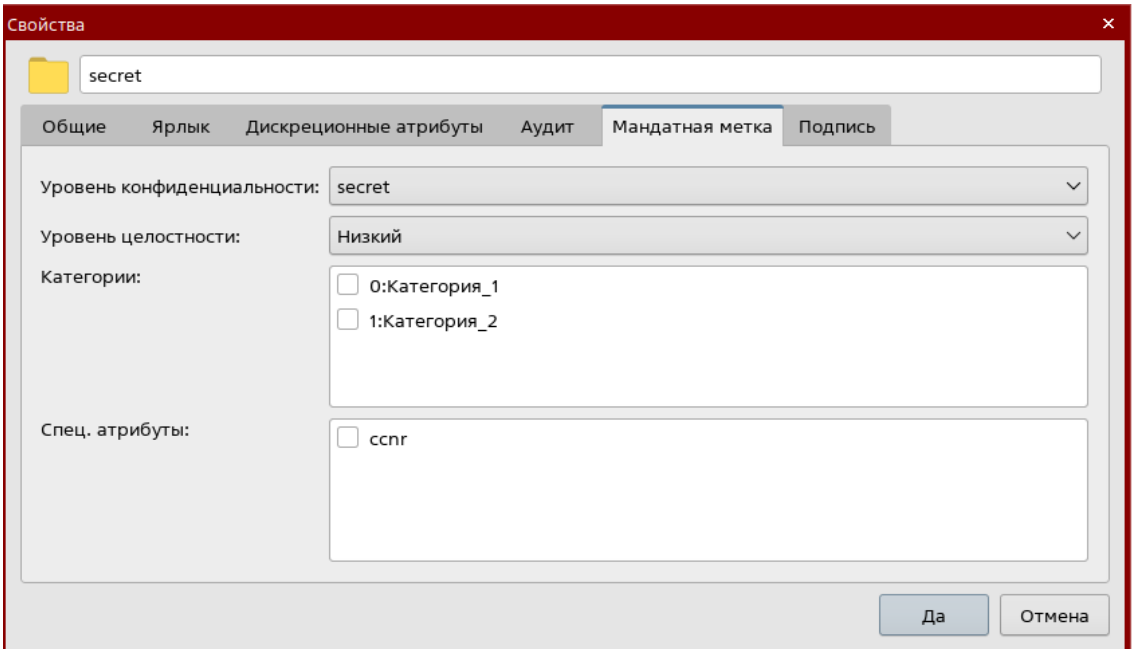

Рисунок 19 – Мандатные метки каталога secret

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

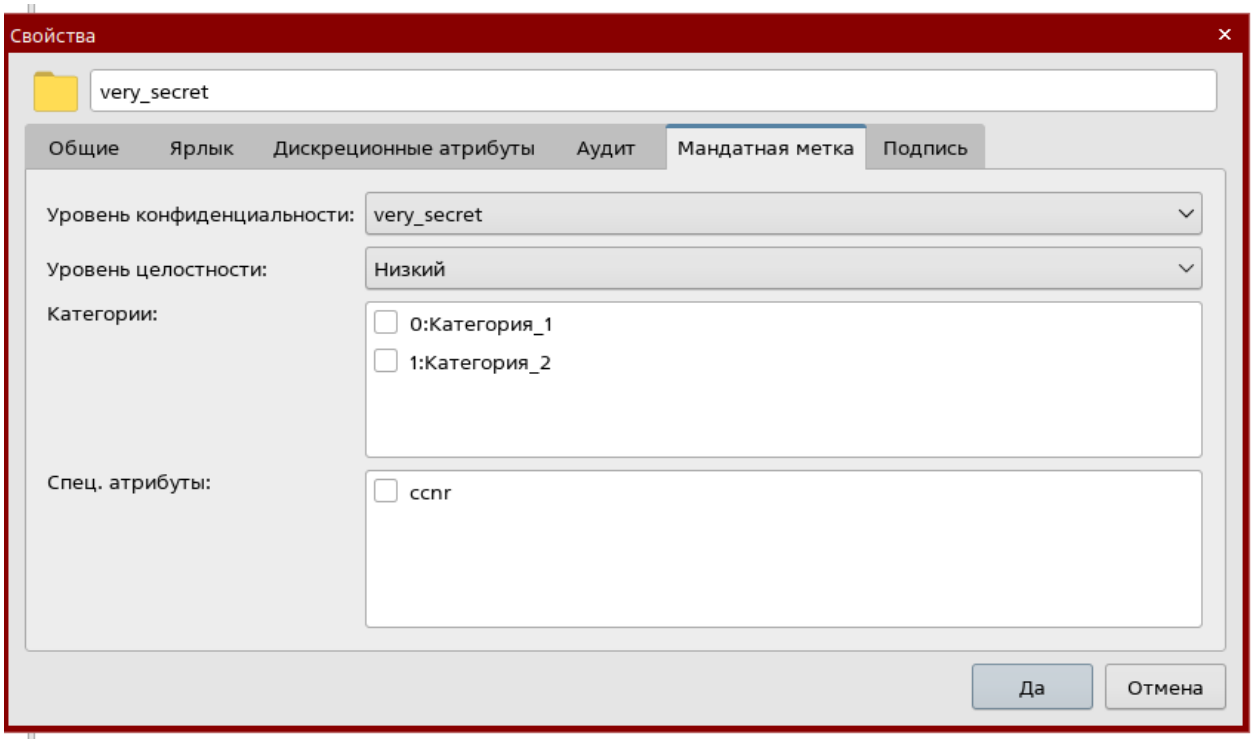

Рисунок 20 – Мандатные метки каталога very_secret

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.

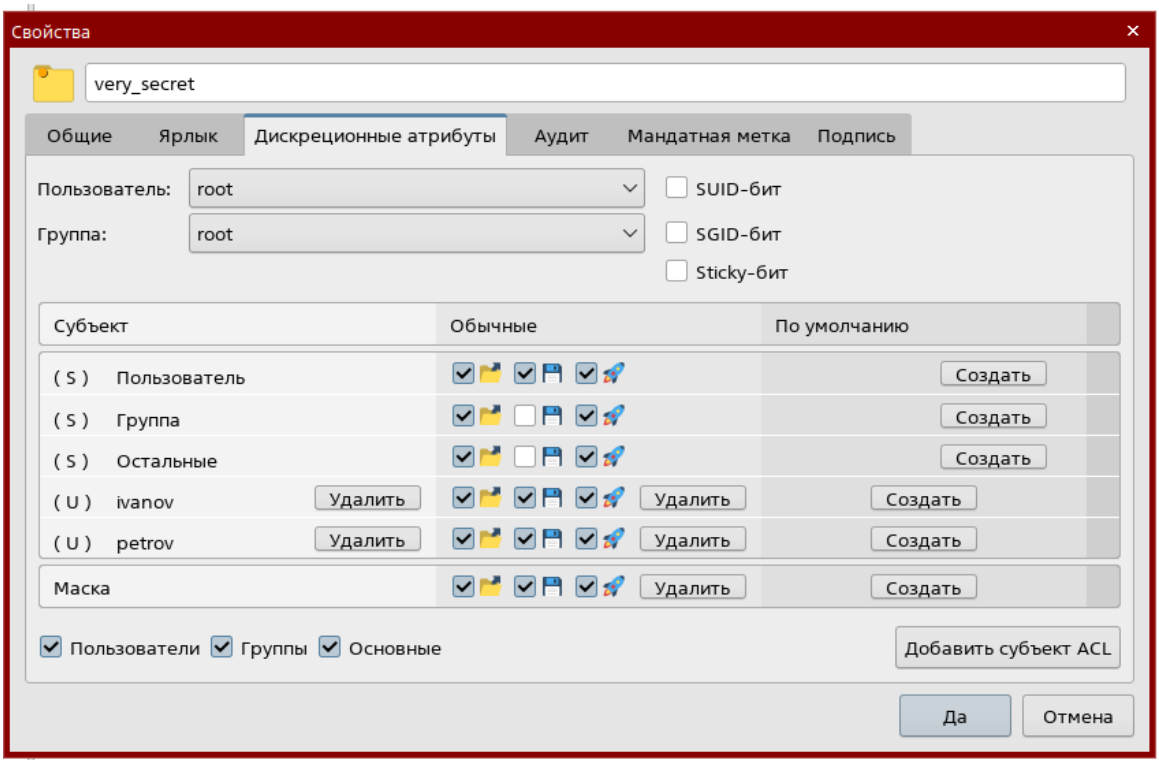

Рисунок 21 – Установленные списки управления доступом

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

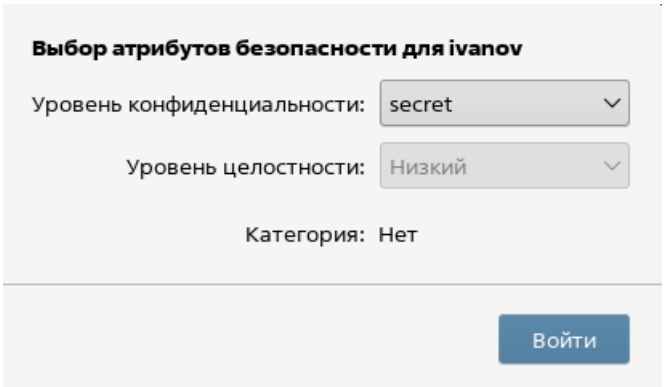

Рисунок 22 – Вход в систему под записью ivanov

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?

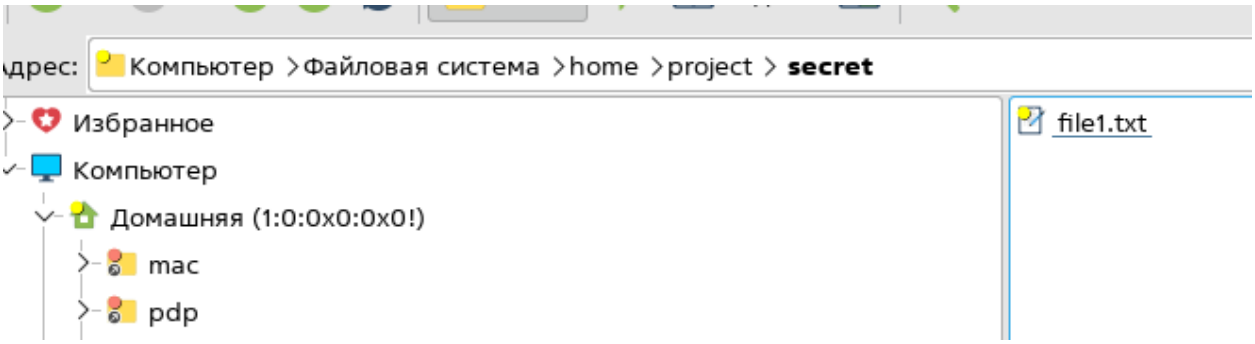

Рисунок 23 – Созданный файл

7. Виден ли каталог /home/project/very _secret?

Каталог /home/project/very _secret не виден:

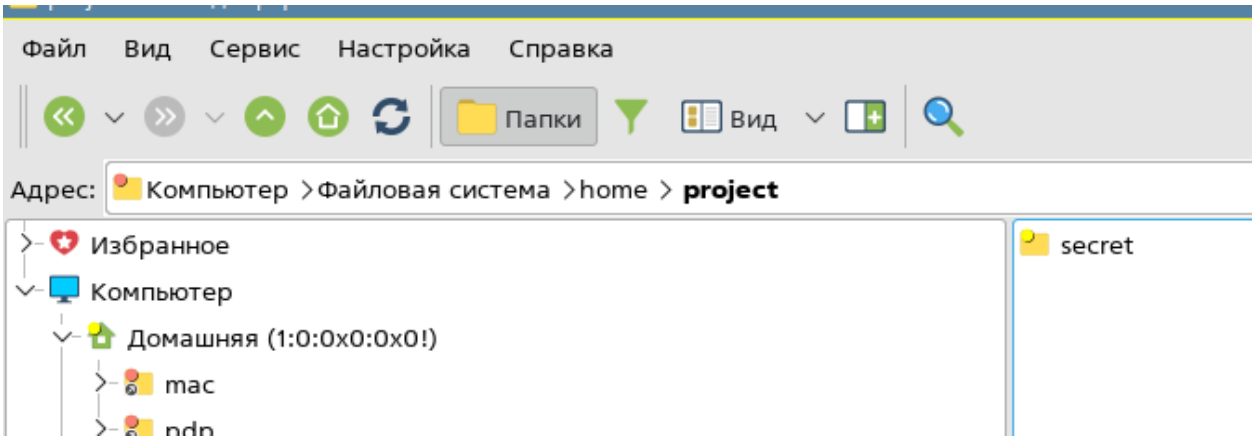

Рисунок 24 – Видимое содержимое каталога

8. Зайдите под учетной записью ivanov в систему с уровнем конфиденциальности very_secret.

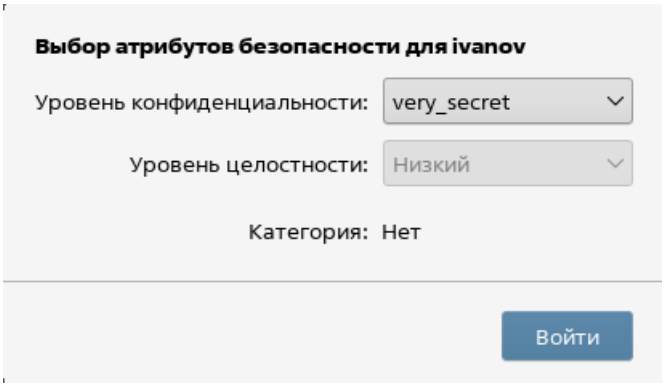

Рисунок 25 – Вход под записью с другим уровнем конфиденциальности

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

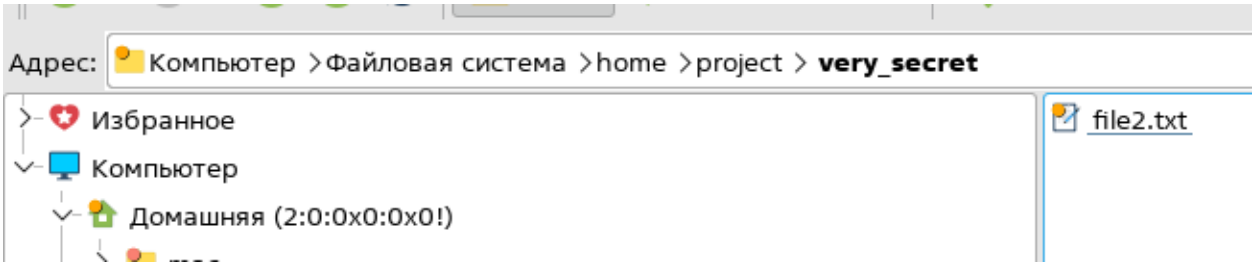

Рисунок 26 – Сохраненный файл

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

Рисунок 27 – Видимое содержимое каталога с другим уровнем конфиденциальности

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

Рисунок 28 – Видимый файл file1

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

Не удалось изменить файл:

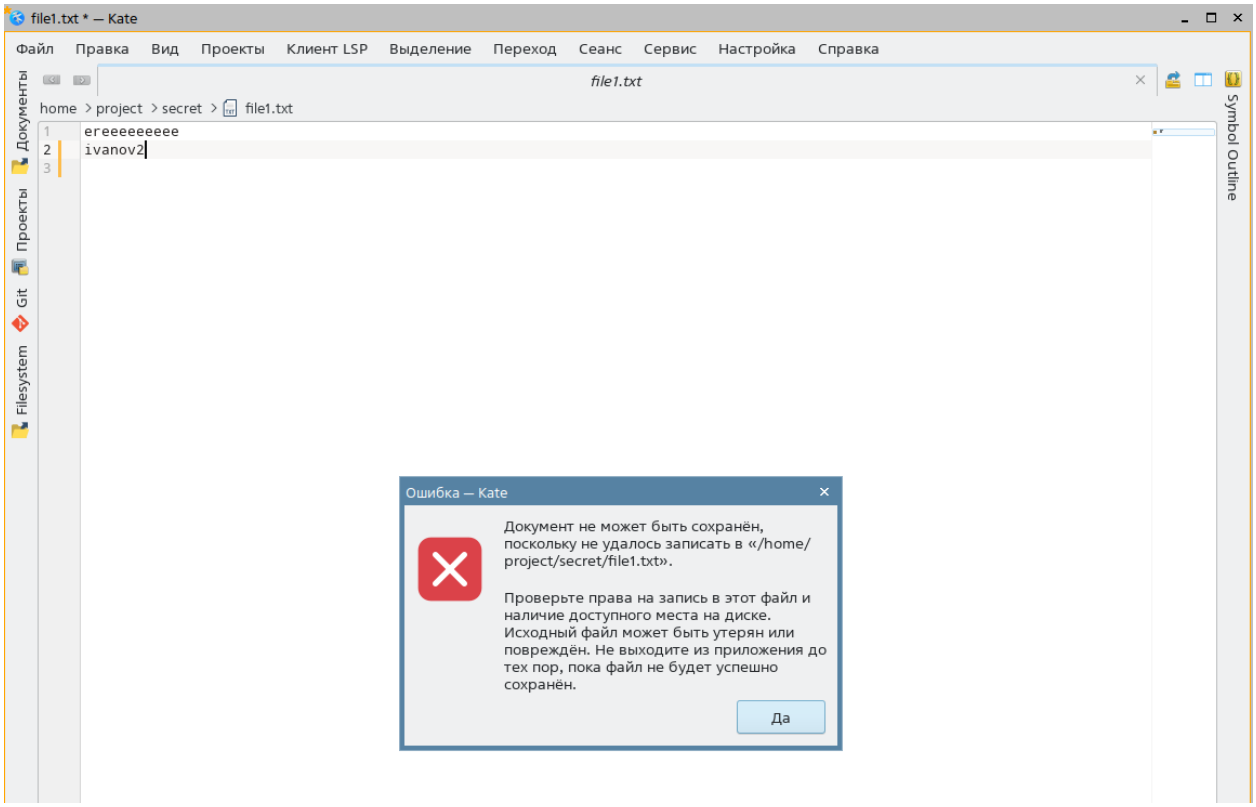

Рисунок 29 – Ошибка при попытке изменить файл

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

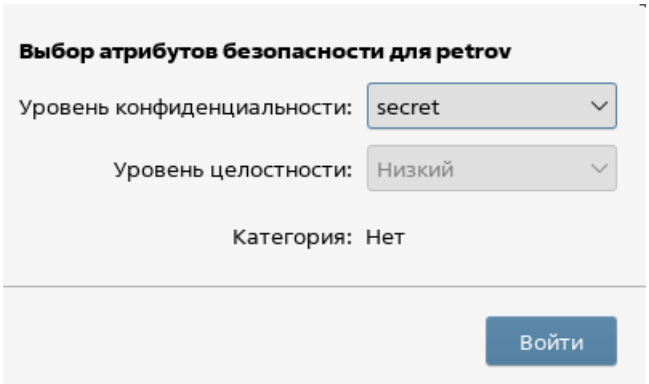

Рисунок 30 – Вход в систему под записью пользователя petrov

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

Изменить содержимое файла не удалось:

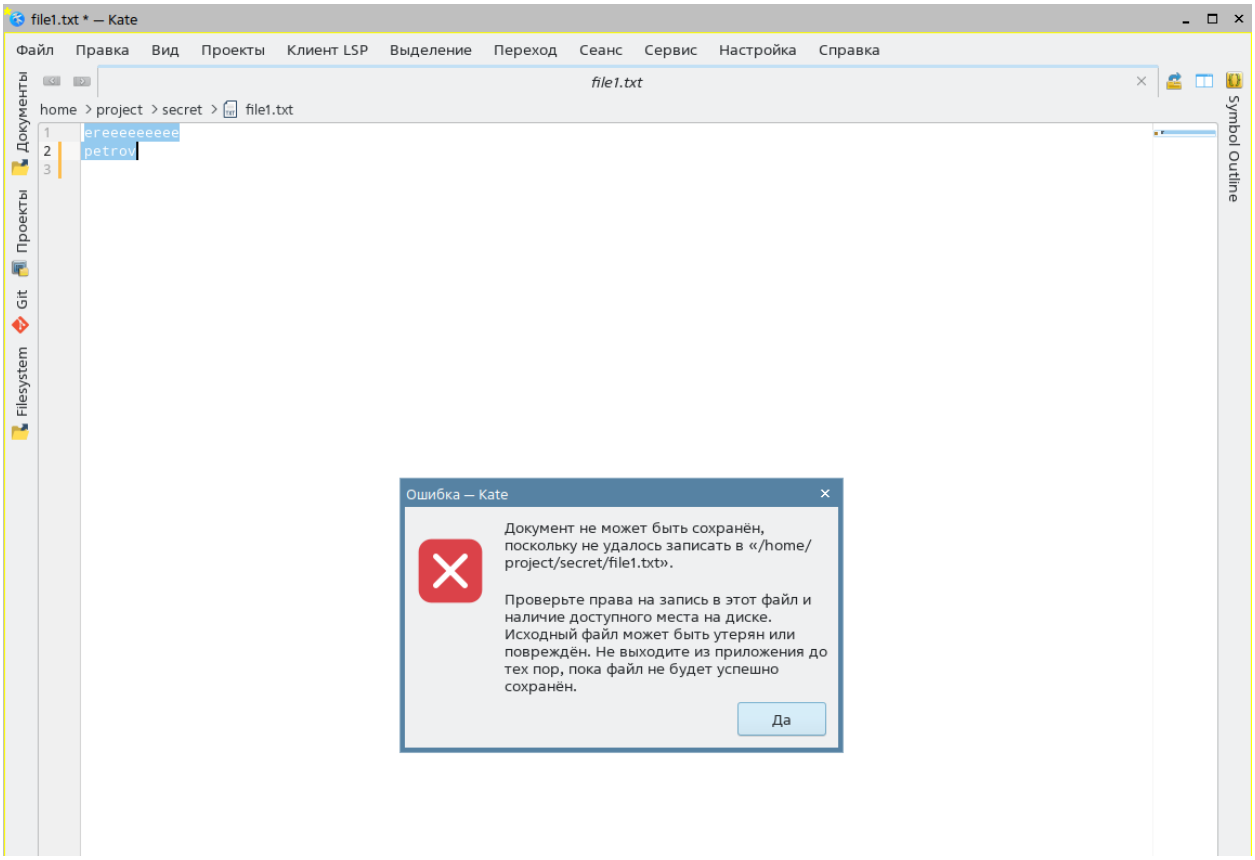

Рисунок 31 – Попытка изменить содержимое файла

15. Можете ли вы прочитать содержимое файла /home/project/very _secret/file2.txt?

Прочитать содержимое файла нельзя

Рисунок 32 – Видимое содержимое каталога project

Задание 4.

1. Создайте пользователей user5, user6 и user7.

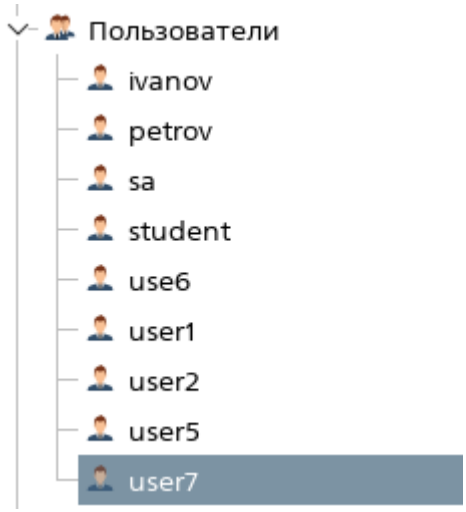

Рисунок 33 – Созданные пользователи

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;

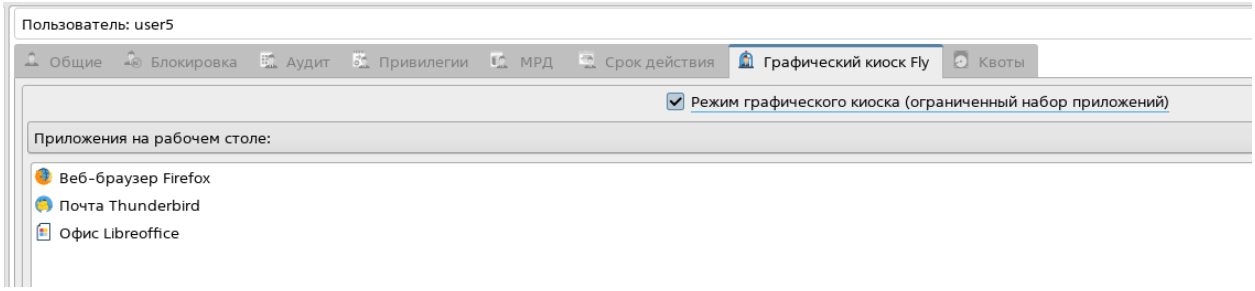

Рисунок 34 – Настройки графического киоска для user5

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?

Есть возможность открывать приложения и создавать файлы и каталоги:

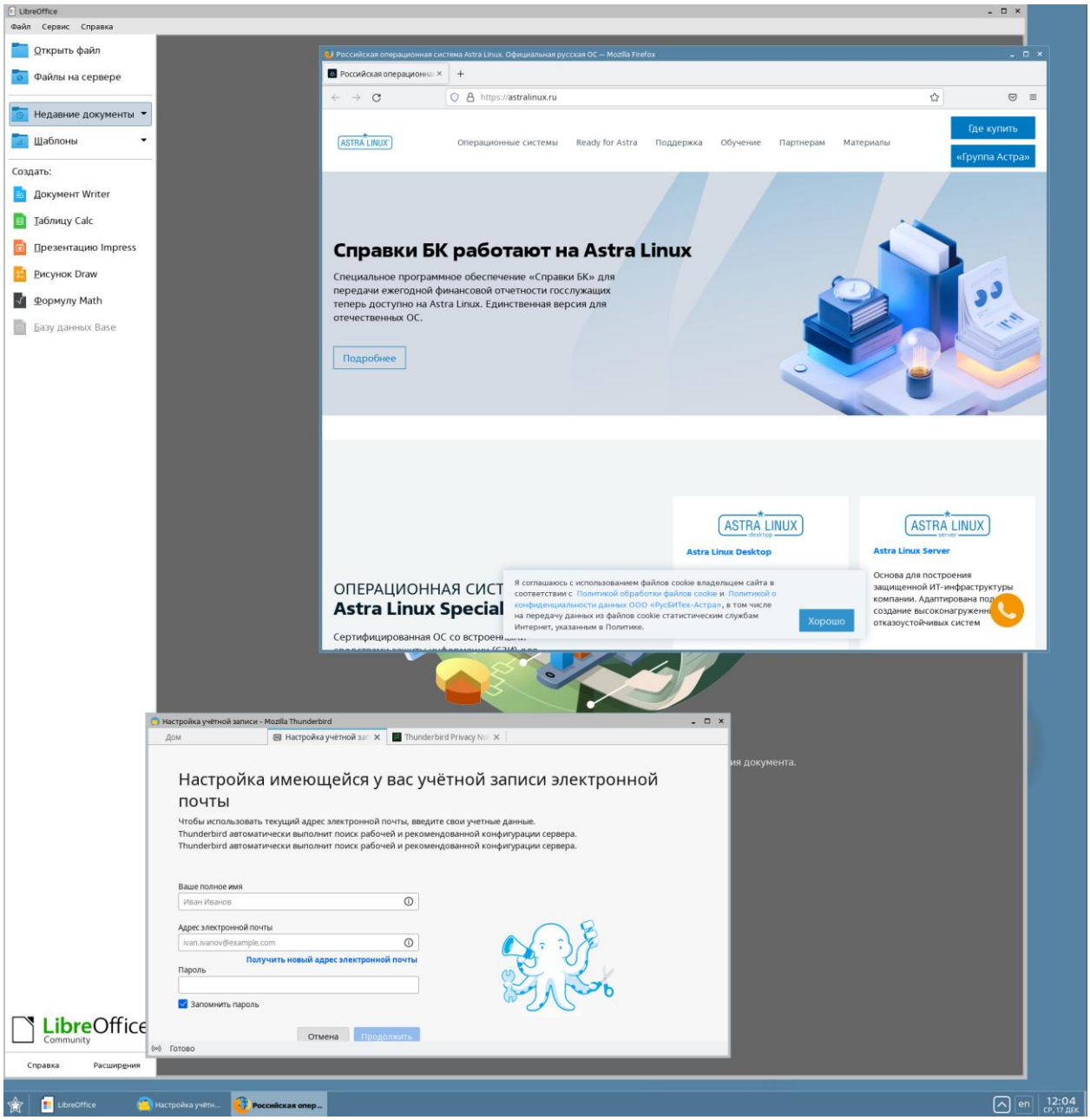

Рисунок 35 – Открытые приложения на рабочем столе

Можно создавать файлы, если в настройках киоска была поставлена галочка "Разрешить создание и удаление файлов на рабочем столе". Без этой галочки создание файлов было бы запрещено.

4. Войдите в ОС под пользователем sa на высоком уровне целостности.

5. 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 ярлык появился на рабочем столе. Путь для копирования: /etc/fly-kiosk/user5/desktop.

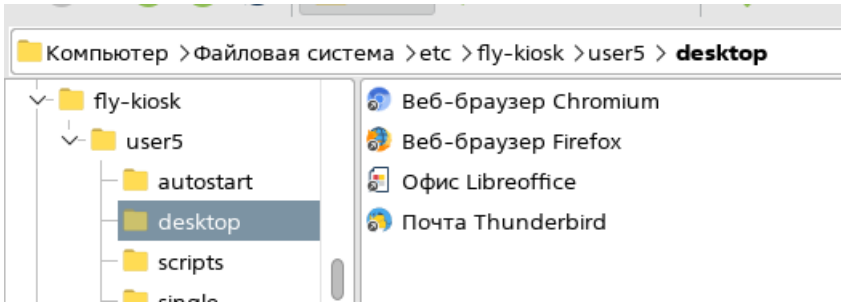

Рисунок 36 – Добавлен ярлык Веб-браузер Chromium

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

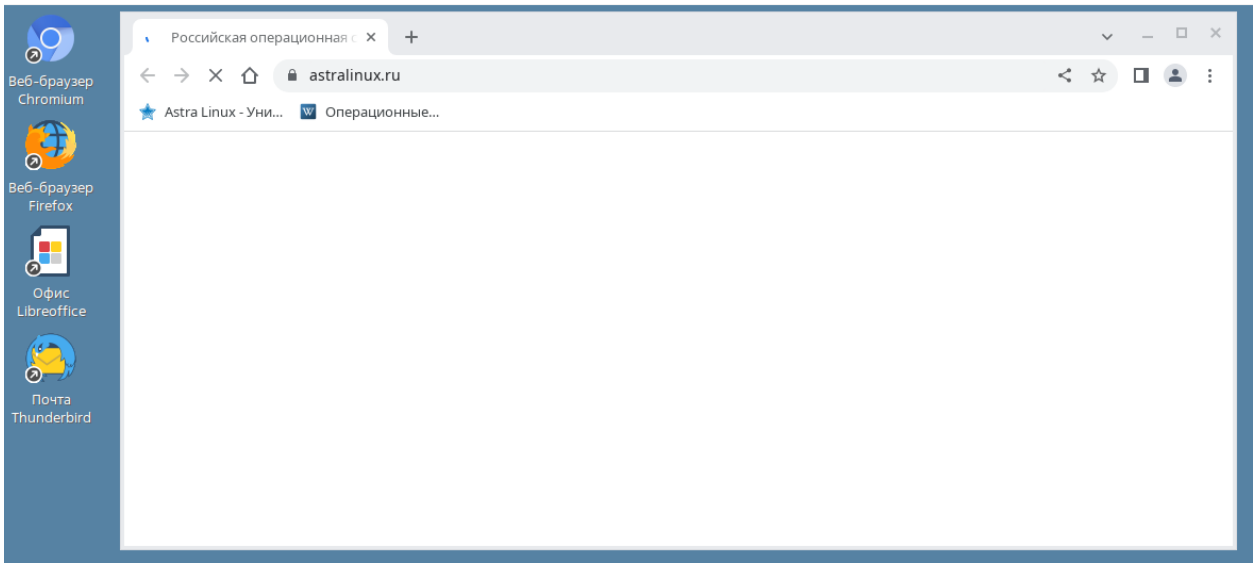

Рисунок 37 – Запуск веб-браузера

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.

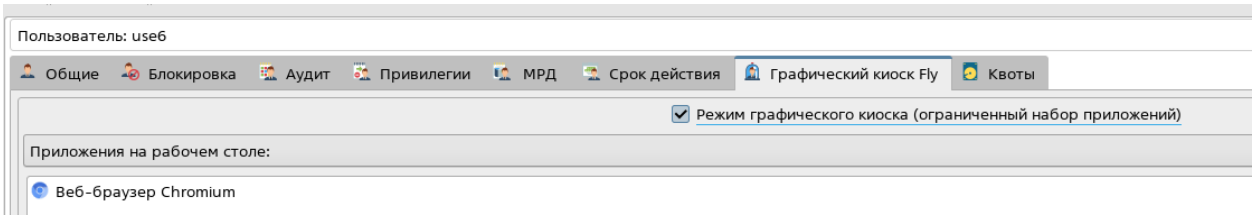

Рисунок 38 – Графический киоск пользователя user6

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

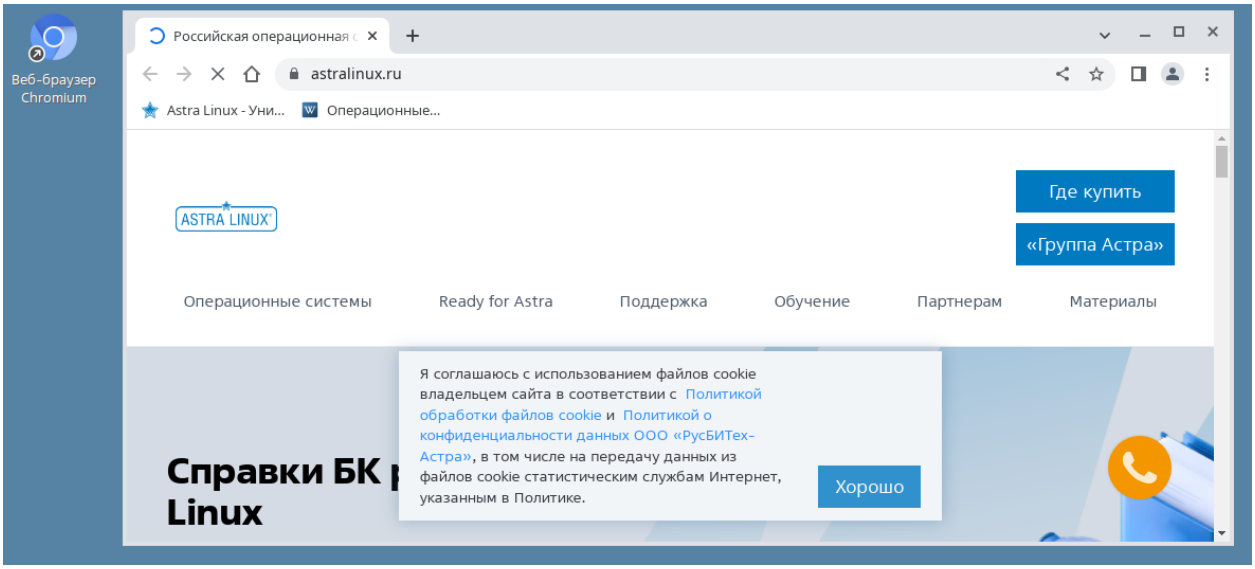

Рисунок 39 – Открытый браузер под записью user6

9. Войдите в ОС под пользователем sa на высоком уровне целостности.

10. 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.

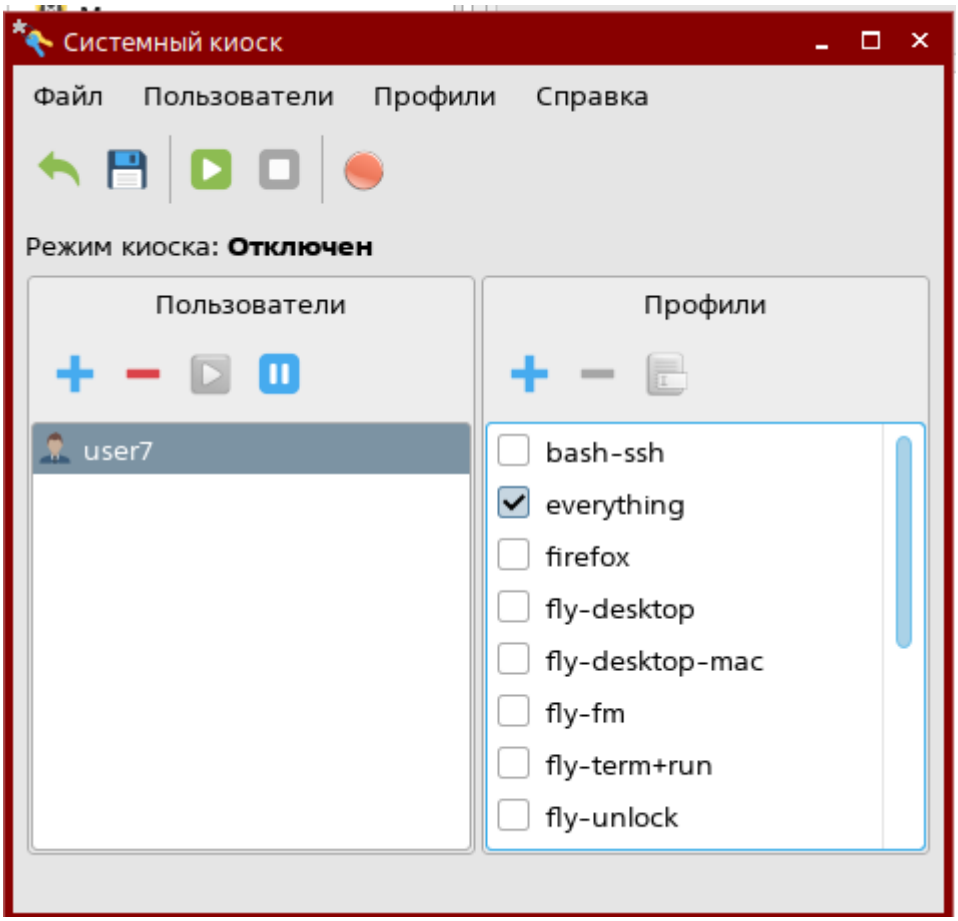

Рисунок 40 – Настройки системного киоска

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 41 – Созданный файл на рабочем столе

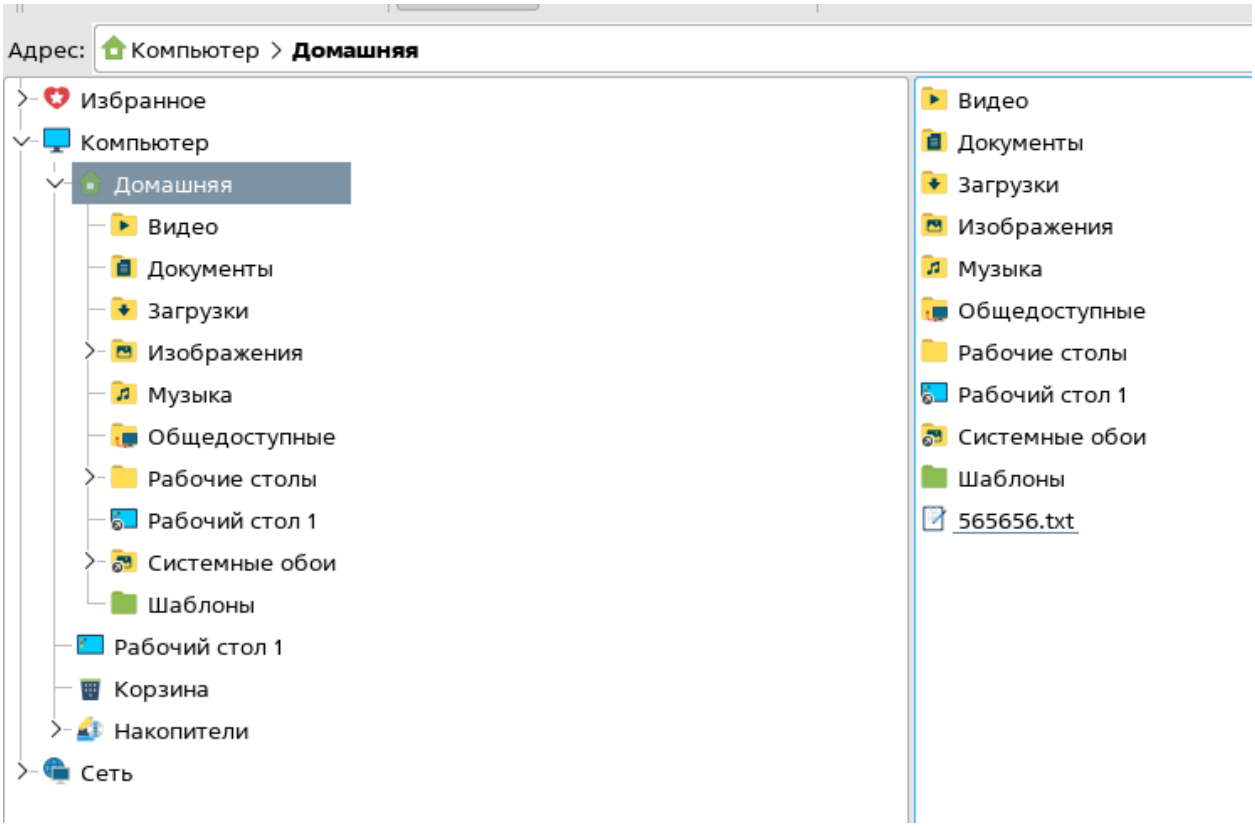

Рисунок 42 – Созданный файл в домашнем каталоге

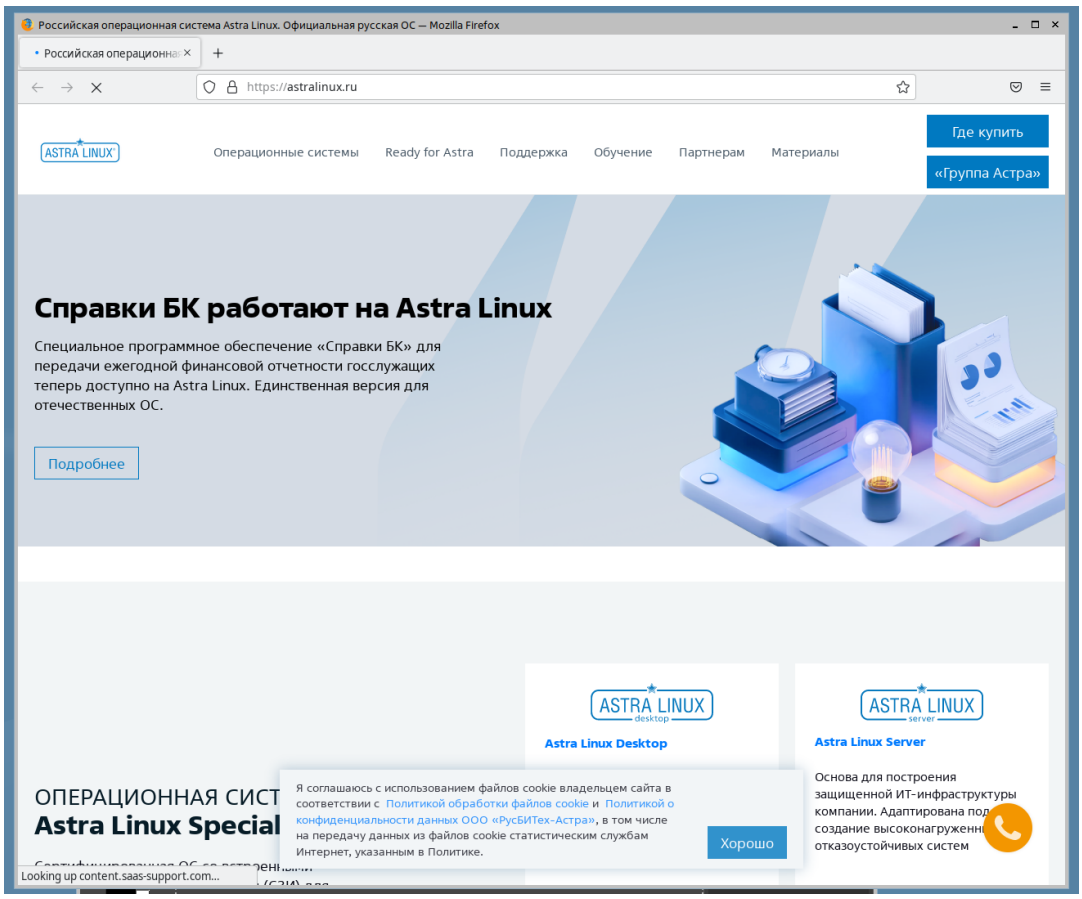

Рисунок 43 – Открытый браузер

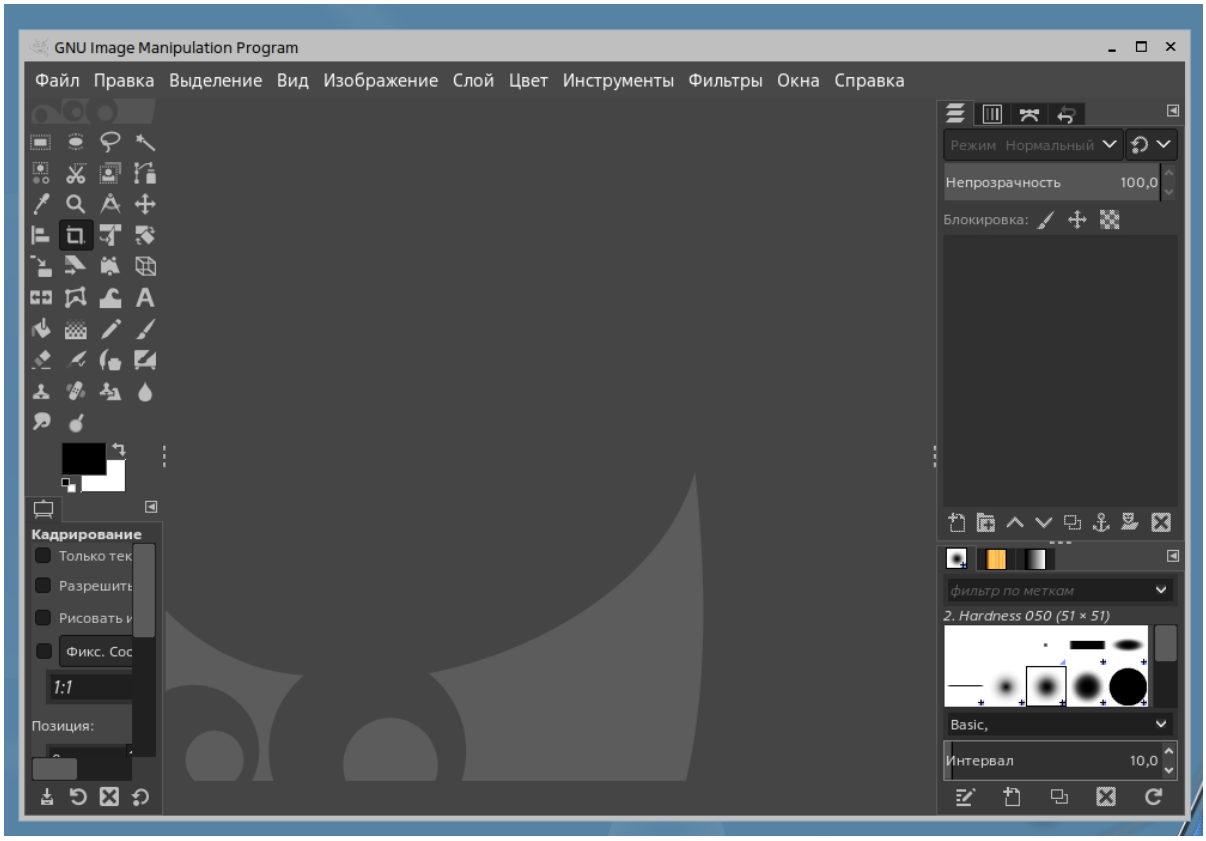

Рисунок 44 – Открытое приложение из меню Пуск

Вопросы

1. Что реализуют политики мандатного контроля целостности?

Политика мандатного контроля целостности реализует распределение информации в системе по явно заданным уровням целостности и назначение прав доступа на основе этих уровней. Основная цель – затруднить внедрение и функционирование программных закладок, а также предотвратить повреждение критически важных модулей ОС некорректно работающими программами.

2. Какой уровень целостности является минимальным?

Уровень 0.

3. Какой уровень целостности присваивается привилегированному пользователю?

Максимальный уровень целостности 63.

4. Для чего предназначен режим графического киоска в Astra Linux?

Режим графического киоска предназначен для ограничения запуска программ локальными пользователями на уровне графической среды. Пользователь может работать только с приложениями из заданного списка.

5. В какой программе настраивается графический киоск?

Графический киоск настраивается в программе управления политикой безопасности.

6. Для чего предназначен системный киоск?

Системный киоск (режим «Киоск-2») предназначен для ограничения возможностей непривилегированных пользователей на уровне ядра системы, на основе профилей доступа к файлам и каталогам.

7. От чего зависит цветовая индикация интерфейса?

Цветовая индикация интерфейса зависит от уровня конфиденциальности текущей сессии пользователя. Каждому уровню закреплён определённый цвет.

8. На что влияет установка минимальной категории конфиденциальности пользователя?

Установка минимальной категории конфиденциальности определяет категории, которые всегда будут выбраны по умолчанию при авторизации пользователя.

9. На каком уровне защищённости доступно редактирование мандатных атрибутов?

Редактирование мандатных атрибутов доступно только на максимальном уровне защищённости.

10. Как изменить мандатные атрибуты объекта?

Для изменения мандатных атрибутов необходимо авторизоваться под учетной записью с высоким уровнем целостности и запустить менеджер файлов от имени root.

11. Что может сделать субъект имеющий первый уровень конфиденциальности с объектом, имеющим второй уровень?

Субъект с уровнем конфиденциальности ниже, чем у объекта, не может получить доступ к объекту.