



**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

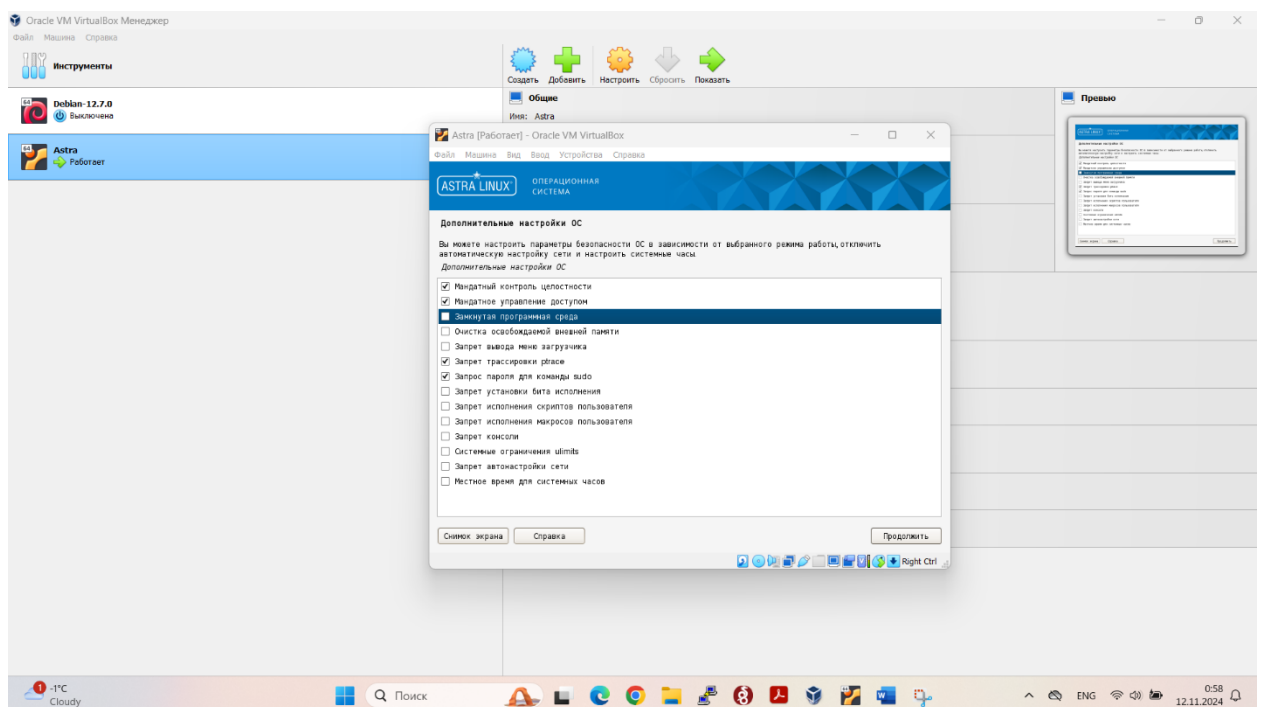
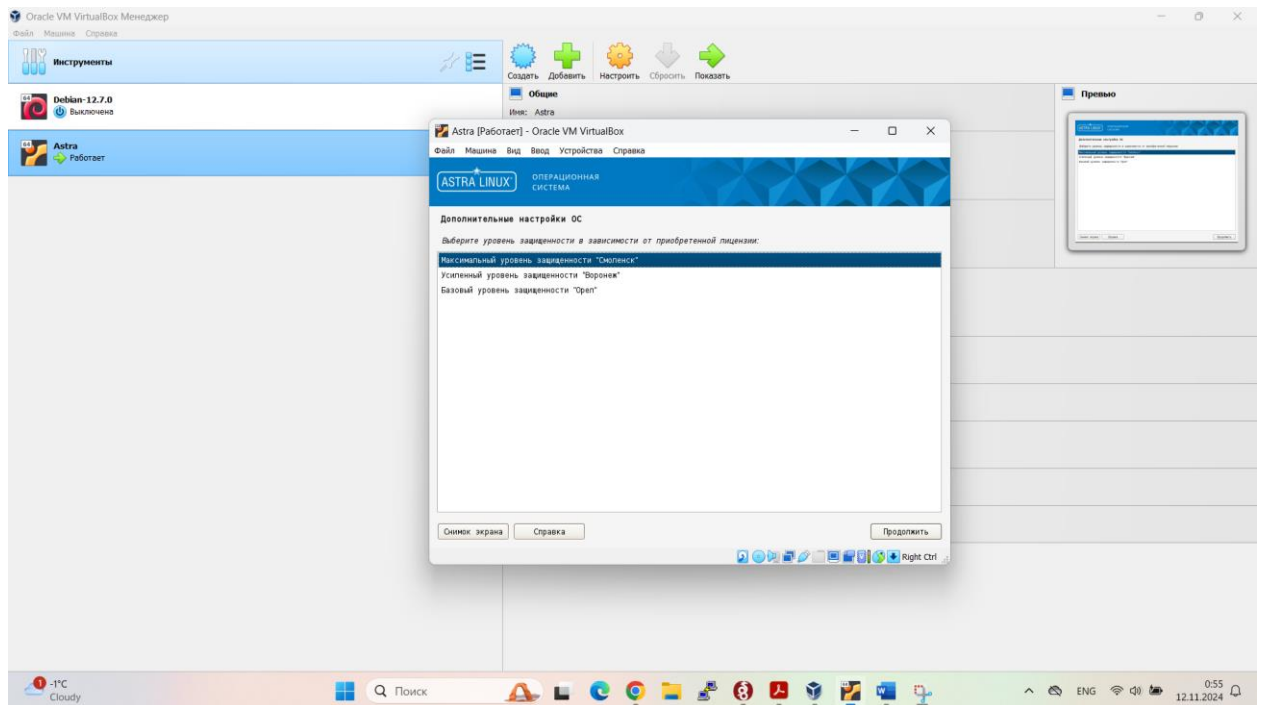
Петров К. Е.

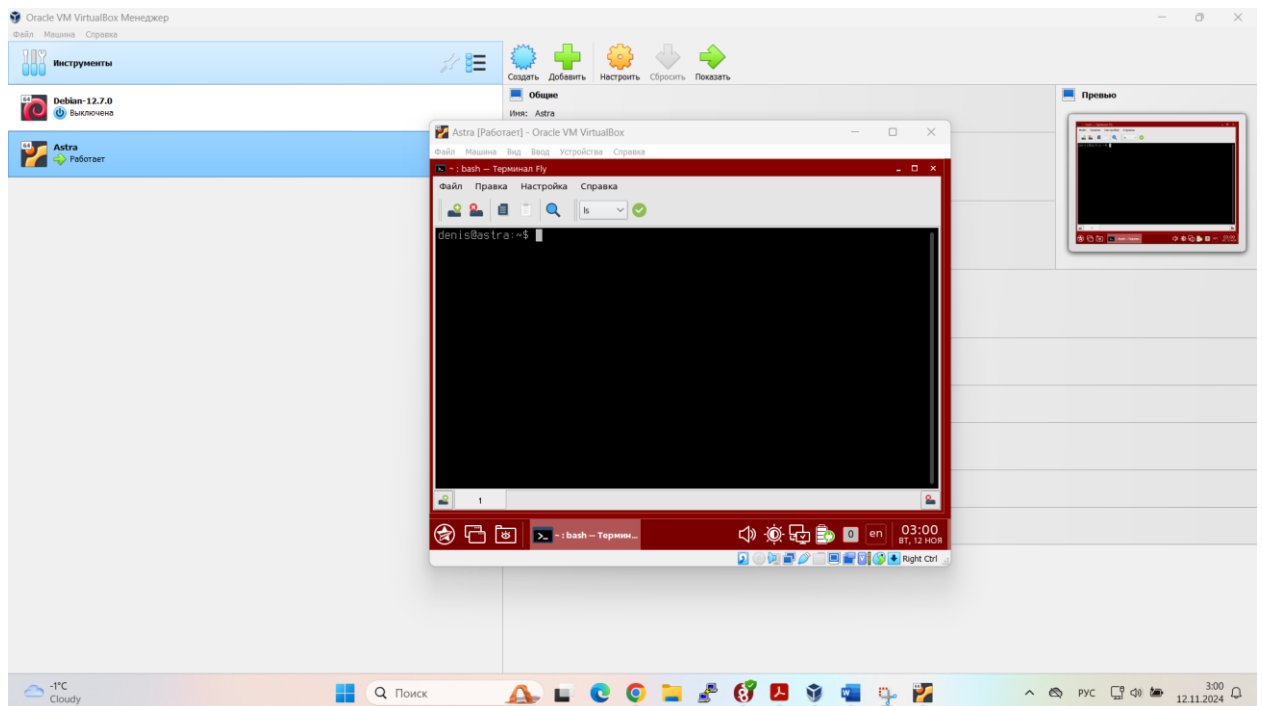
Москва

2024

# 1. Скачать и развернуть VM с ОС Astra Linux для отработки практических заданий

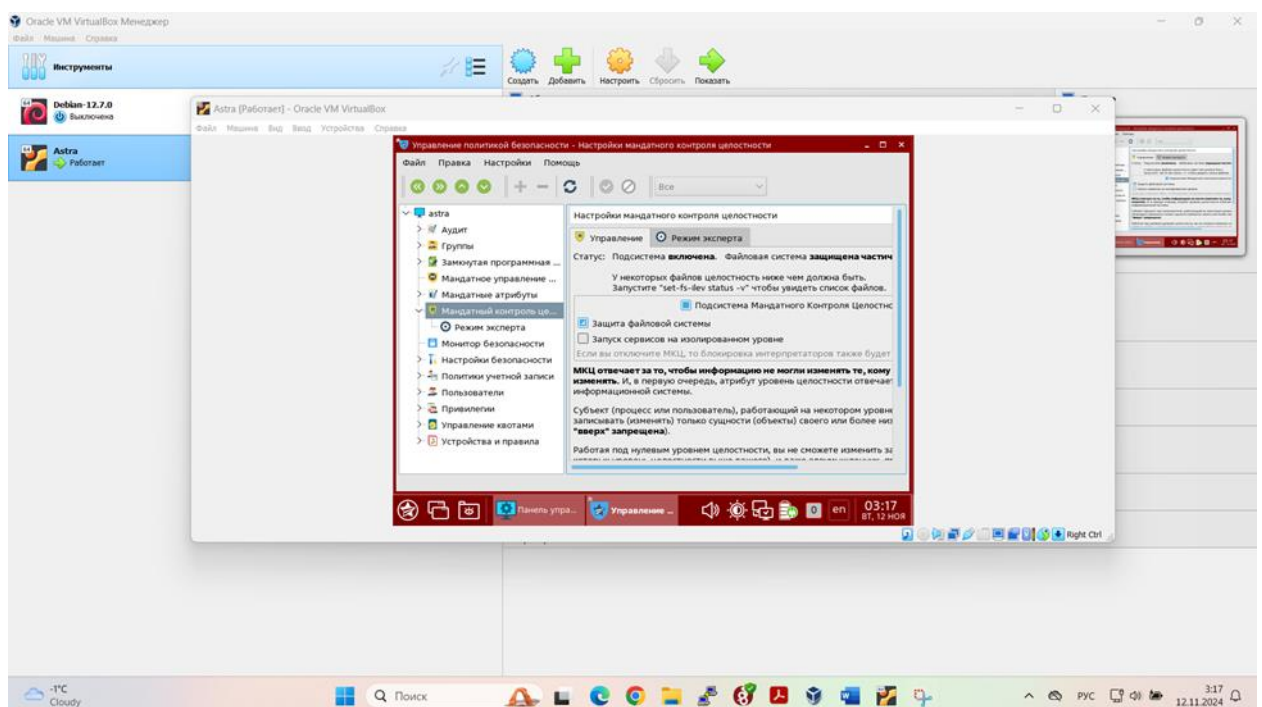
Для выполнения этой части задания был скачан (.iso) файл и выбрана версия системы с максимальным уровнем защищенности «Смоленск»





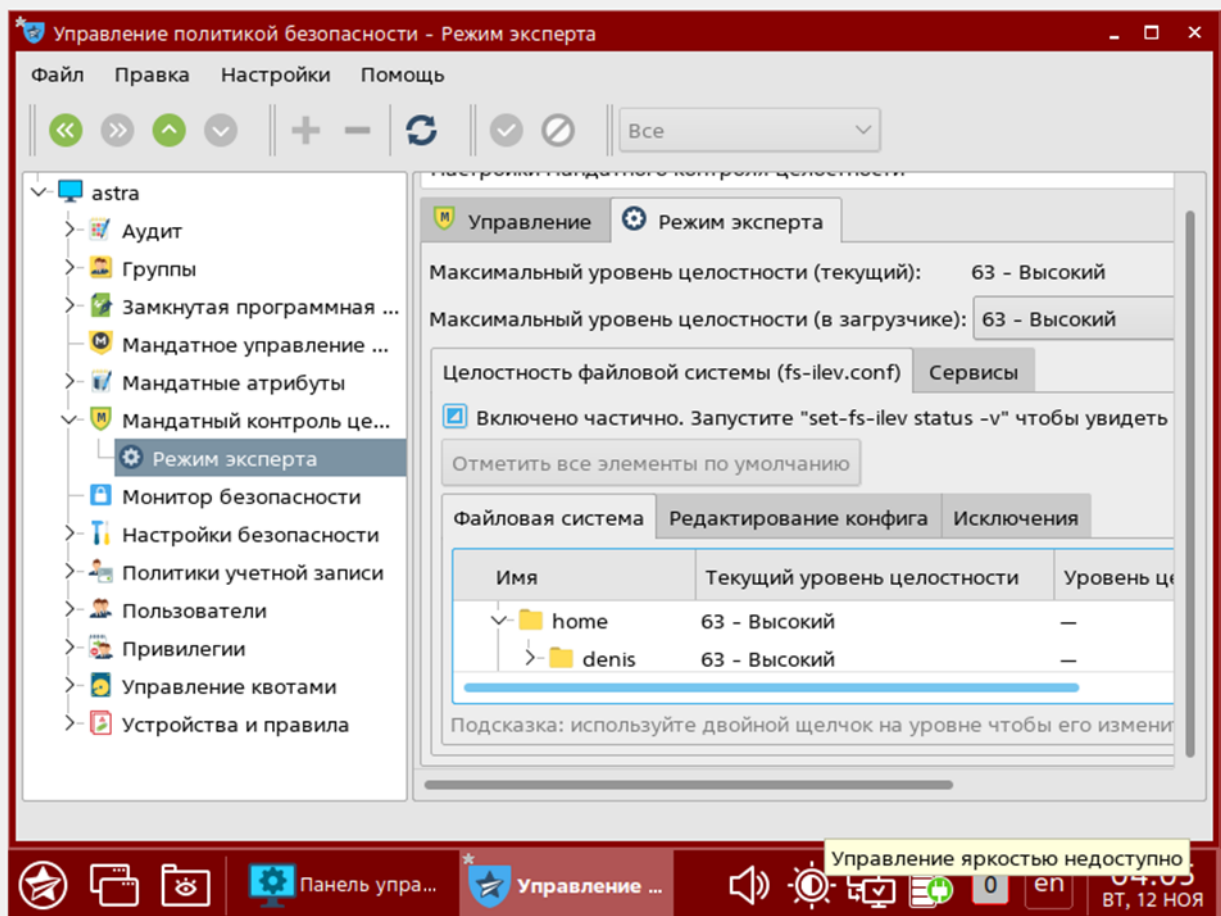
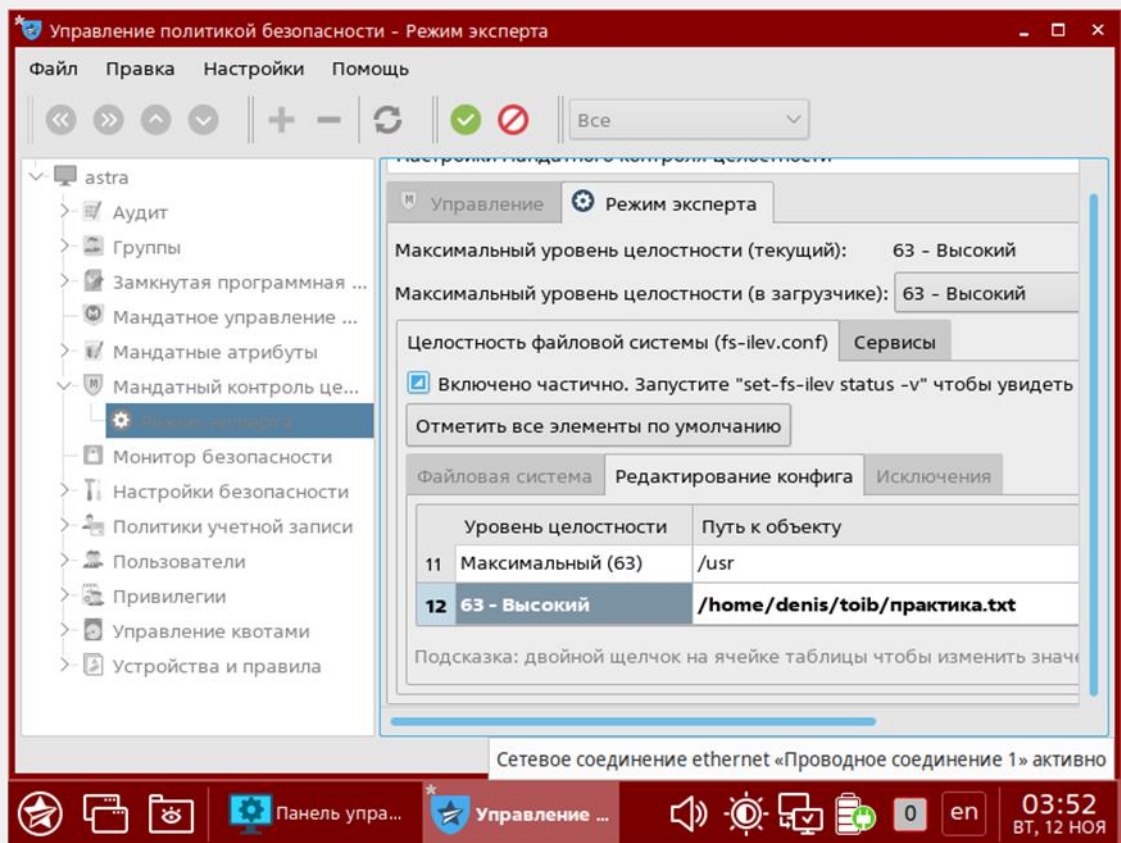
## 2. Включить мандатный контроль целостности (МКЦ) в соответствии с руководством по Wiki, КСЗ

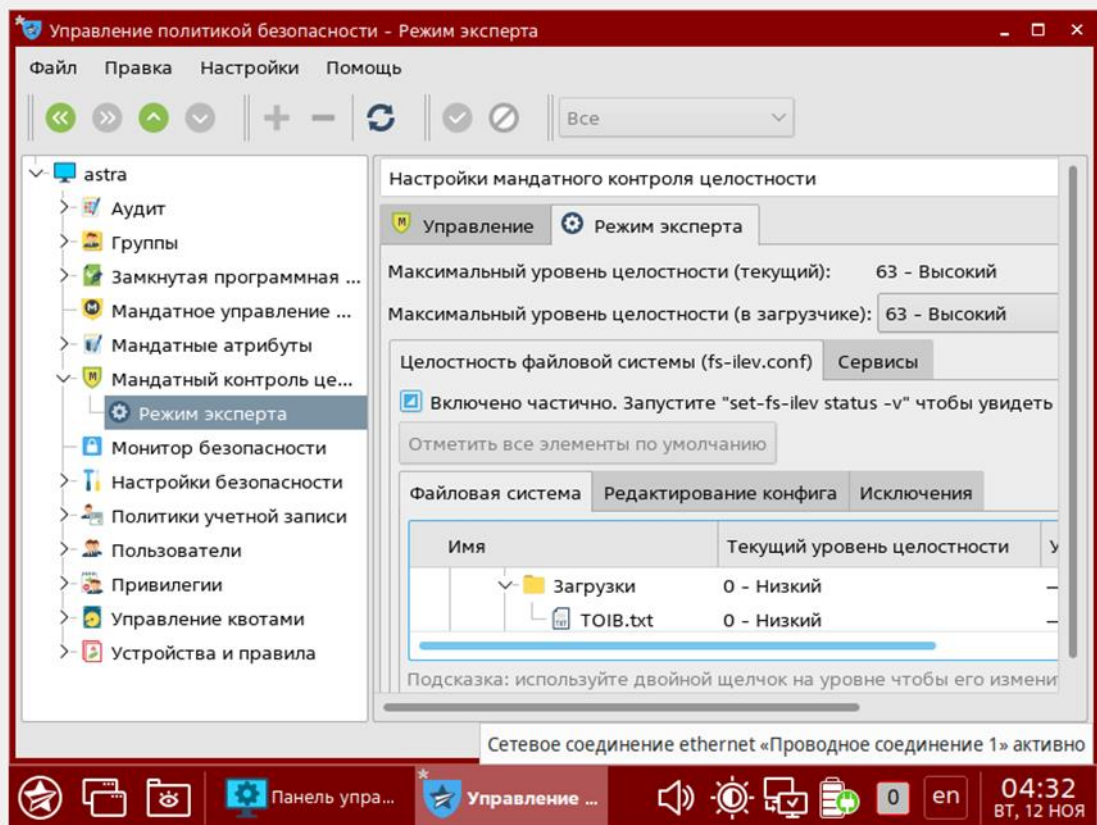
Для настройки МКЦ нам понадобится зайти в раздел «Политика Безопасности»:



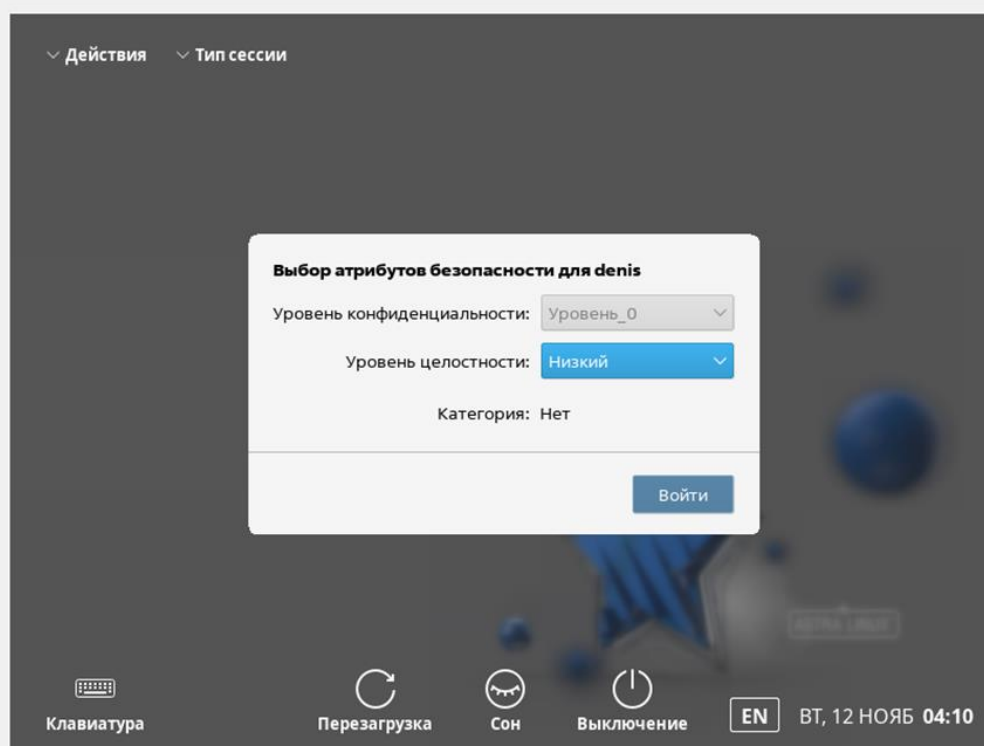
## 3. Проверить работу механизма МКЦ (запрет на запись "вверх" - NWU), в отчете показать блокировку доступа

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»:

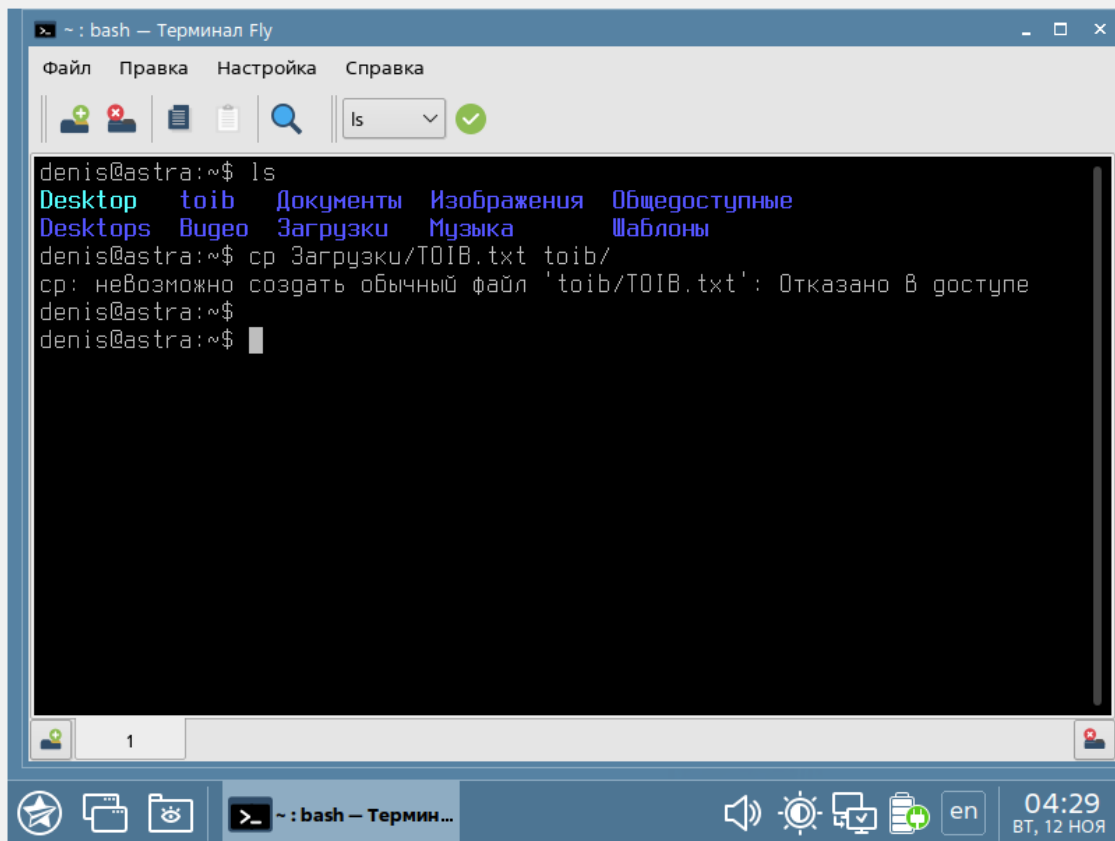




Для проверки мандатного контроля целостности нужно зайти в учетную запись с атрибутом целостности уровня «Низкий»:

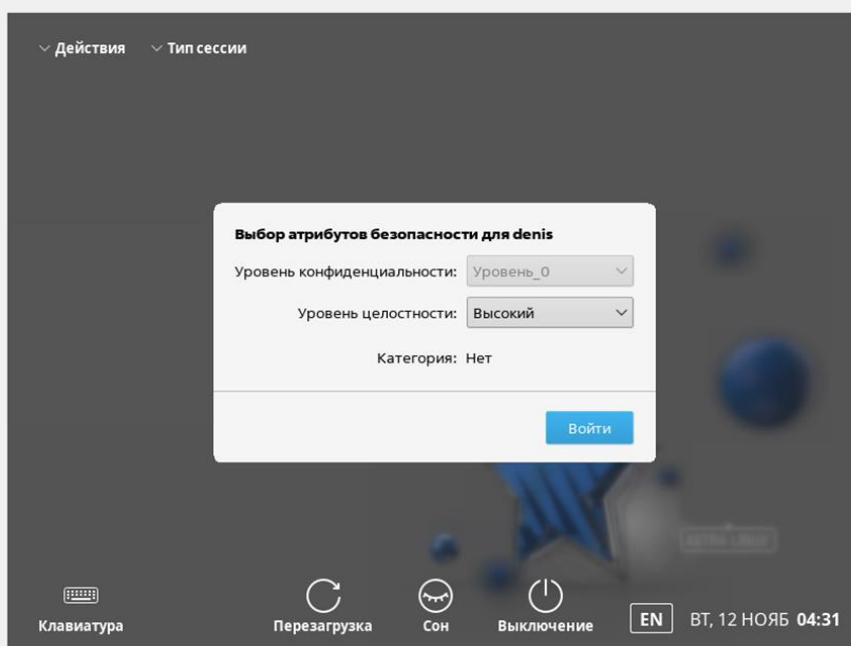


Далее можем увидеть пример взаимодействия между папками, в котором показано, что копирование файла с меньшим атрибутом в папку с большим атрибутом не сработало (была получена ошибка доступа).



```
denis@astra:~$ ls
Desktop  toib  Документы  Изображения  Общедоступные
Desktops Bugeo  Загрузки  Музыка        Шаблоны
denis@astra:~$ cp Загрузки/TOIB.txt toib/
cp: невозможно создать обычный файл 'toib/TOIB.txt': Отказано в доступе
denis@astra:~$
denis@astra:~$
```

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



Действия Тип сессии

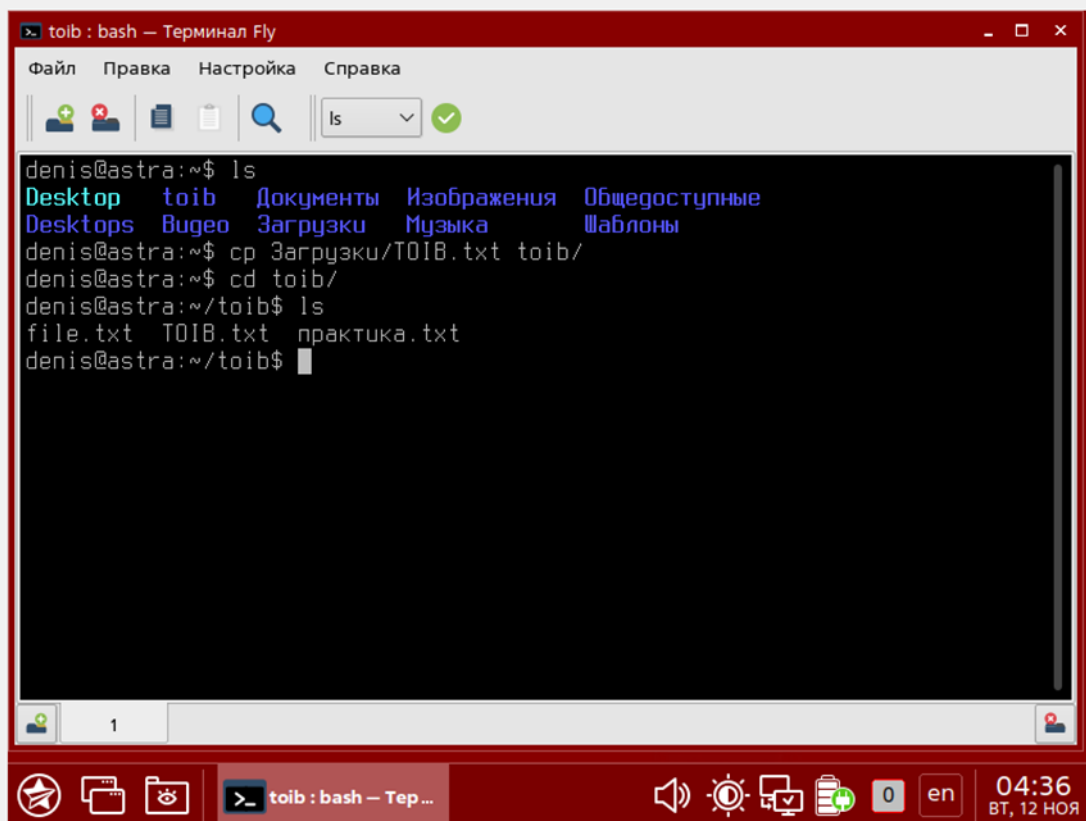
**Выбор атрибутов безопасности для denis**

Уровень конфиденциальности:

Уровень целостности:

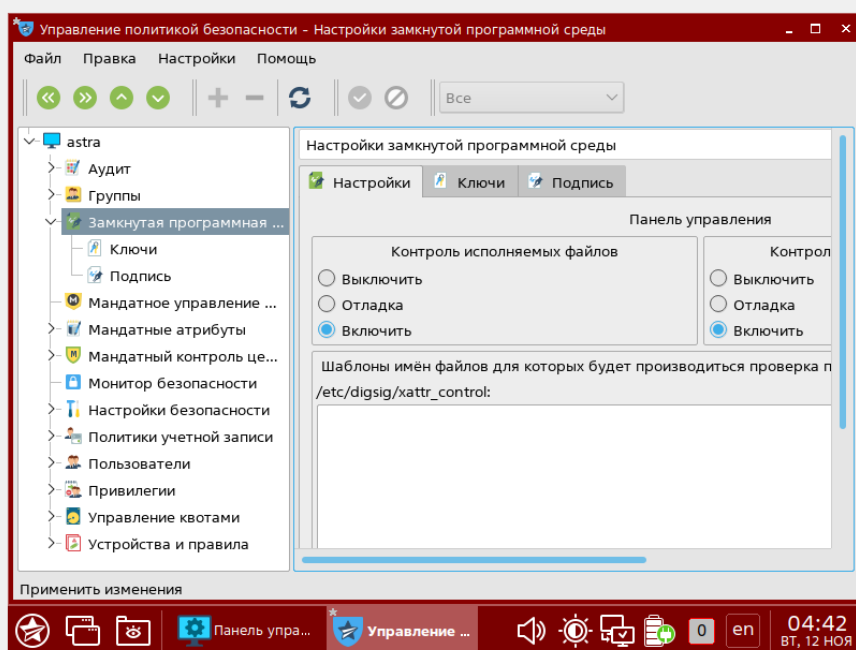
Категория: Нет

Клавиатура Перезагрузка Сон Выключение EN ВТ, 12 НОЯБ 04:31



**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:

```
denis@astra:~$ ./Desktop/test.sh
bash: ./Desktop/test.sh: Операция не позволена
denis@astra:~$
```

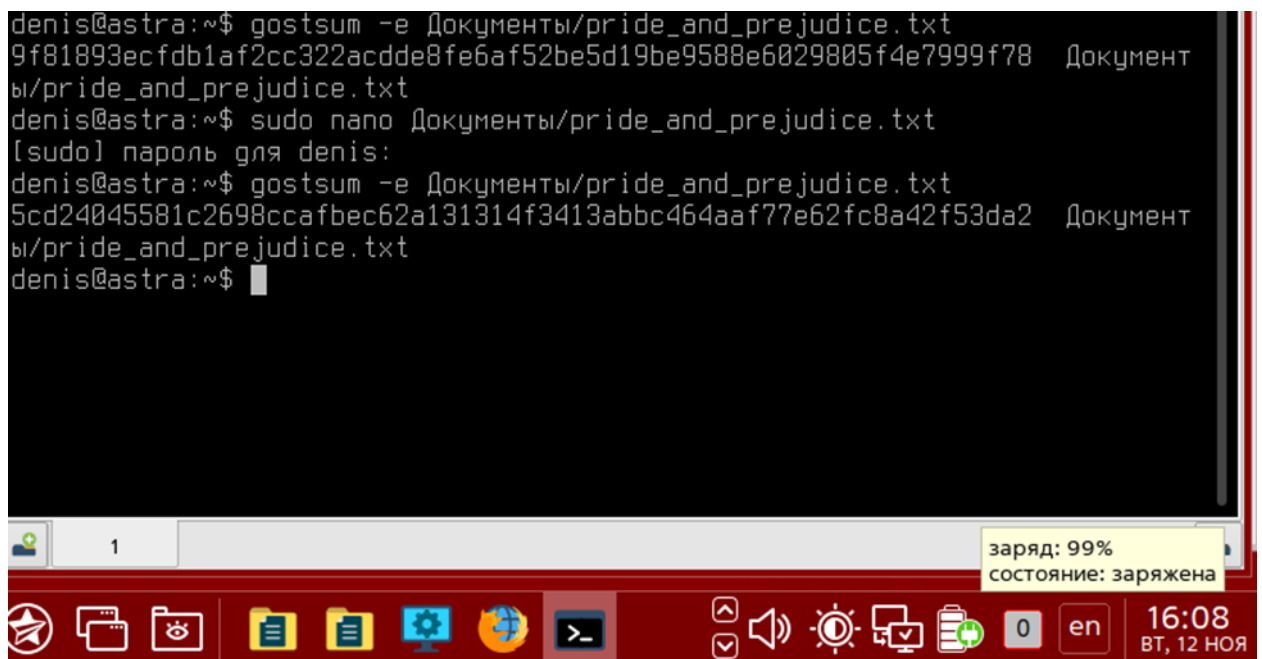


## 5. Настроить и продемонстрировать работ утилит контроля целостности и регламентного контроля целостности gostsum, afick

**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

```
denis@astra:~$ gostsum -e Документы/pride_and_prejudice.txt
9f81893ecfdb1af2cc322acdde8fe6af52be5d19be9588e6029805f4e7999f78  Документ
ы/pride_and_prejudice.txt
denis@astra:~$ sudo nano Документы/pride_and_prejudice.txt
[sudo] пароль для denis:
denis@astra:~$ gostsum -e Документы/pride_and_prejudice.txt
5cd24045581c2698ccafbec62a131314f3413abbc464aaf77e62fc8a42f53da2  Документ
ы/pride_and_prejudice.txt
denis@astra:~$
```





**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 иницирует 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 копии файла **/sbin/blkid**.

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

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

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

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

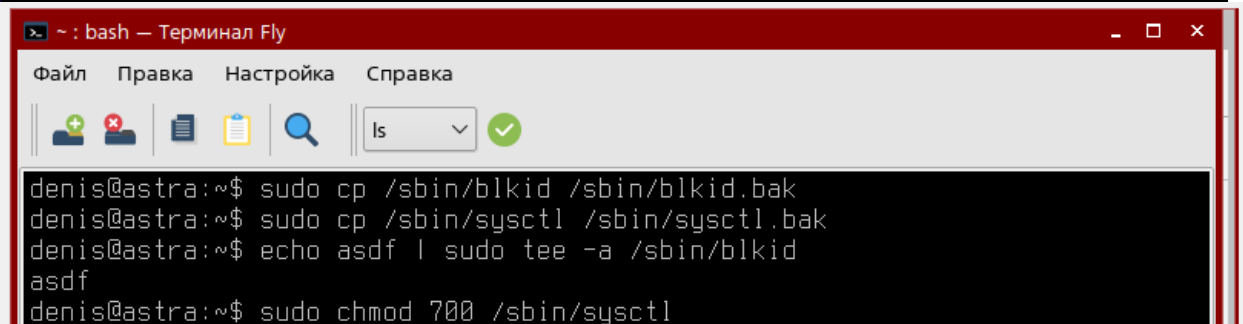
5. **sudo chmod 770 /sbin/sysctl**

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.

```
denis@astra:~$ sudo afick -i
[sudo] пароль для denis:
WARNING: (create) init on an already existing database : changes will be lost
# Afick (2.11-1) init at 2024/11/12 10:30:38 with options (/etc/afick.conf):
# database:=/var/lib/afick/afick
# history:=/var/lib/afick/history
# archive:=/var/lib/afick/archive
# report_url:=stdout
# allow_overload:=1
# running_files:=1
# timing:=1
# exclude_suffix:= log LOG html htm HTM txt TXT xml hlp pod chm tmp old bak
# fon ttf TTF bmp BMP jpg JPG gif png ico wav WAV mp3 avi
# max_checksum_size:=100000000
# dbm:=GDBM_File
# Hash database created successfully. 7865 files entered.
```



```
# detailed changes
changed directory : /usr/sbin
      mtime           : Tue Nov 12 01:00:45 2024      Tue Nov 12
      10:31:03 2024
changed file : /usr/sbin/blkid
      md5             : vGIhWTf57o++mh2BDTPz3g      EDKwAXMpeR
      /Qg6m1UJf7HA
      filesize        : 113264      113269
      mtime           : Thu Sep  3 10:57:46 2020      Tue Nov 12
      10:31:43 2024
changed file : /usr/sbin/sysctl
      filemode        : 100755      100700
```

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