



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»

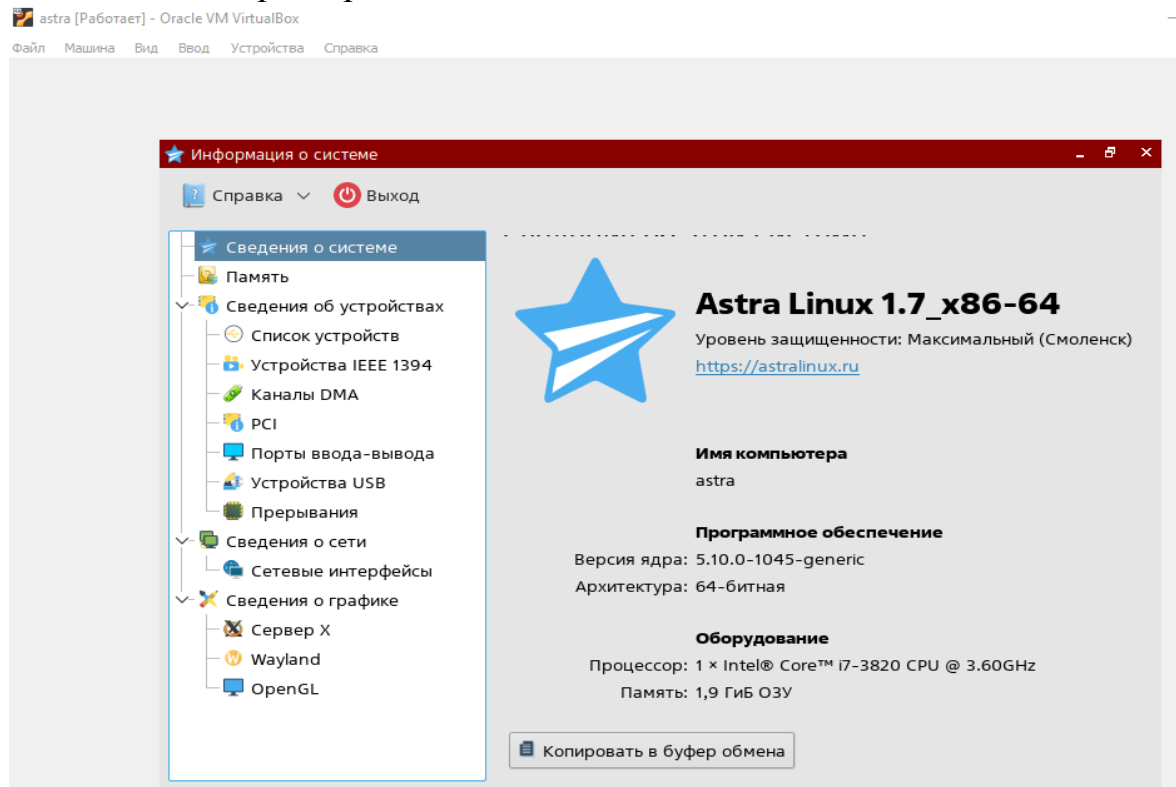
Дисциплина «Технологии обеспечения информационной безопасности»

**Отчет
о проделанной практической работе**

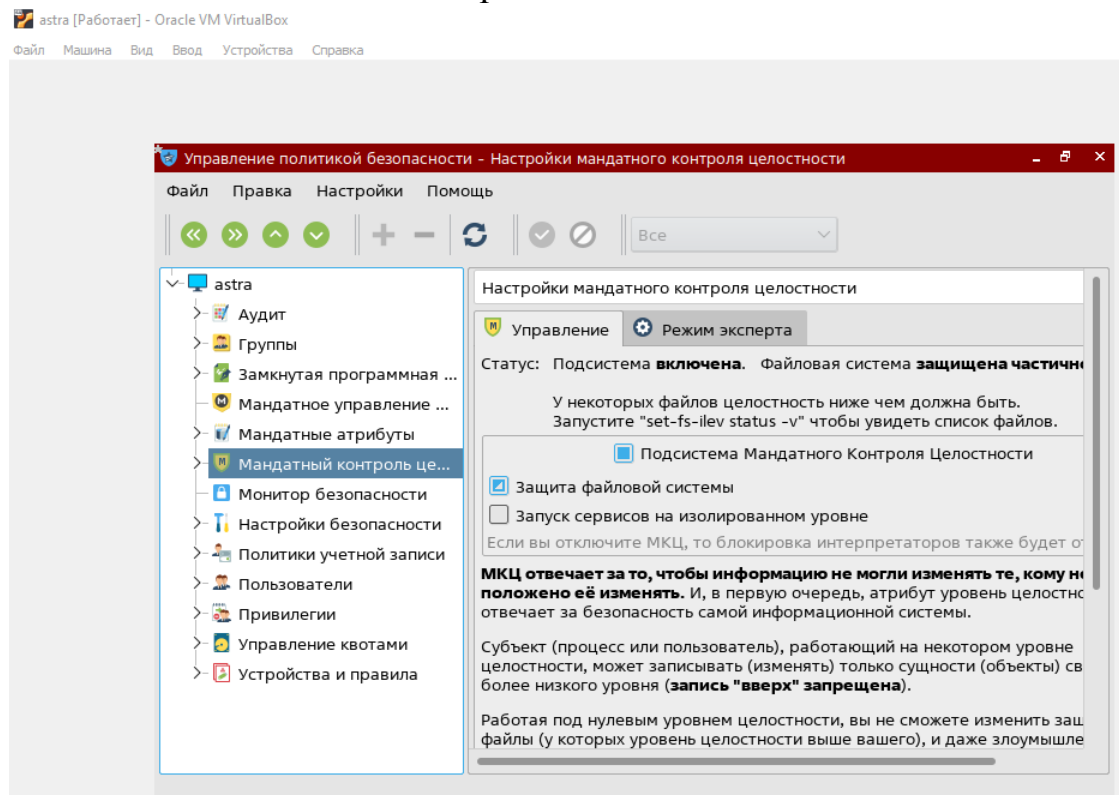
**Выполнил студент 1 курса
Группы: ББМО-02-24
ФИО
Овечкин Александр Романович**

**Москва
2024**

1. Скачиваем и разворачиваем VM с ОС Astra Linux



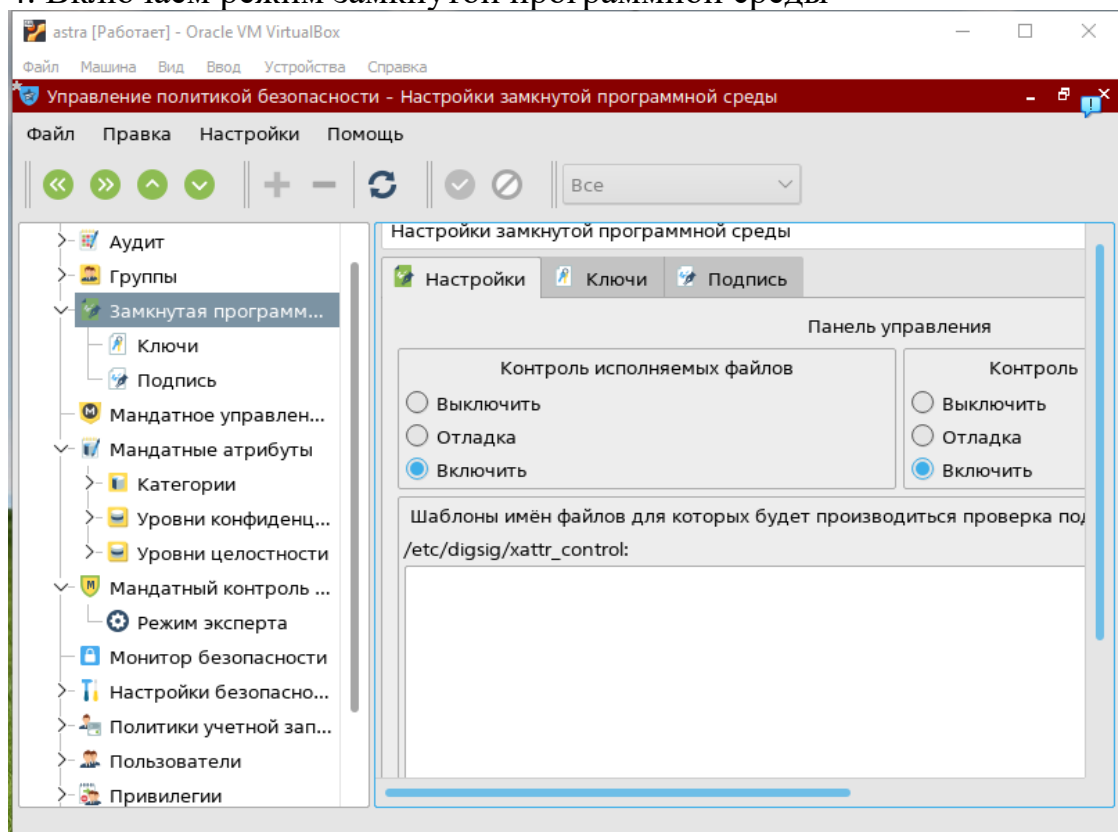
2. Включаем мандатный контроль целостности

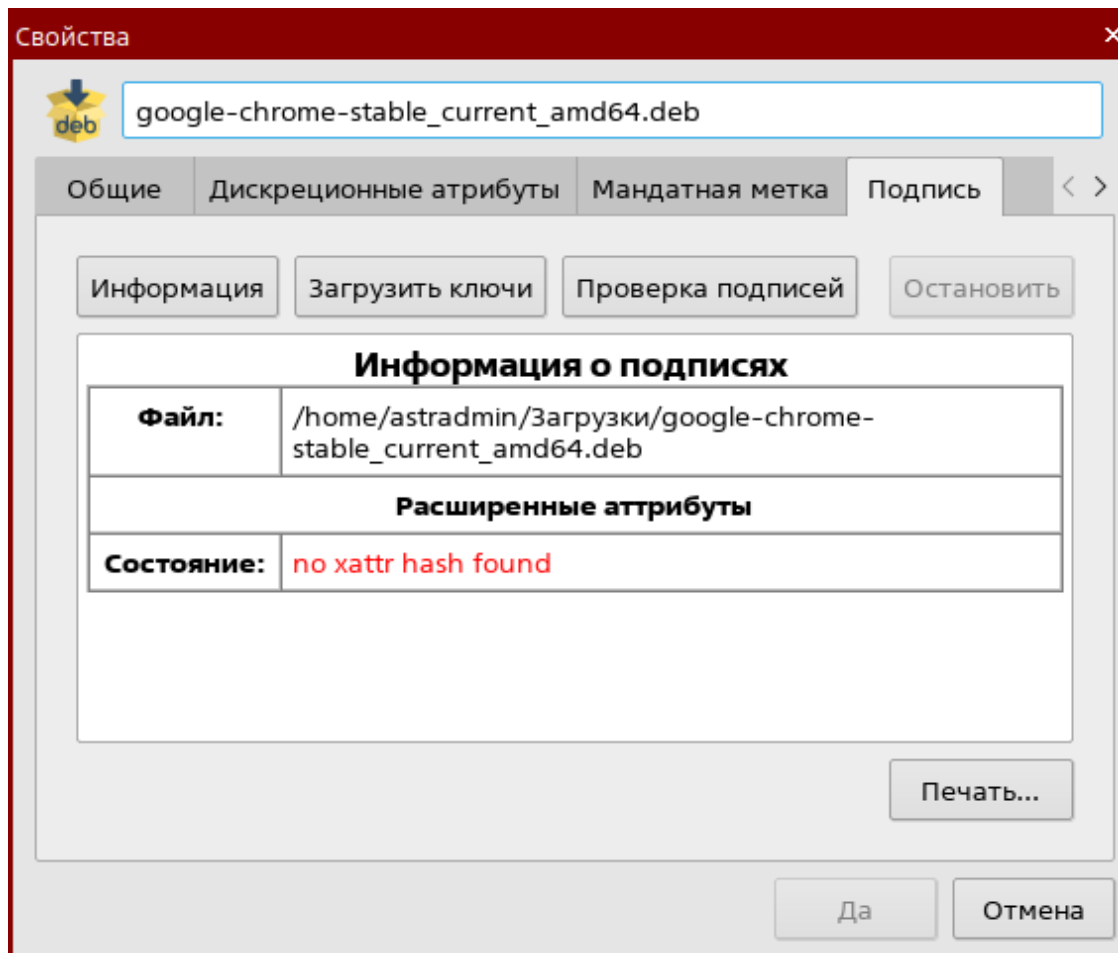


3. Проверка работы механизма МКЦ

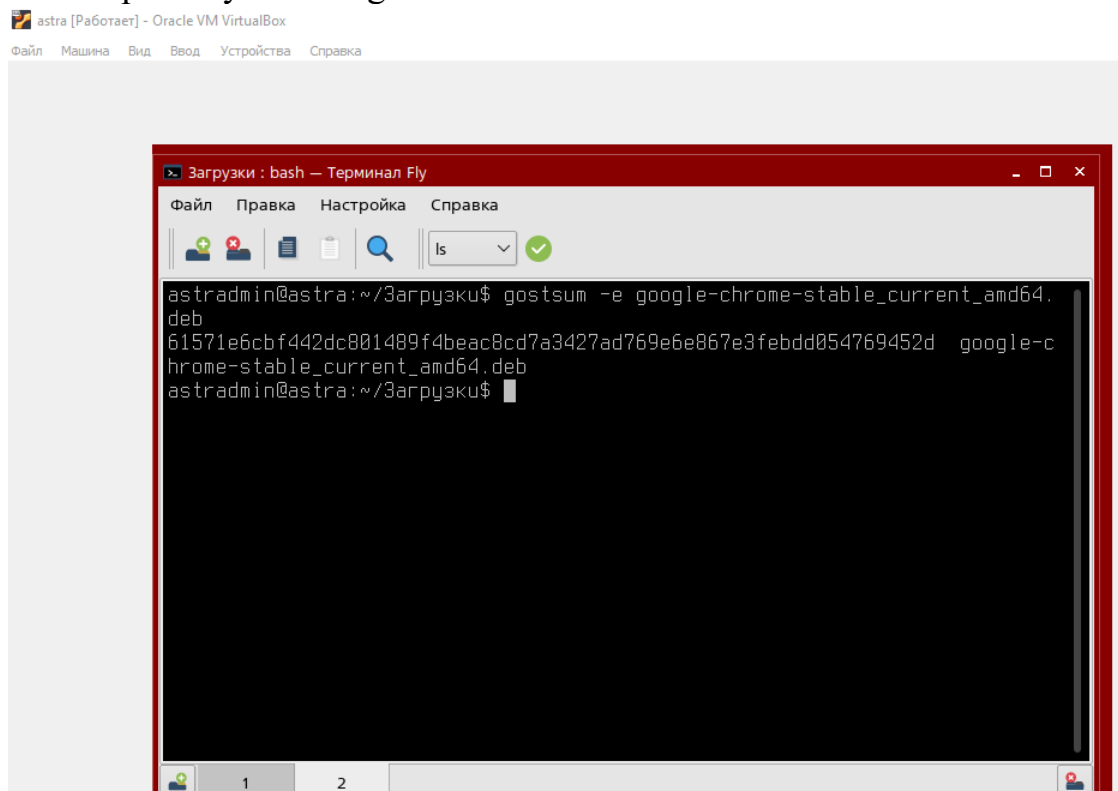
```
astradmin@astra:~/Зарпезку$ whoami
astradmin
astradmin@astra:~/Зарпезку$ ls
google-chrome-stable_current_amd64.deb  mandat.txt
astradmin@astra:~/Зарпезку$
```

4. Включаем режим замкнутой программной среды





5. Настройка утилиты gostsum



6. Настройка утилиты afick

```

astradmin@astra:~$ sudo afick -i
[sudo] пароль гня astradmin:
WARNING: (create) init on an already existing database : changes will be lost
# Afick (2.11-1) init at 2024/02/14 08:14:46 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:=10000000
# dbm:=GDBM_File

astradmin@astra:~$ sudo touch /sbin/exlploit.sh
astradmin@astra:~$ sudo afick -k
# Afick (2.11-1) compare at 2024/02/14 08:16:04 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:=10000000
# dbm:=GDBM_File
# last run on 2024/02/14 08:15:11 with afick version 2.11-1
new file : /usr/sbin/exlploit.sh
changed directory : /usr/sbin

# detailed changes

# detailed changes
new file : /usr/sbin/exlploit.sh
inode_date : Wed Feb 14 08:15:57 2024
changed directory : /usr/sbin
mtime : Tue Feb 13 23:00:58 2024 Wed Feb 14 08:15:57 2024

# Hash database : 7864 files scanned, 2 changed (new : 1; delete : 0; changed : 1; dangling : 0; exclude_suffix : 0; exclude_prefix : 0; exclude_re : 0; degraded : 0)
# #####
# MD5 hash of /var/lib/afick/afick => hJ6KwOCqYtKF784Ep8VFRQ
# user time : 2.14; system time : 4.48; real time : 7

```