|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА –Российский технологический университет»**  **РТУ МИРЭА**  **Институт кибербезопасности и цифровых технологий**  **Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»** |
|  |

Дисциплина «Технологии обеспечения информационной безопасности»

Отчет

о проделанной практической работе №4

Выполнил студент 1 курса

Группы: ББМО-02-24

Дмитриев Д.В.

Проверил

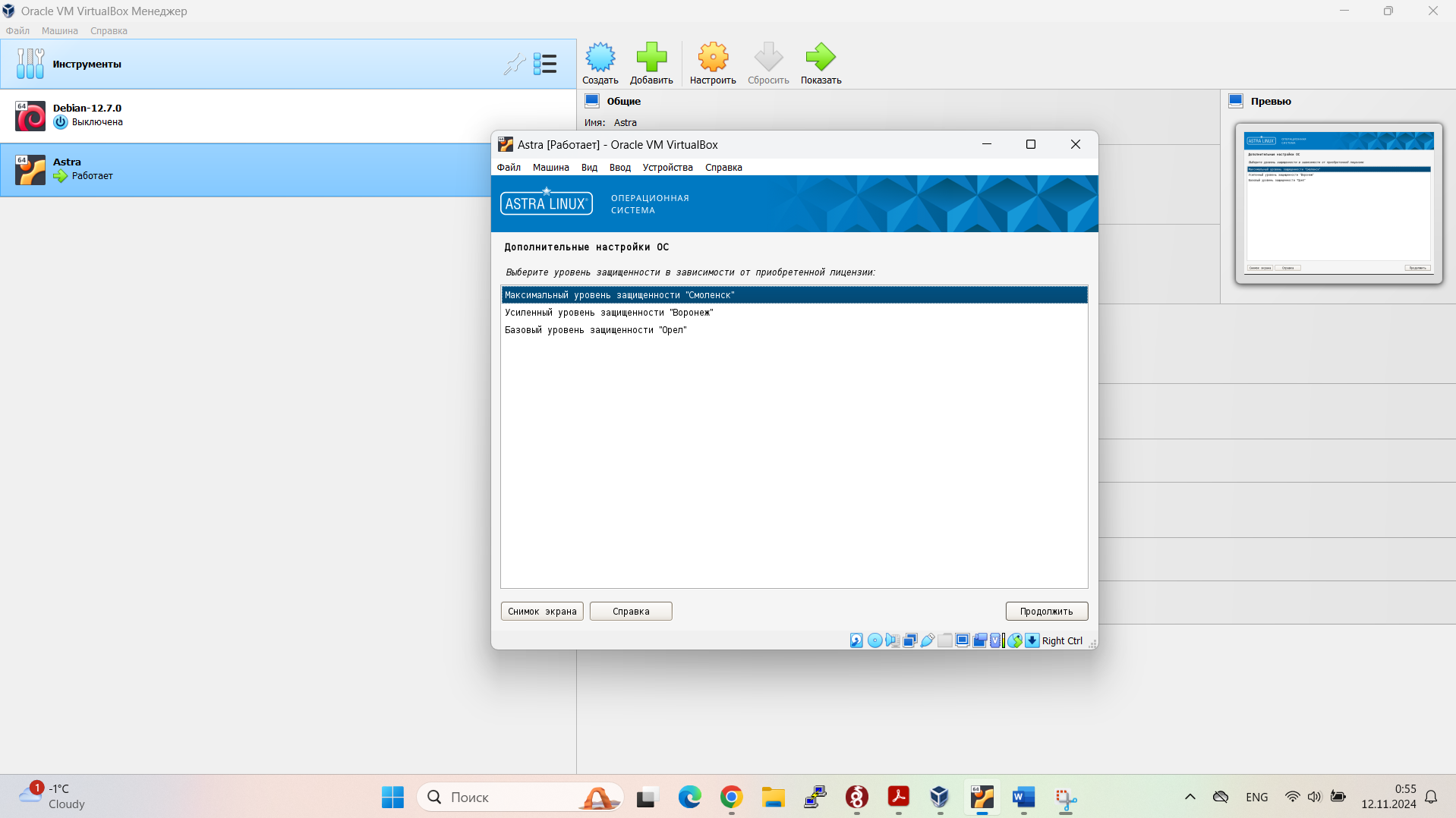
Петров К. Е.

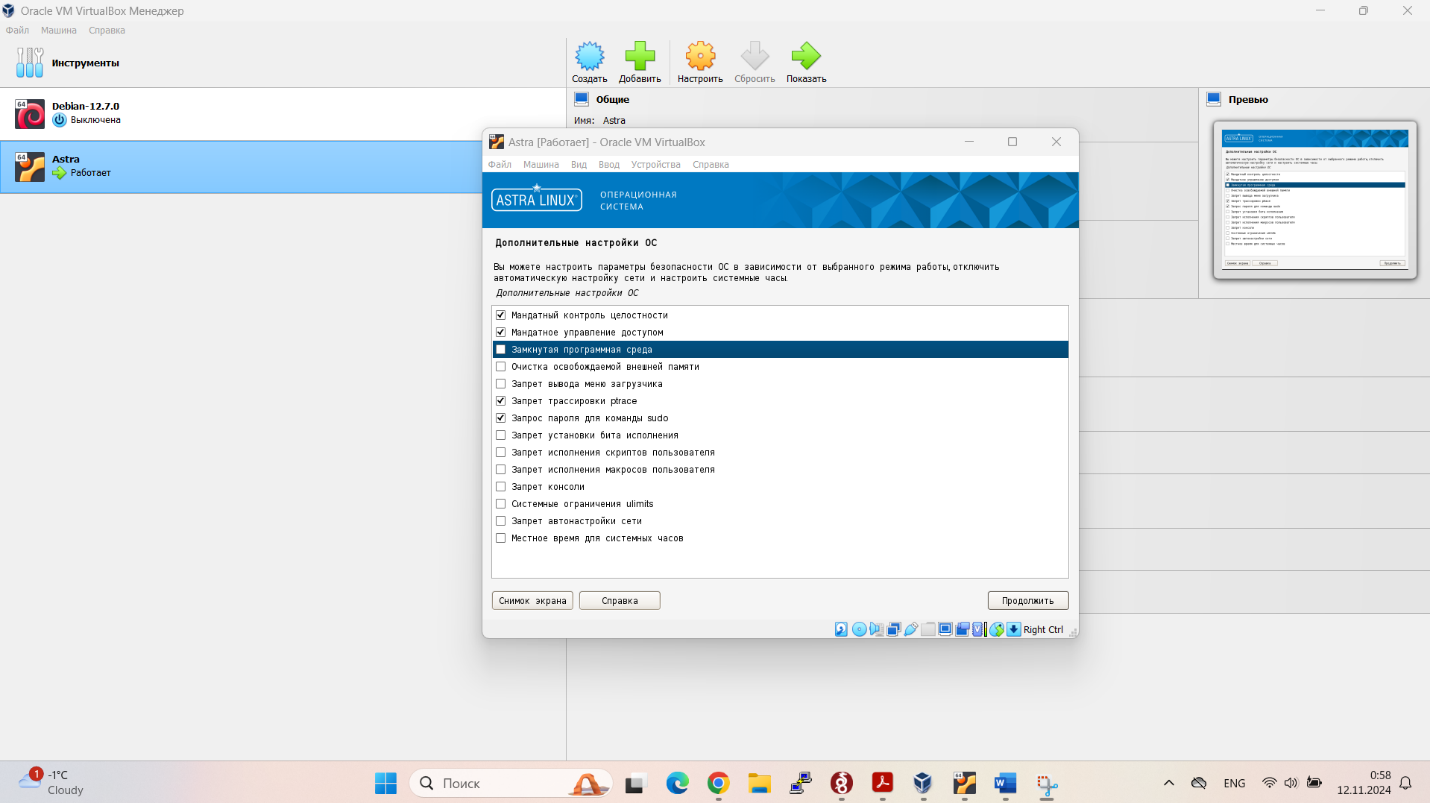
Москва

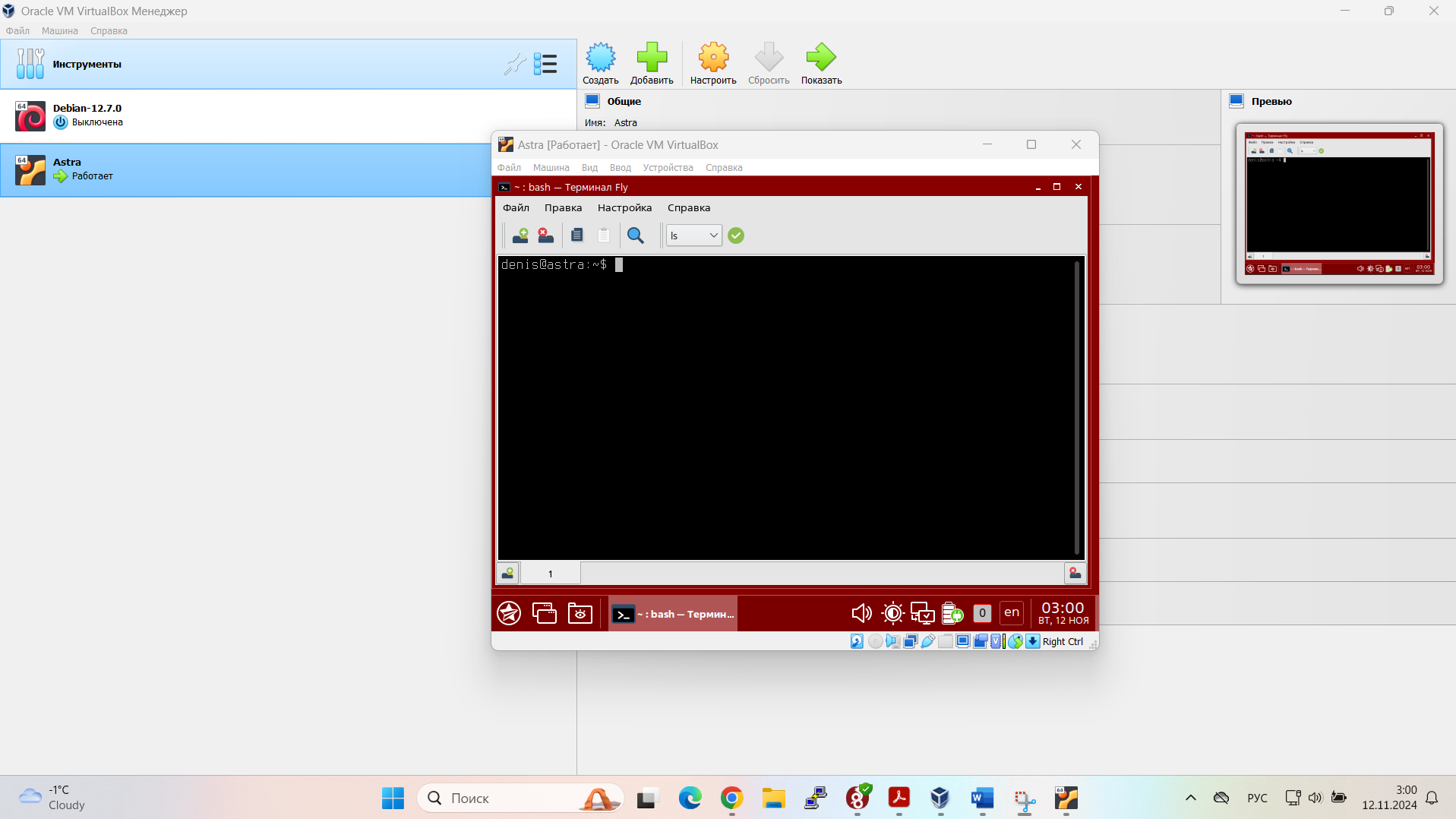
2024

**1. Скачать и развернуть ВМ с ОС Astra Linux для отработки практических заданий**

**Для выполнения этой части задания был скачан (.iso) файл и выбрана версия системы с максимальным уровнем защищенности «Смоленск»**

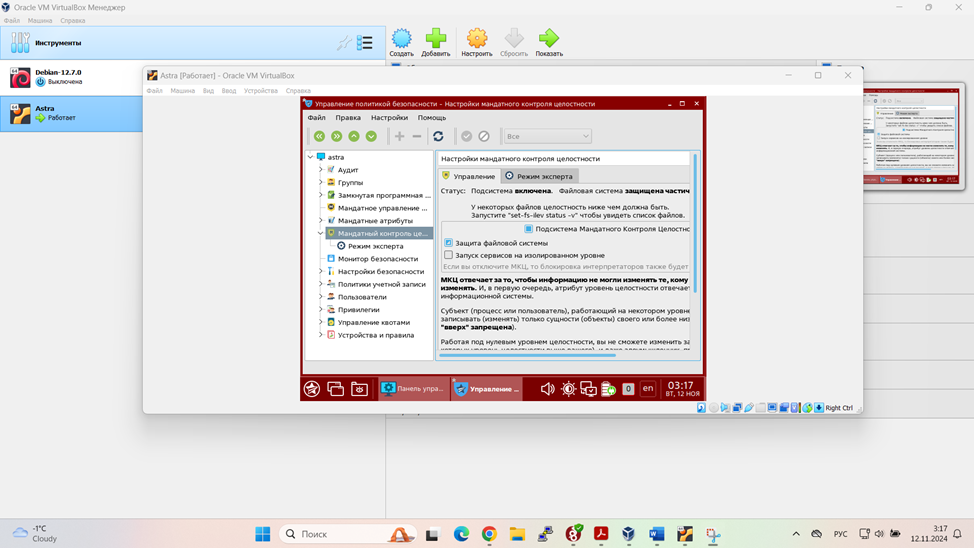






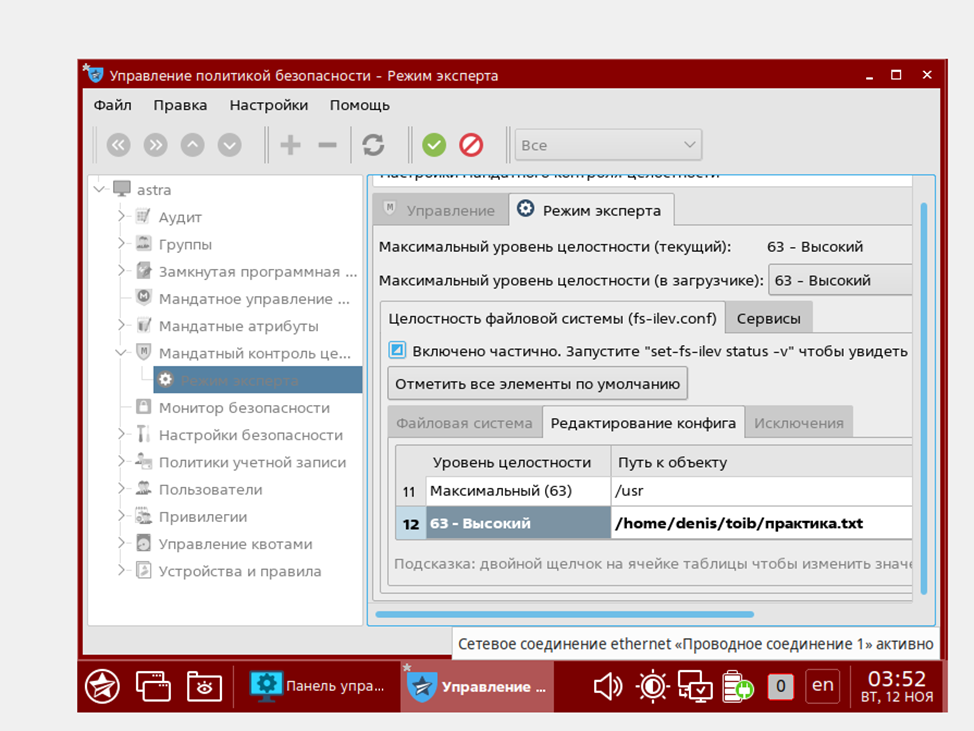
**2. Включить мандатный контроль целостности (МКЦ) в соответствии с руководством по Wiki, КСЗ**

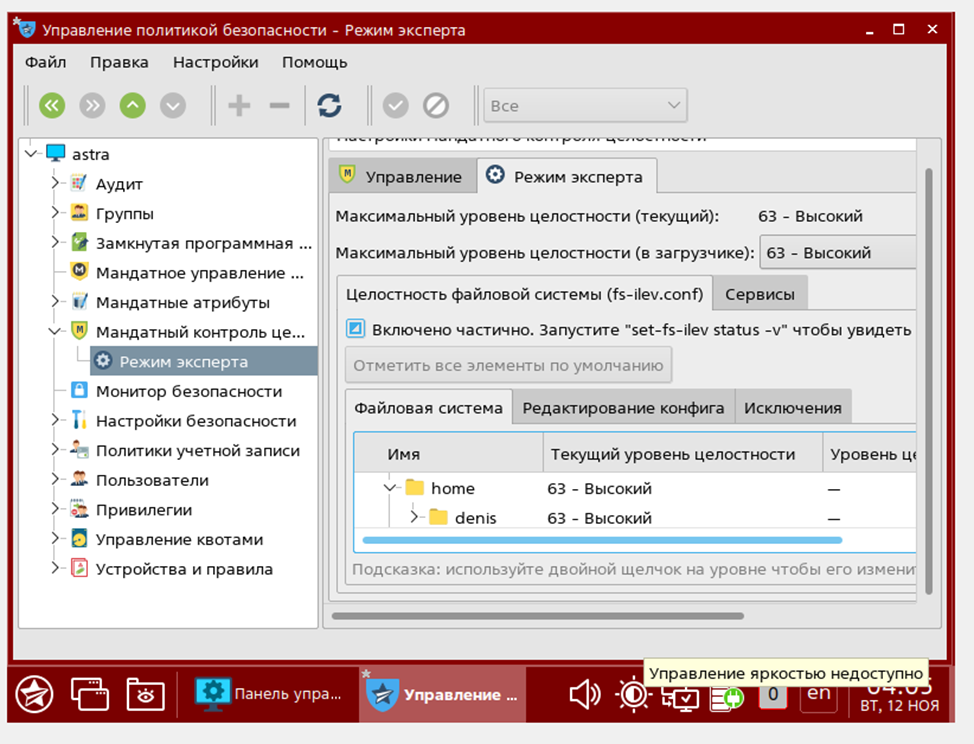
**Для настройки МКЦ нам понадобится зайти в раздел «Политика Безопасности»:**

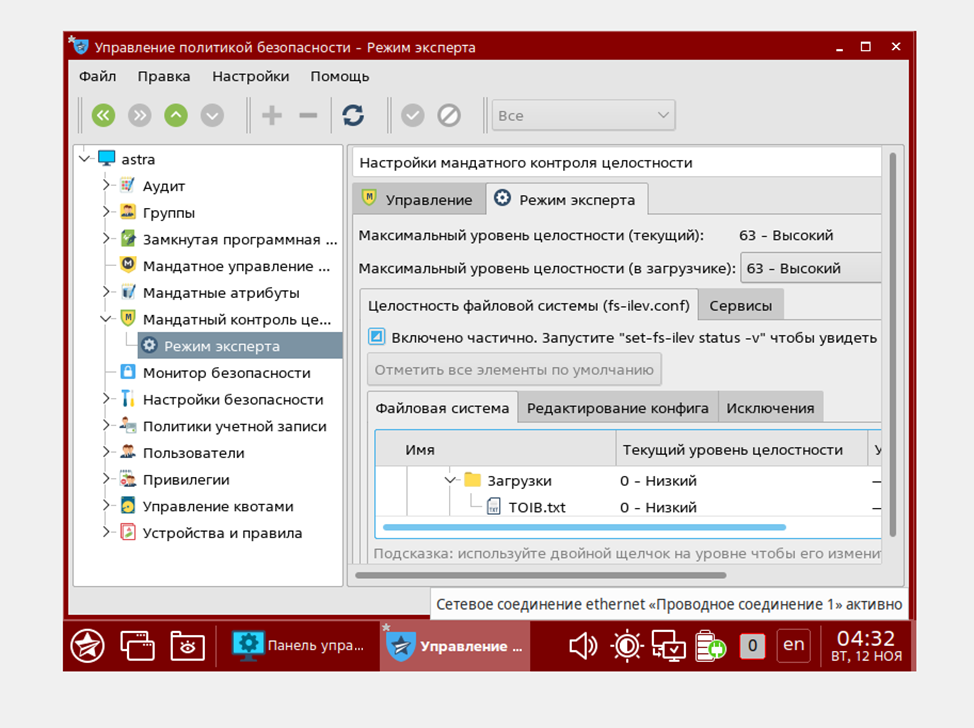
****

**3. Проверить работу механизма МКЦ (запрет на запись "вверх" - NWU), в отчете показать блокировку доступа**

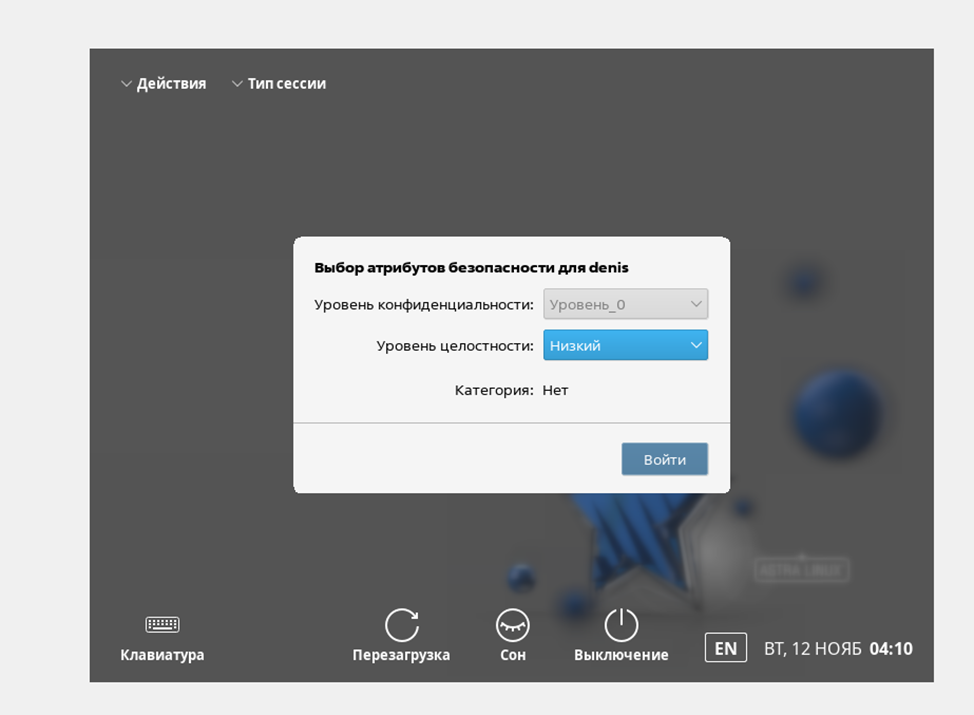
**В разделе «Режим эксперта» можно изменять уровни целостности для директорий и файлов, для проверки правила NWU был изменен уровень целостности директории «toib» (и содержащегося в ней файла) с «0» на «63»:**

****

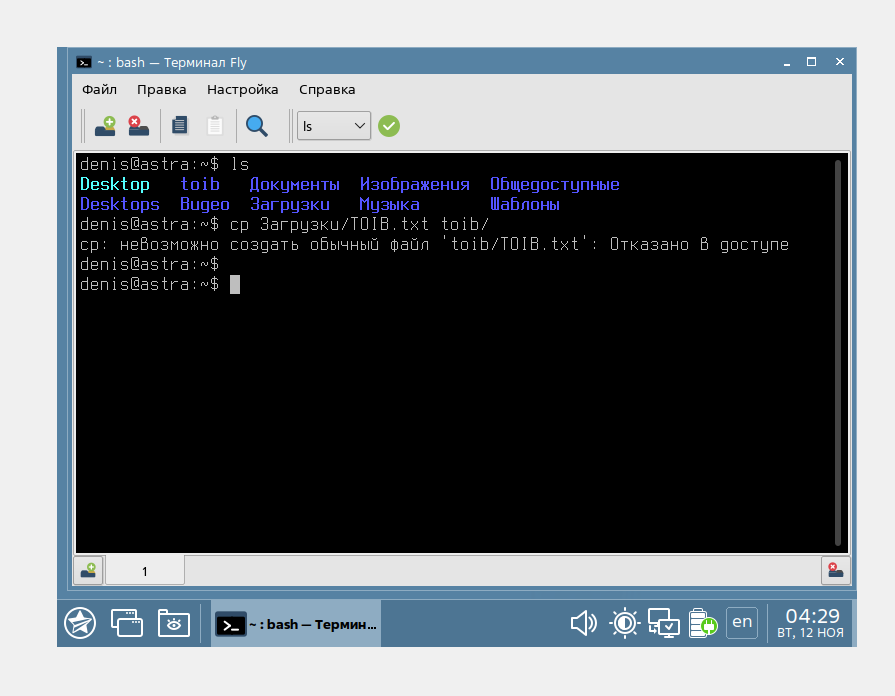
****

****

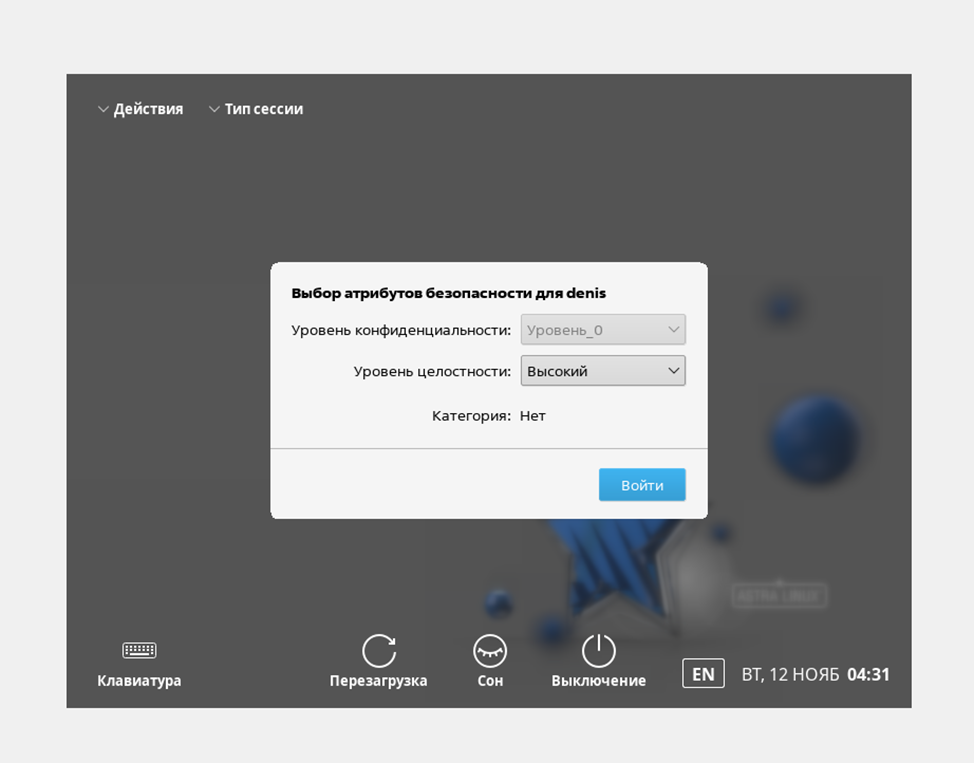
**Для проверки мандатного контроля целостности нужно зайти в учетную запись с атрибутом целостности уровня «Низкий»:**

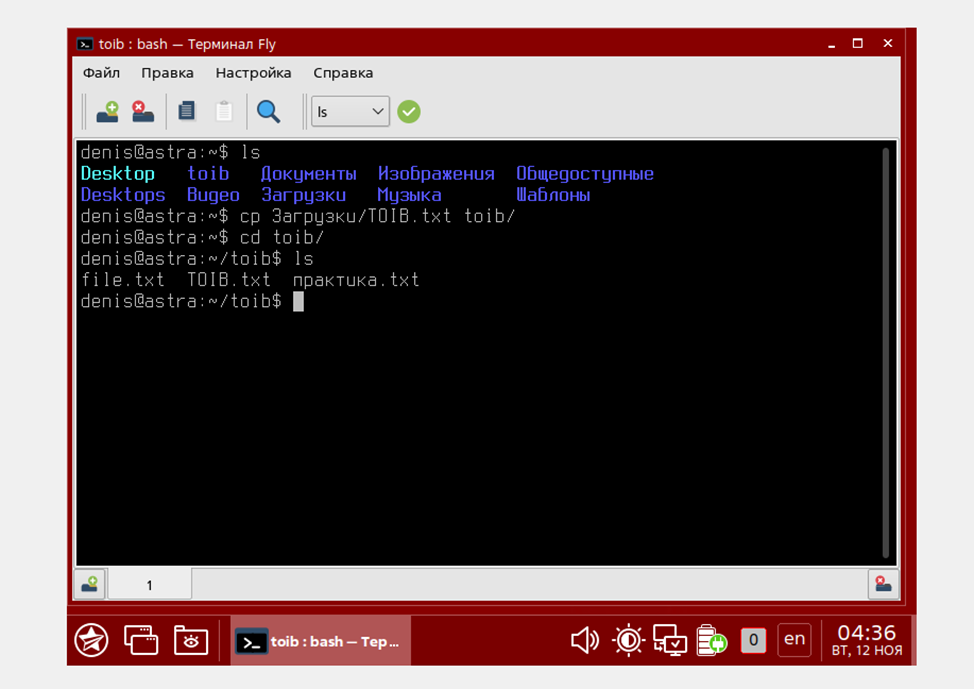
****

**Далее можем увидеть пример взаимодействия между папками, в котором показано, что копирование файла с меньшим атрибутом в папку с большим атрибутом не сработало (была получена ошибка доступа).**



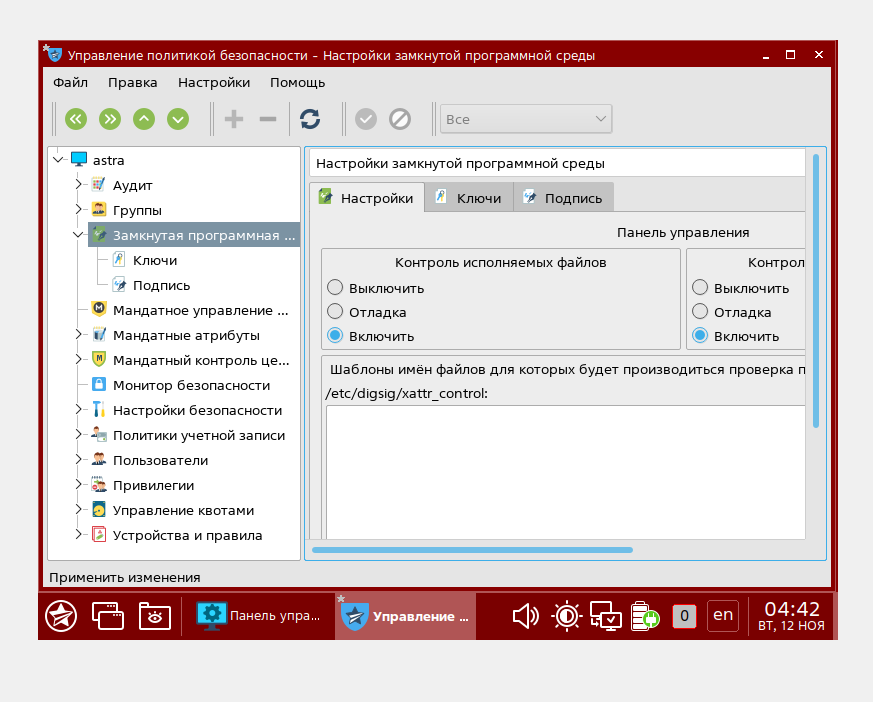
**А если мы зайдем в учетную запись с атрибутом целостности уровня «Высокий», то получать ошибки мы не будем**

****

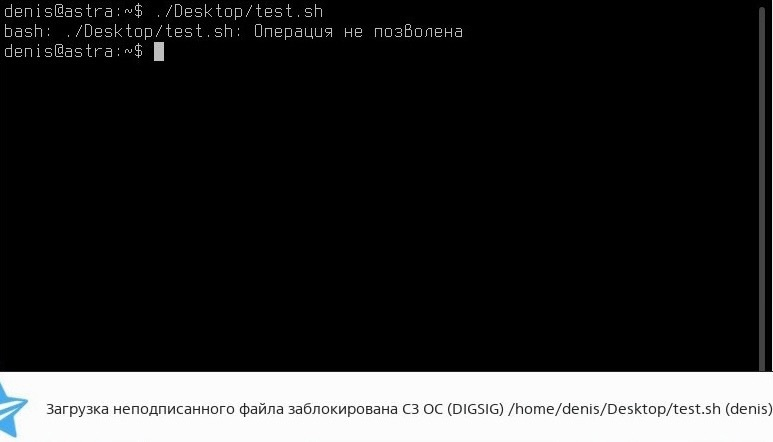
****

**4. Включить режим замкнутой программной среды (ЗПС), проверить работу механизма (попытка запуска неподписанного исполняемого файла), в отчете показать блокировку доступа**

**Для проверки корректной работы режима ЗПС в разделе «Политика безопасности» необходимо включить следующие утилиты:**



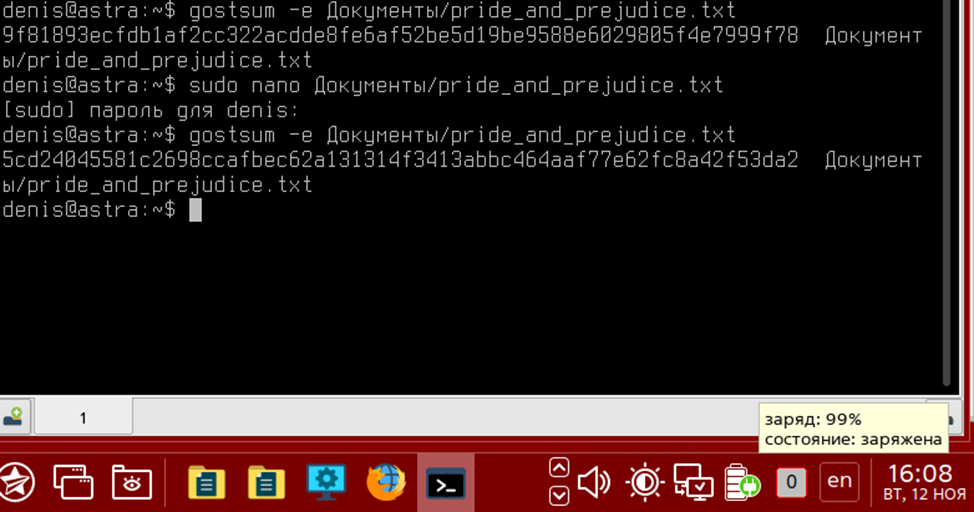
**Результат выполнения в виде ошибки представлен на скриншоте ниже:**

****

**5. Настроить и продемонстрировать работ утилит контроля целостности и регламентного контроля целостности gostsum, afick**

**gostsum — это утилита для вычисления и проверки хеш-сумму файлов с использованием российских криптографических стандартов ГОСТ. Обычно она применяется в системах, где требуется проверка целостности данных.**

**Можно отметить, что gostsum вычисляет хеш-сумму файлов и при изменении самого файла меняется и его хеш-сумма**

****

**afick - это утилита для контроля целостности файлов в Linux**

**Объяснение команд:**

**1. sudo afick -i**

**Команда для запуска утилиты afick (Advanced File Integrity Checker) с параметром -i, который инициирует процесс сканирования файловой системы для создания или обновления базы данных контрольных сумм и другой информации о файлах.**

**2. sudo cp /sbin/blkid /sbin/blkid.bak**

**Команда для создания резервной копию файла /sbin/blkid.**

**3. sudo cp /sbin/sysctl /sbin/sysctl.bak**

**Команда для создания резервной копию файла /sbin/sysctl.**

**4. echo asdf | sudo tee -a /sbin/blkid**

**Эта команда добавляет строку «asdf» в конец файла /sbin/bklid.**

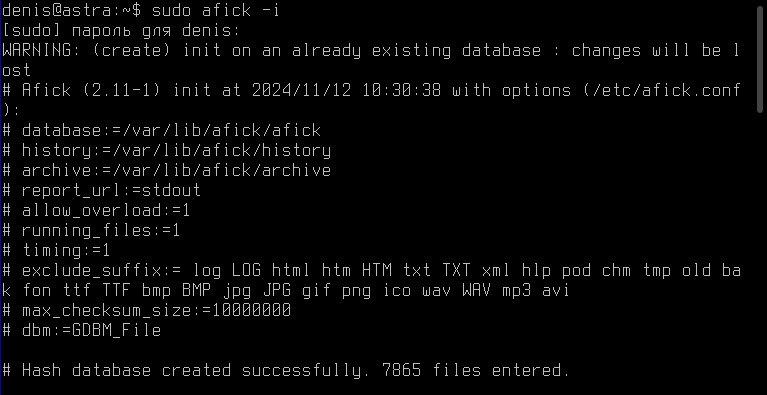
**5. sudo chmod 770 /sbin/sysctl**

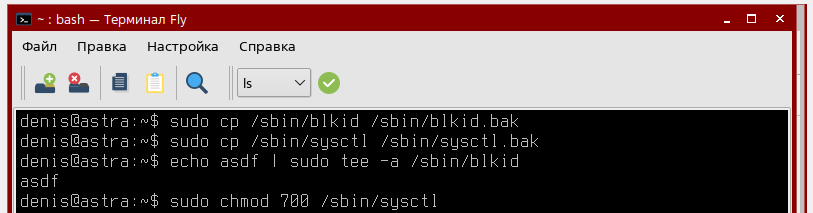
**Эта команда изменяет права доступа к файлу /sbin/sysctl, 770 означает, что владелец файла и группа имеют право читать, записывать и выполнять файл, а остальные пользователи не имеют прав**

**6. sudo afick -k**

**Эта команда запускает проверку целостности файлов, ключ k используется**

**для проверки целостности файлов и сверки с ранее созданной базой данных контрольных сумм, чтобы выявить изменения в файлах с момента последнего сканирования.**







**На последнем скриншоте можно заметить, что утилита нашла файлы, которые были изменены после последнего сканирования файловой системы**