



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

Худяков Д.А.

Проверил

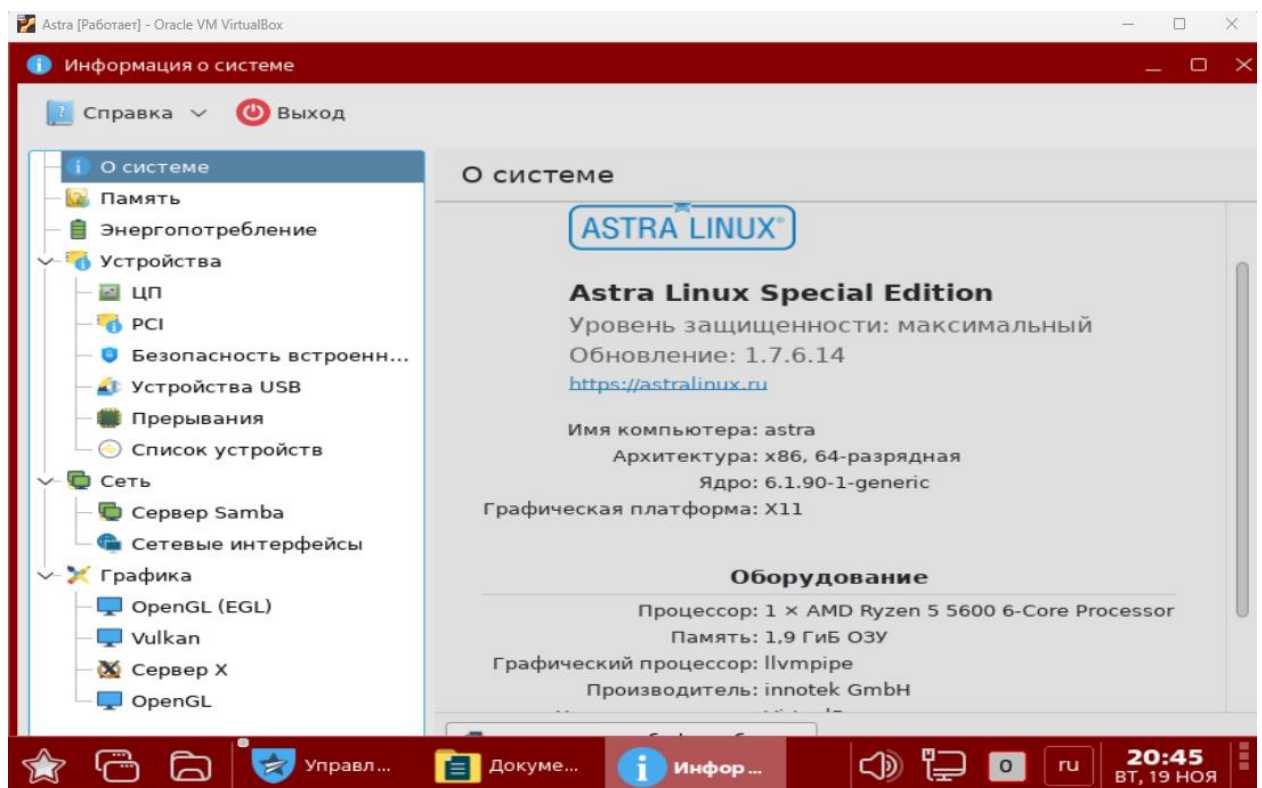
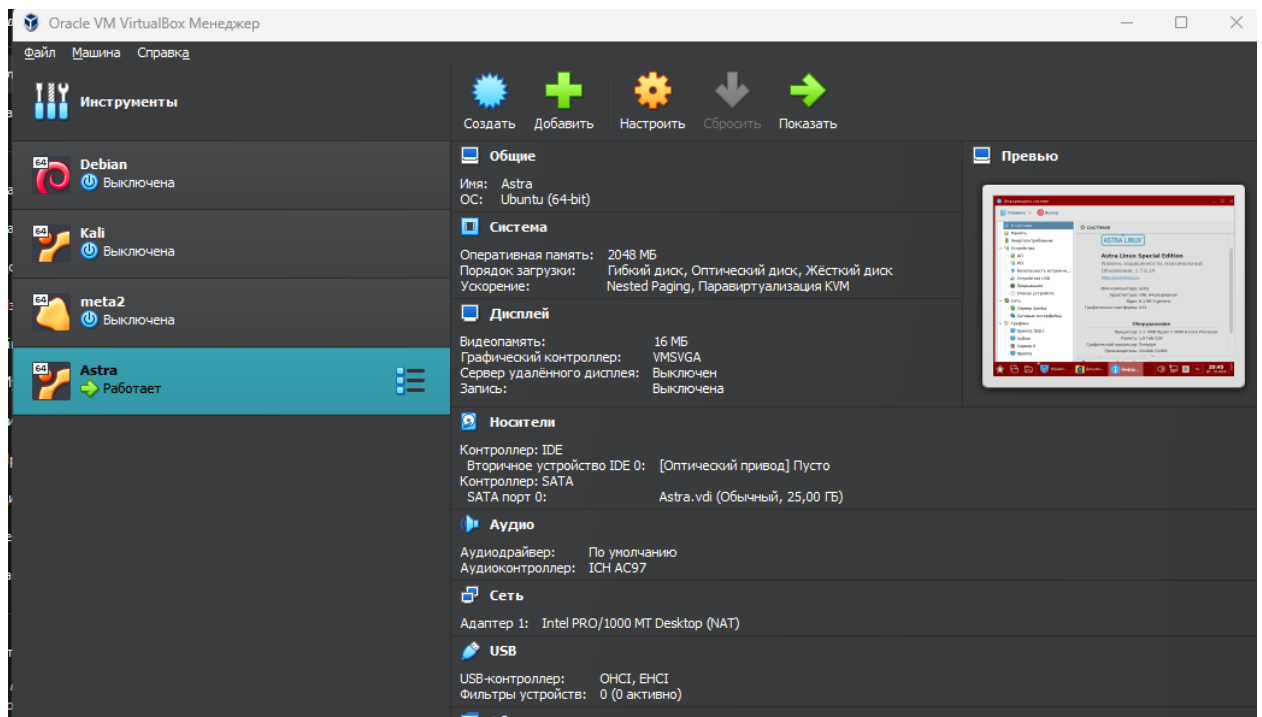
Петров К. Е.

Москва

2024

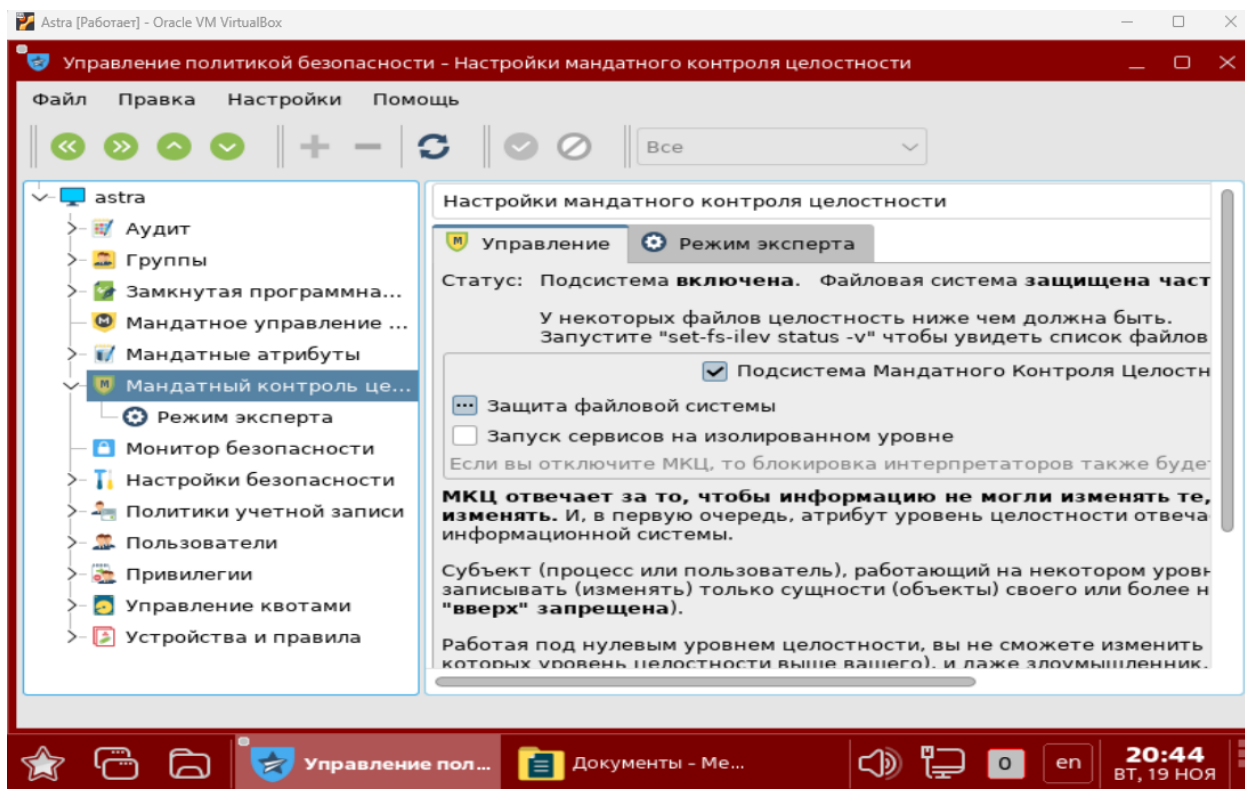
1. Скачать и развернуть VM с ОС Astra Linux для отработки практических заданий

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



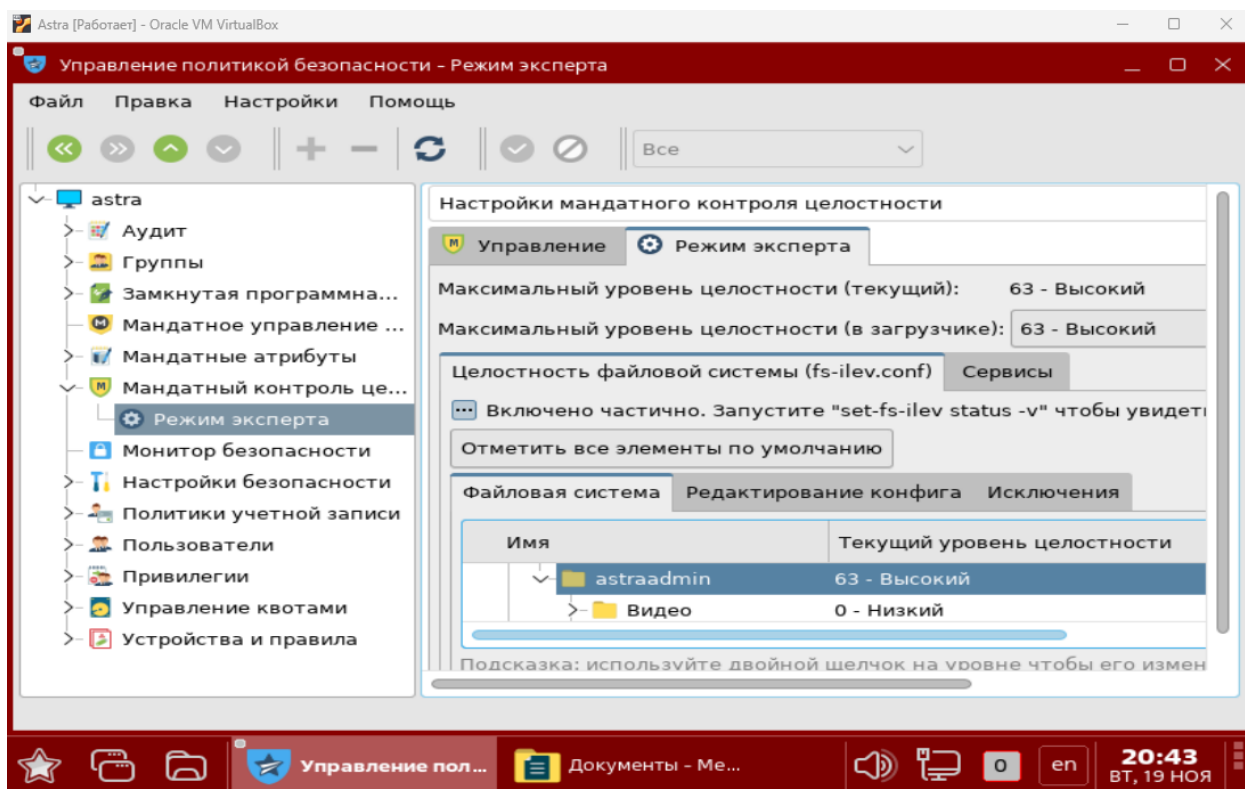
2. Включить мандатный контроль целостности (МКЦ) в соответствии с руководством по Wiki, КСЗ

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

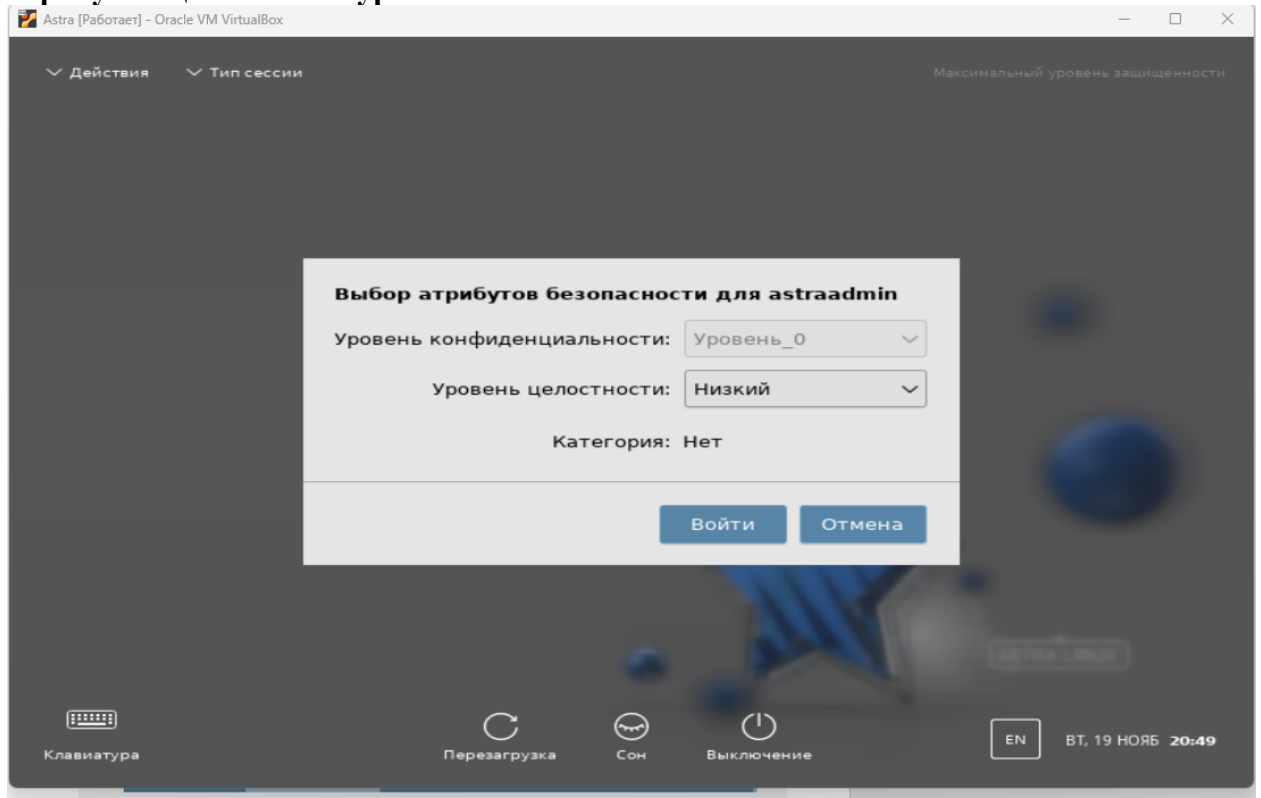


3. Проверить работу механизма МКЦ (запрет на запись "вверх" - NWU), в отчете показать блокировку доступа

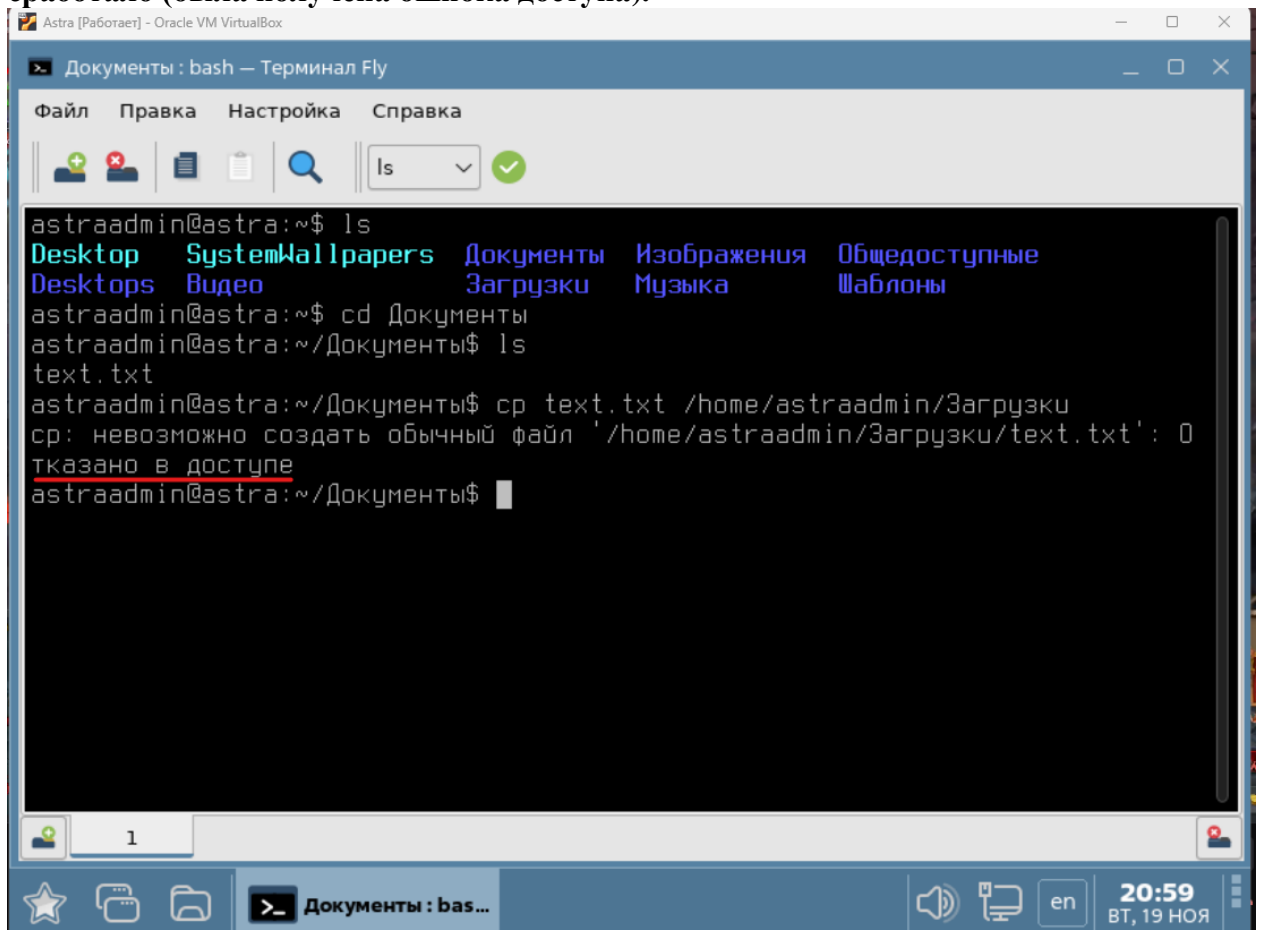
В разделе «Режим эксперта» можно изменять уровни целостности для директорий и файлов, для проверки правила NWU был изменен уровень целостности директории «toib» (и содержащегося в ней файла) с «0» на «63»:



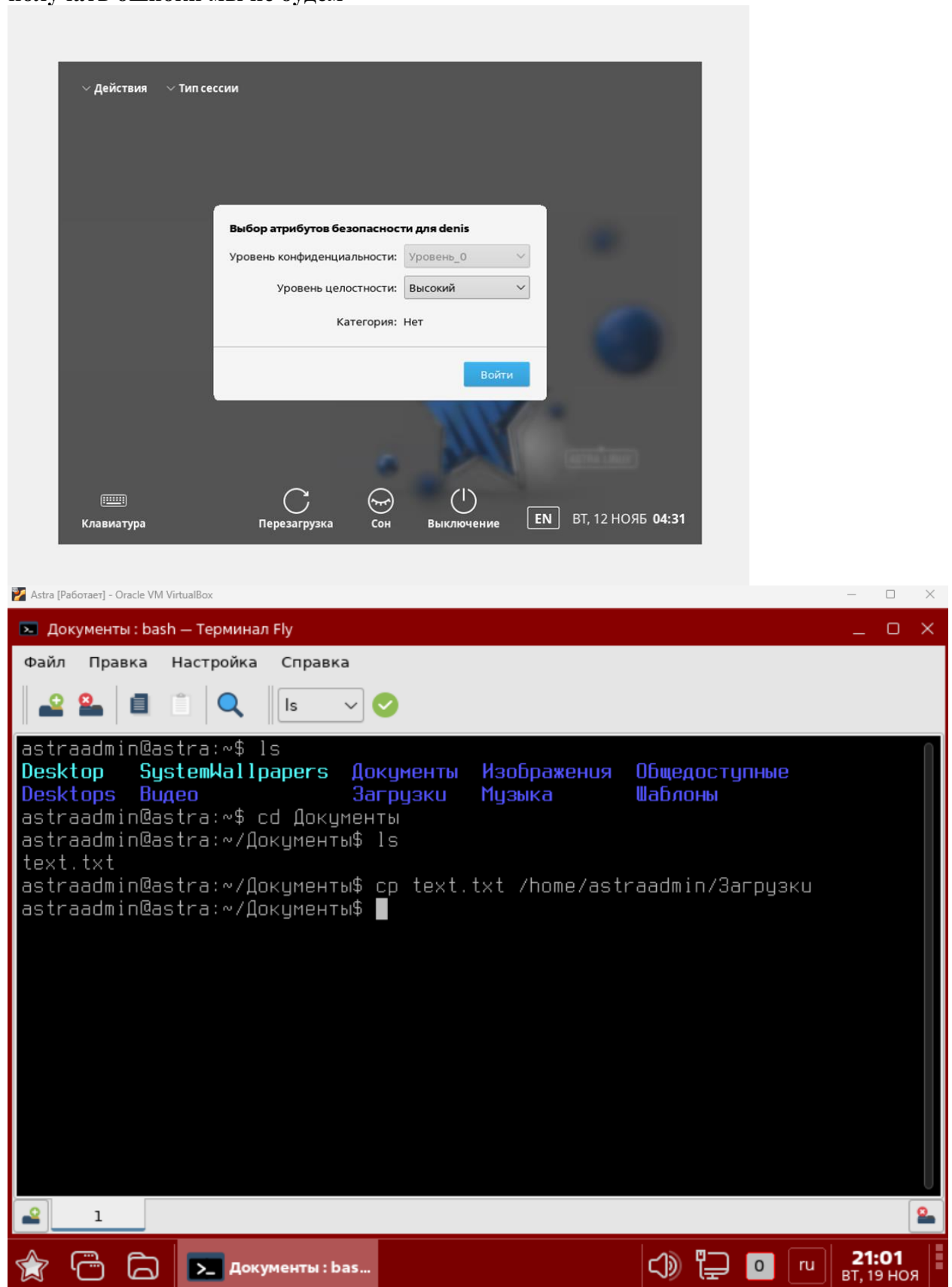
Для проверки мандатного контроля целостности нужно зайти в учетную запись с атрибутом целостности уровня «Низкий»:



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).

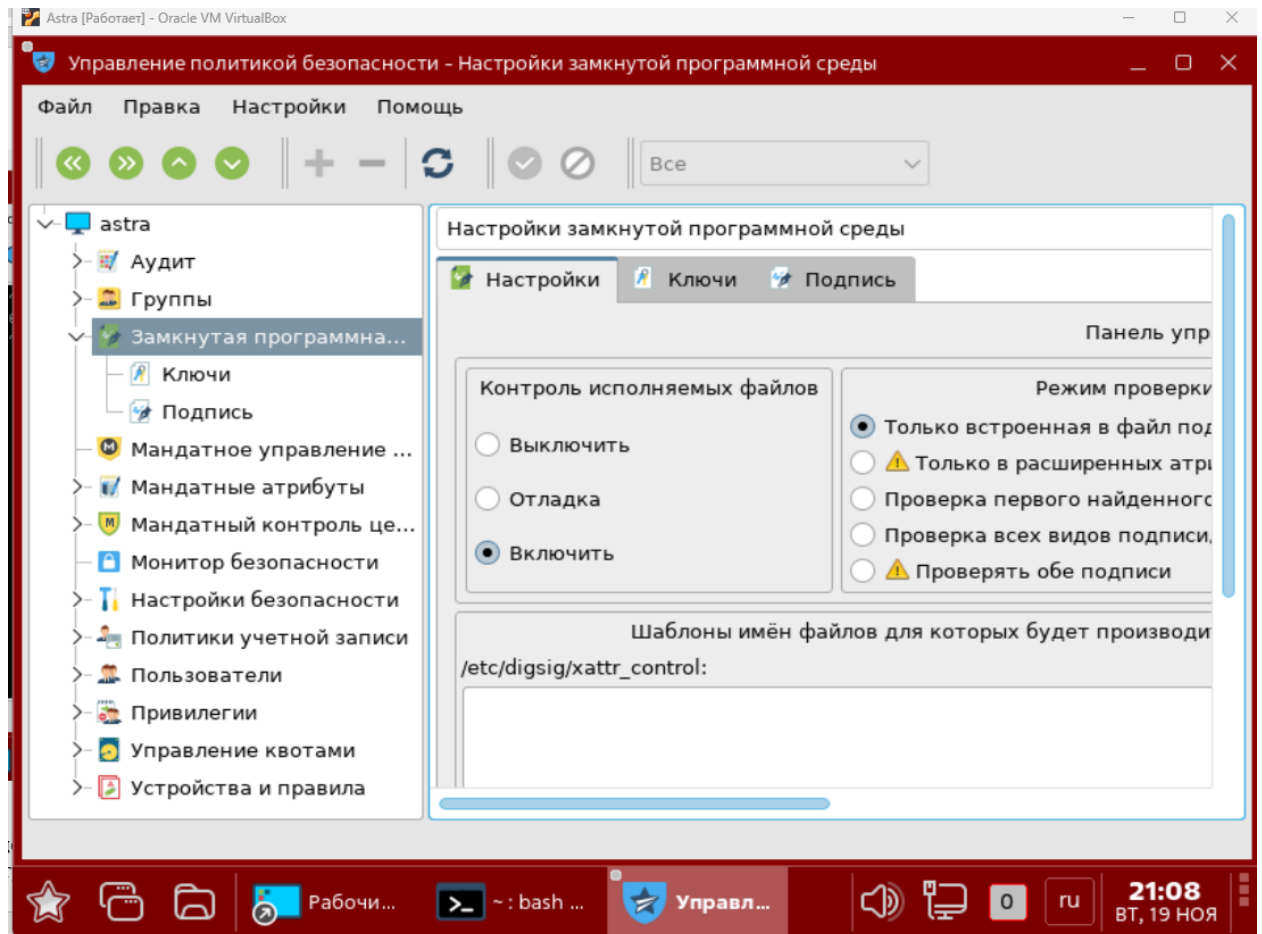


А если мы зайдем в учетную запись с атрибутом целостности уровня «Высокий», то получать ошибки мы не будем

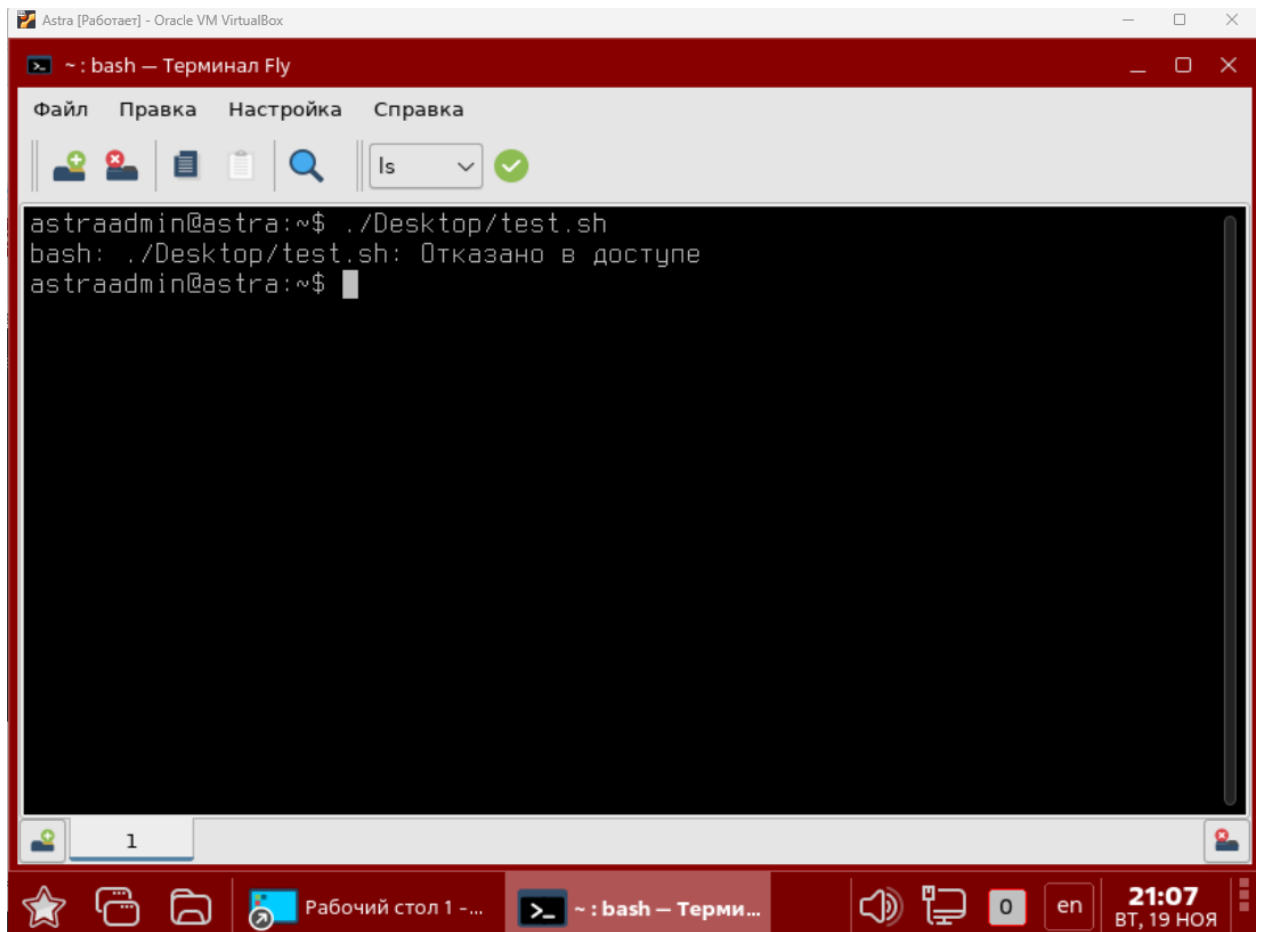


4. Включить режим замкнутой программной среды (ЗПС), проверить работу механизма (попытка запуска неподписанного исполняемого файла), в отчете показать блокировку доступа

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



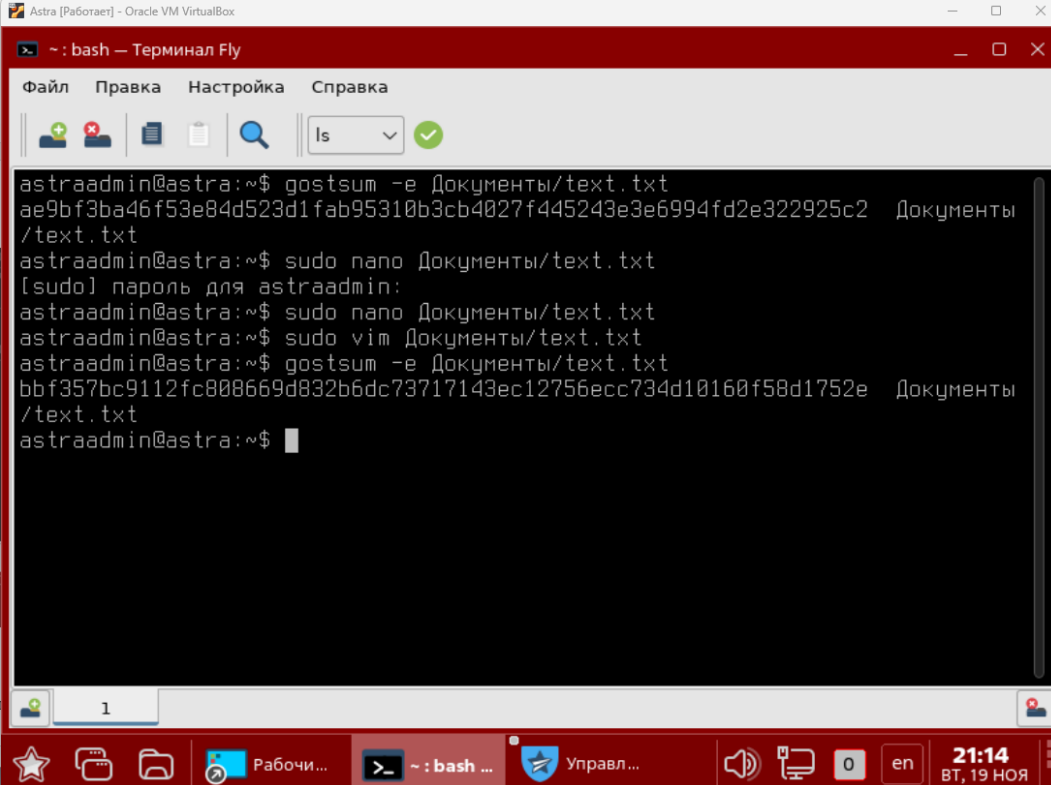
Результат выполнения в виде ошибки представлен на скриншоте ниже:



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



```
Astra [Работа] - Oracle VM VirtualBox
~: bash — Терминал Fly
Файл  Правка  Настройка  Справка
[Icons] [Search] [ls] [Checkmark]

astraadmin@astra:~$ gostsum -e Документы/text.txt
ae9bf3ba46f53e84d523d1fab95310b3cb4027f445243e3e6994fd2e322925c2  Документы
/text.txt
astraadmin@astra:~$ sudo nano Документы/text.txt
[sudo] пароль для astraadmin:
astraadmin@astra:~$ sudo nano Документы/text.txt
astraadmin@astra:~$ sudo vim Документы/text.txt
astraadmin@astra:~$ gostsum -e Документы/text.txt
bbf357bc9112fc808669d832b6dc73717143ec12756ecc734d10160f58d1752e  Документы
/text.txt
astraadmin@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 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 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

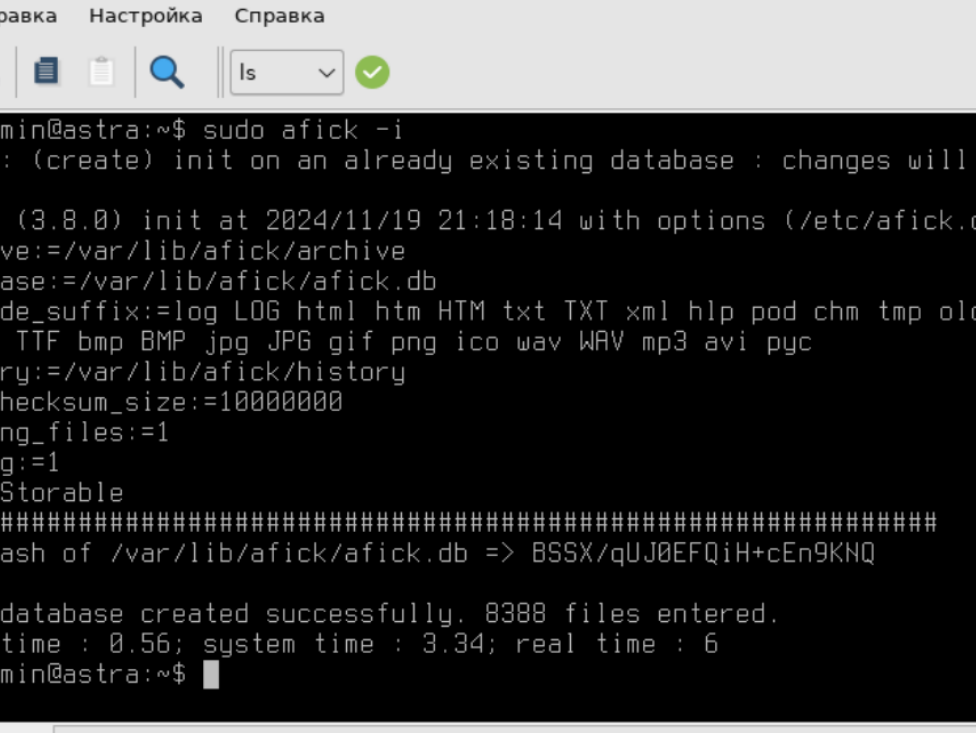
Эта команда добавляет строку «asdf» в конец файла /sbin/blkid.

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.




The screenshot shows a terminal window titled '~: bash — Терминал Fly' with a menu bar (Файл, Правка, Настройка, Справка) and a toolbar. The terminal output is as follows:

```
astraadmin@astra:~$ sudo afick -i
WARNING: (create) init on an already existing database : changes will be lost
# Afick (3.8.0) init at 2024/11/19 21:18:14 with options (/etc/afick.conf):
# archive:=/var/lib/afick/archive
# database:=/var/lib/afick/afick.db
# 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 pyc
# history:=/var/lib/afick/history
# max_checksum_size:=10000000
# running_files:=1
# timing:=1
# dbm:=Storable
# #####
# MD5 hash of /var/lib/afick/afick.db => BSSX/qUJ0EFQiH+cEn9KNQ

# Hash database created successfully. 8388 files entered.
# user time : 0.56; system time : 3.34; real time : 6
astraadmin@astra:~$
```

The bottom of the image shows the Windows taskbar with icons for a star, chat, folder, and a clock displaying 21:20 on 19 NOV.



```
Astra [PaGoRaer] - Oracle VM VirtualBox
~: bash — Терминал Fly
Файл  Правка  Настройка  Справка
|| [Icons] || [ls] [✓]
astraadmin@astra:~$ sudo cp /sbin/sysctl /sbin/sysctl.bak
astraadmin@astra:~$ sudo cp /sbin/blkid/ /sbin/blkid.bak
cp: не удалось выполнить stat для '/sbin/blkid/': Это не каталог
astraadmin@astra:~$ sudo cp /sbin/blkid /sbin/blkid.bak
astraadmin@astra:~$
```

```

astraadmin@astra:~$ echo asdf | sudo tee -a /sbin/blkid
asdf
astraadmin@astra:~$ sudo chmod 700 /sbin/sysctl

```

```
# detailed changes
changed file : /usr/sbin/blkid
      filesize      : 113264      113269
      md5           : 0d2dddda0d2af4f4bd79a5608f2ad790      c90b7136664
7de097d0f38721274e5cb
      mtime         : Mon Apr  1 18:15:26 2024      Tue Nov 19 21:31:46
      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

Возвращаем исходное состояние файлов

```
astraadmin@astra:~$ sudo cp /sbin/blkid.bak /sbin/blkid
astraadmin@astra:~$ sudo cp /sbin/sysctl.bak /sbin/sysctl
astraadmin@astra:~$ sudo afick -k
```

```
# summary changes
changed file : /usr/sbin/blkid
changed file : /usr/sbin/sysctl

# detailed changes
changed file : /usr/sbin/blkid
      mtime      : Mon Apr  1 18:15:26 2024      Tue Nov 19 21:34:36
      2024
changed file : /usr/sbin/sysctl
      filemode    : 100755      100700
      mtime      : Mon Jun 17 02:25:17 2024      Tue Nov 19 21:35:01
      2024
# #####
```