

ПРЗ 4.2 Контроль целостности

Задание

Astra Linux SE

1. Скачать и развернуть [ВМ с ОС Astra Linux](#) для отработки практических заданий
2. Включить мандатный контроль целостности (МКЦ) в соответствии с руководством по [Wiki](#), [КСЗ](#)
3. Проверить работу механизма МКЦ (запрет на запись "вверх" - NWU), в отчете показать блокировку доступа
4. Включить режим замкнутой программной среды (ЗПС), проверить работу механизма (попытка запуска неподписанного исполняемого файла), в отчете показать блокировку доступа
5. Настроить и продемонстрировать работ утилит контроля целостности и регламентного контроля целостности [gostsum](#), [afick](#)

Рис. 1 – Astra Linux.

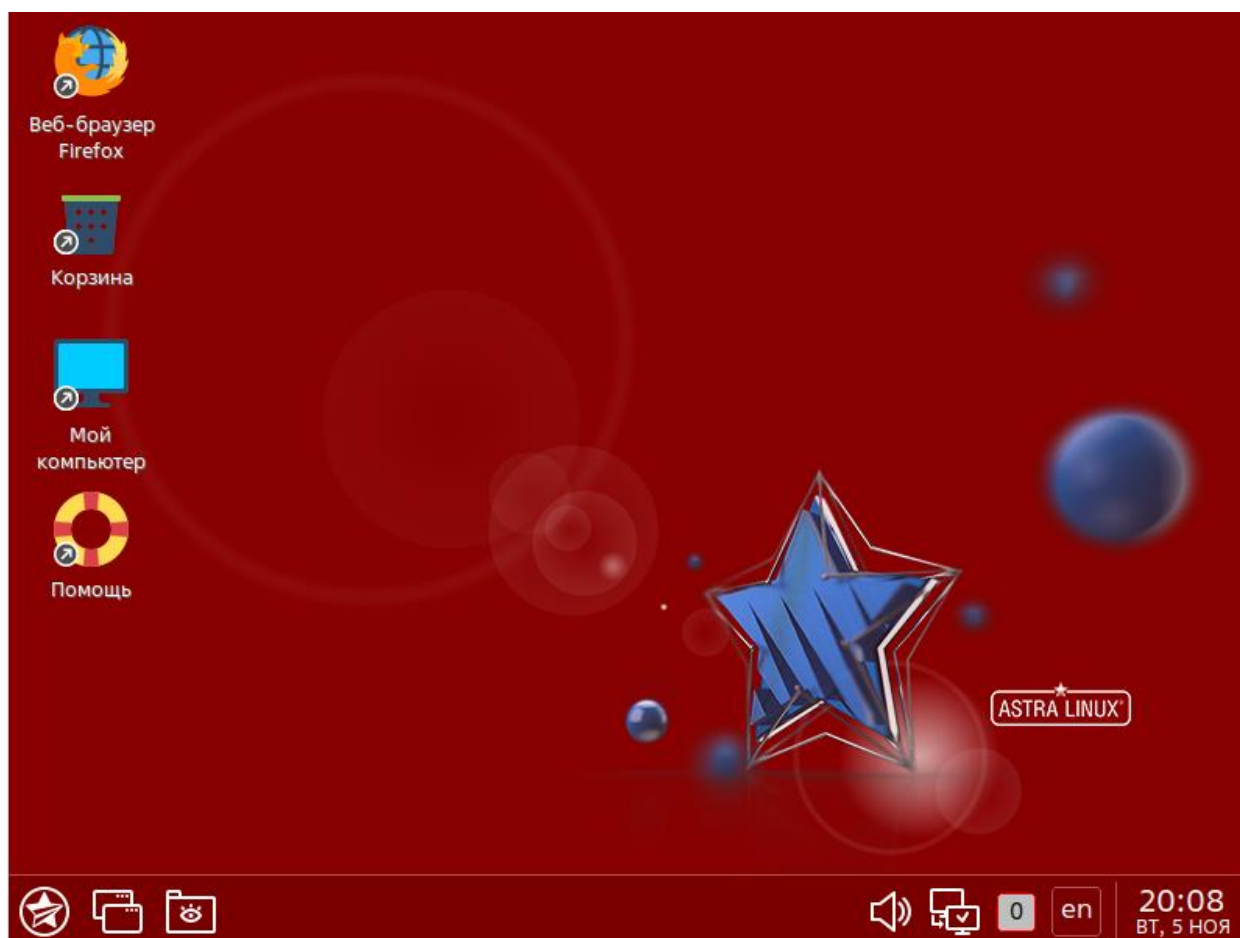


Рис. 2 – Включение мандатного доступа.

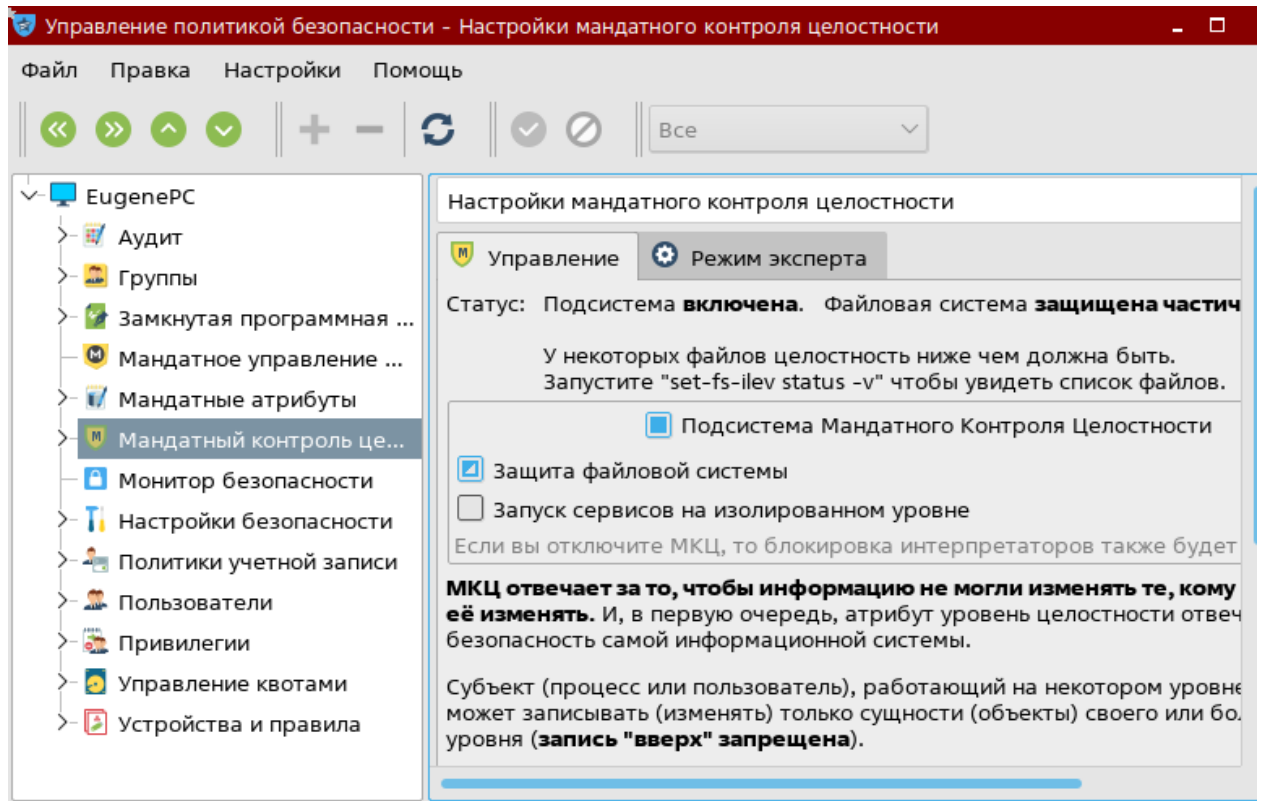


Рис. 3 – АВАС для начальника отдела безопасности.

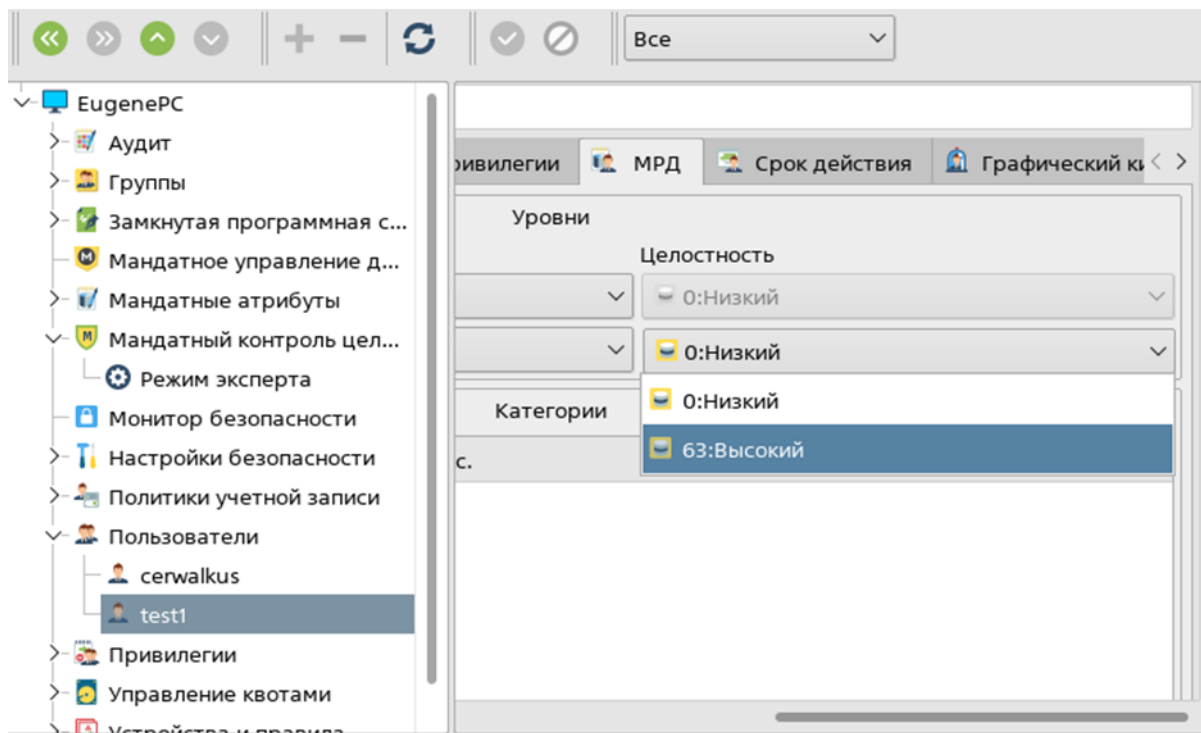


Рис. 4 – Вход под новым пользователем

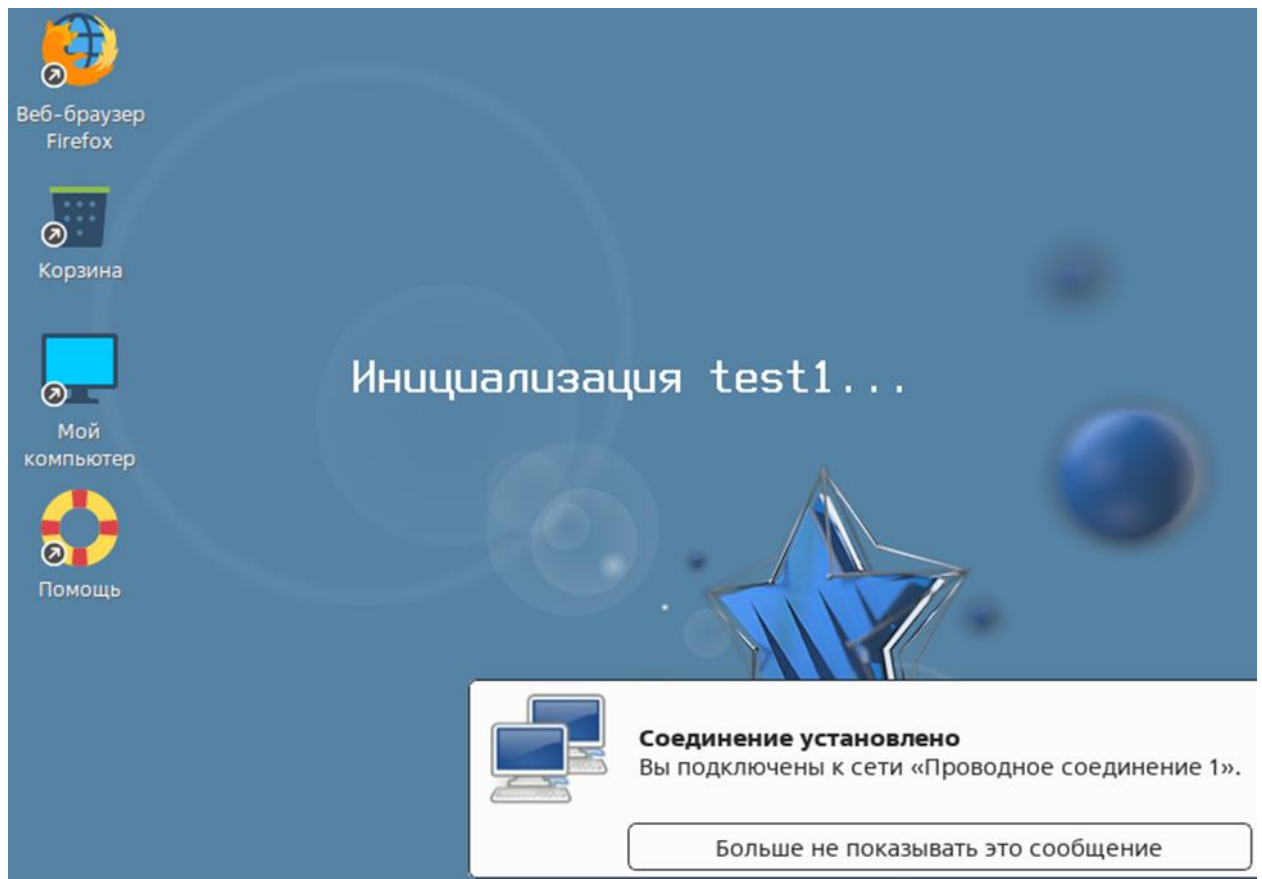




Рис. 5 – Уровень целостности пользователя

```
test1@EugenePC:~$ su
Пароль:
Password blocked
^C
test1@EugenePC:~$ su
Пароль:
Password blocked
su: Сбой при проверке подлинности
test1@EugenePC:~$ pdp-id
Уровень конф.=0(Уровень_0), Уровень целостности:0(Низкий), Категории=0x0(Нет)
Ролл=()
test1@EugenePC:~$ id
uid=1001(test1) gid=1002(test1) группы=1002(test1),20(dialout),24(cdrom),25(floppy),29(audio),44(video),46(plugdev),100(users)
test1@EugenePC:~$
```

Рис. 6 – Уровень контроля файла

Файловая система			Редактирование конфига	Исключения
Имя			Текущий уровень целостности	
		 sudoers	63 - Высокий	
		 sysctl.conf	63 - Высокий	

Подсказка: используйте двойной щелчок на уровне чтобы его изменить

Рис. 7 – Открытие файла от лица администратора

```
GNU nano 3.2 /etc/sudoers
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr$
```

Рис. 8 – Редактирование файла

```
GNU nano 3.2 /etc/sudoers
#hello world!
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr$
# Host alias specification

[ Wrote 28 lines ]
^G Помощь      ^O Записать    ^W Поиск      ^K Вырезать   ^J Выровнять
^X Выход       ^R ЧитФайл    ^\ Замена     ^U Отмен. Выр ^T Словарь
```

Рис. 9 – Попытка открыть файл

```
test1@EugenePC:~$ sudo nano /etc/sudoers

Мы полагаем, что Ваш системный администратор изложил Вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

    №1) Уважайте частную жизнь других.
    №2) Думайте, прежде что-то вводить.
    №3) С большой властью приходит большая ответственность.

[sudo] пароль для test1:
Попробуйте ещё раз.
[sudo] пароль для test1:
Попробуйте ещё раз.
[sudo] пароль для test1:
test1 is not in the sudoers file. This incident will be reported.
test1@EugenePC:~$
```

Рис. 10 – Открытие пользователем файла

```
GNU nano 3.2 /etc/sudoers

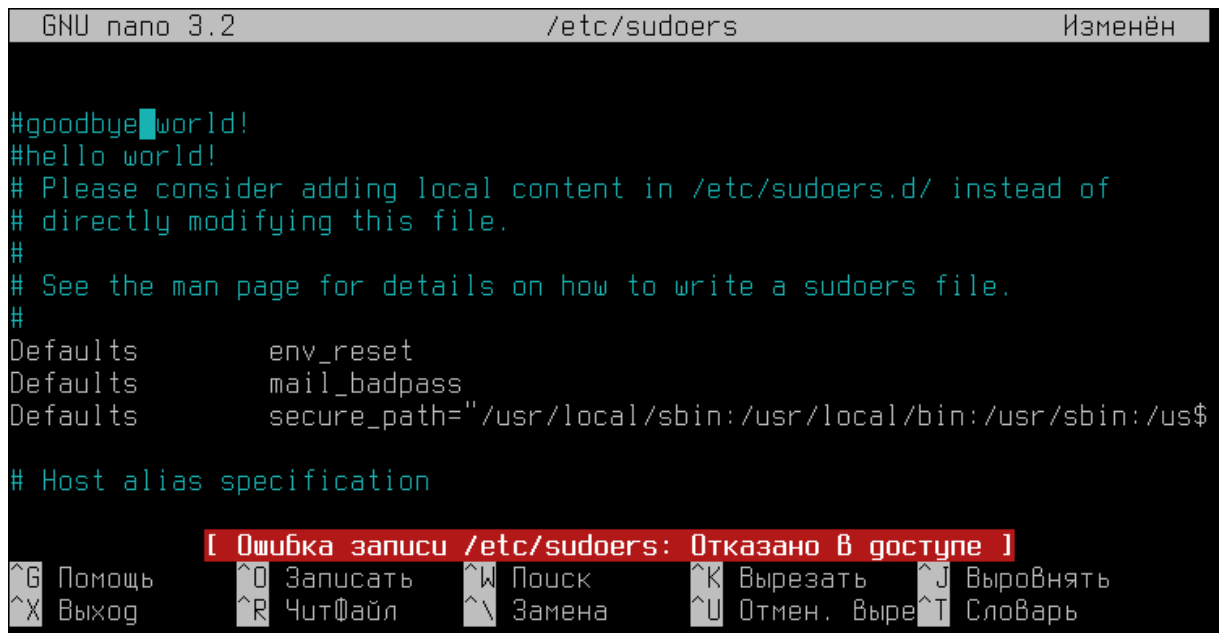
#hello world!
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr$

# Host alias specification

[ File '/etc/sudoers' is unwritable ]

^G Помощь      ^O Запустить  ^W Поиск      ^K Вырезать   ^J Выводить
^X Выход       ^R Чтение     ^\ Замена     ^U Отмен. Выр ^T Словарь
```

Рис. 11 – Попытка сохранить изменения



```
GNU nano 3.2 /etc/sudoers Изменён

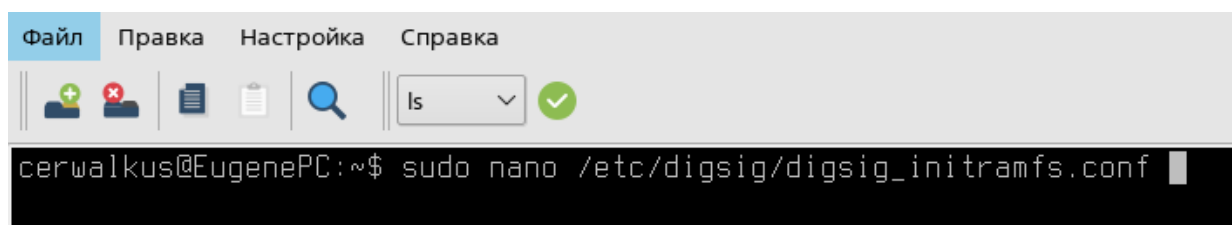
#goodbye world!
#hello world!
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr$

# Host alias specification

[ Ошибка записи /etc/sudoers: Отказано в доступе ]

^G Помощь      ^O Запустить  ^W Поиск      ^K Вырезать   ^J Выровнять
^X Выход        ^R ЧутьФайл   ^\ Замена     ^U Отмен. Выре ^T Словарь
```

Рис. 12 – Включение режима замкнутой программной среды (ЗПС)

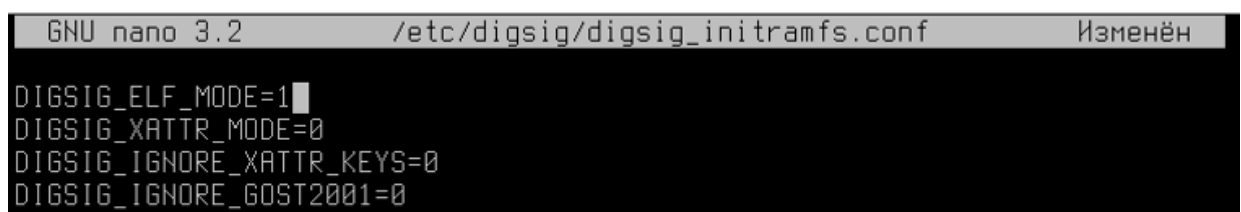


```
Файл  Правка  Настройка  Справка

|| [Icons] || [ls] [checkmark]

cerwalkus@EugenePC:~$ sudo nano /etc/digsig/digsig_initramfs.conf
```

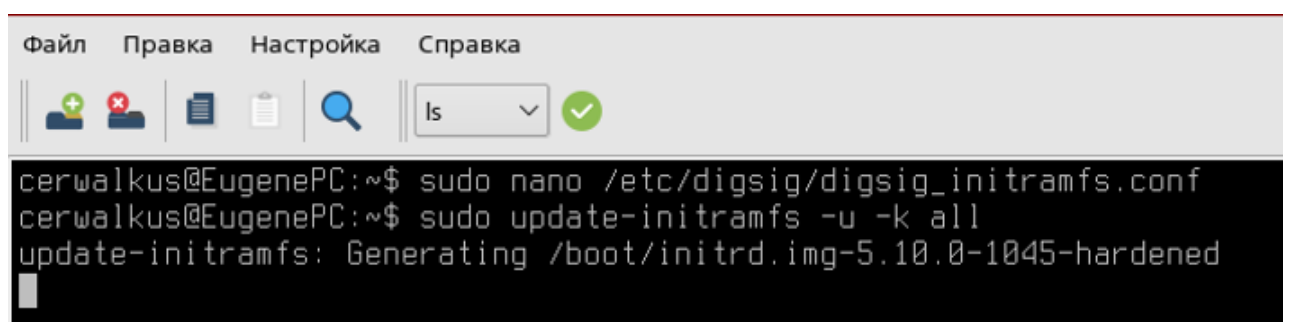
Рис. 13 – Конфигурационный файл



```
GNU nano 3.2 /etc/digsig/digsig_initramfs.conf Изменён

DIGSIG_ELF_MODE=1
DIGSIG_XATTR_MODE=0
DIGSIG_IGNORE_XATTR_KEYS=0
DIGSIG_IGNORE_GOST2001=0
```

Рис. 14 – Подтверждение



```
Файл  Правка  Настройка  Справка

|| [Icons] || [ls] [checkmark]

cerwalkus@EugenePC:~$ sudo nano /etc/digsig/digsig_initramfs.conf
cerwalkus@EugenePC:~$ sudo update-initramfs -u -k all
update-initramfs: Generating /boot/initrd.img-5.10.0-1045-hardened
```

Рис. 15 – Попытка установки ПО при включенном ЗПС

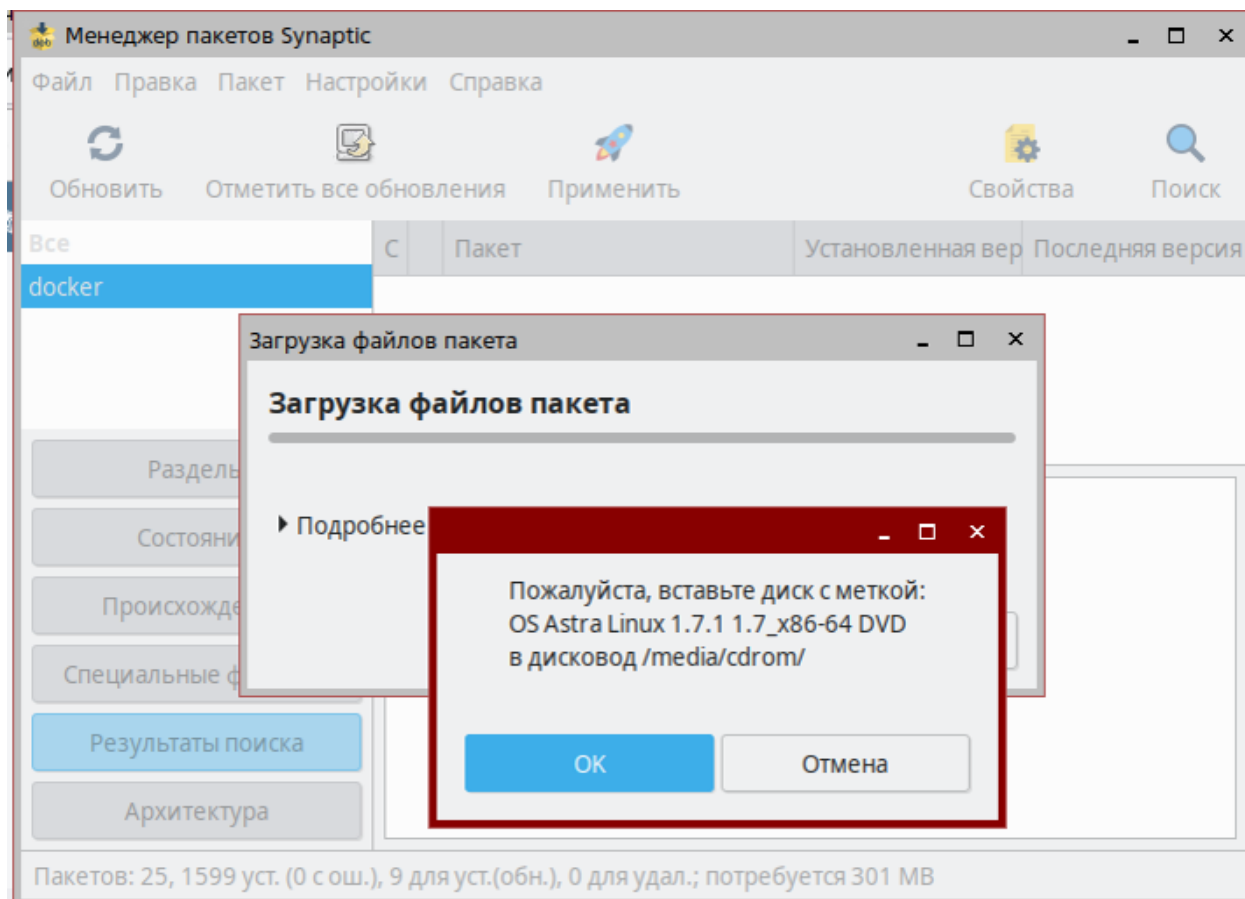


Рис. 16 – Попытки установки через командную строку

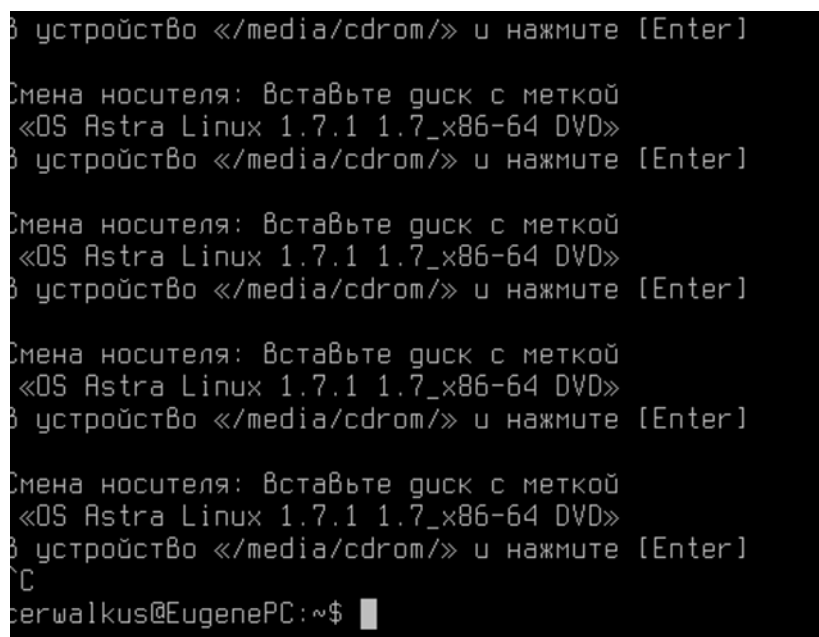


Рис. 17 – Включение режима контроля целостности (неизменности) объектов файловой системы

```
/etc/afick.conf
# afick config sample file
# $Id: afick.conf 987 2006-12-21 15:31:16Z gerbier $
# see afick.conf documentation for more informations

#####
# directives section
#####
# binary values can be : yes/1/true or no/0/false
# database : name with full path to database file
database:=/var/lib/afick/afick
# history : name with full path to history file
history := /var/lib/afick/history
# archive : name with full path to directory for archived results
archive := /var/lib/afick/archive
# report_url : where to send the result : stdout/stderr/null
report_url := stdout
# report_syslog : send output to syslog ?
report_syslog := no
# verbose : (obsolete) boolean value
# use debug parameter below
verbose := no
# debug : set a level of debugging messages, from 0 (none) to 4 (full)
debug := 0
# warn_dead_symlinks : boolean : if set, warn about dead symlinks
warn_dead_symlinks := no
```

Рис. 18 – Добавление созданного файла в конфигурационный файл режима контроля целостности (с допущенной ошибкой).

```
/etc/afick.conf
#!/root/.bash_history
#!/root/.mc
# !/root/tmp

#/var/ftp MyRule
#/var/log Logs
# ! /var/log/ksymoops
# /var/www MyRule
# ! /var/www/html/snortsnarf
/boot GOST
/lib/modules PARSEC
/etc/security PARSEC
/etc/pam.d PARSEC
/lib/x86_64-linux-gnu/security PARSEC
/lib/security PARSEC
/sbin PARSEC
/etc/fstab PARSEC
/usr/sbin PARSEC
/home/testa/test1

#####
# to allow easier upgrade, my advice is too separate
# the default configuration file (above) from your
# local configuration (below).
# default configuration will be upgraded
```


Рис. 19 – Уведомление об изменении

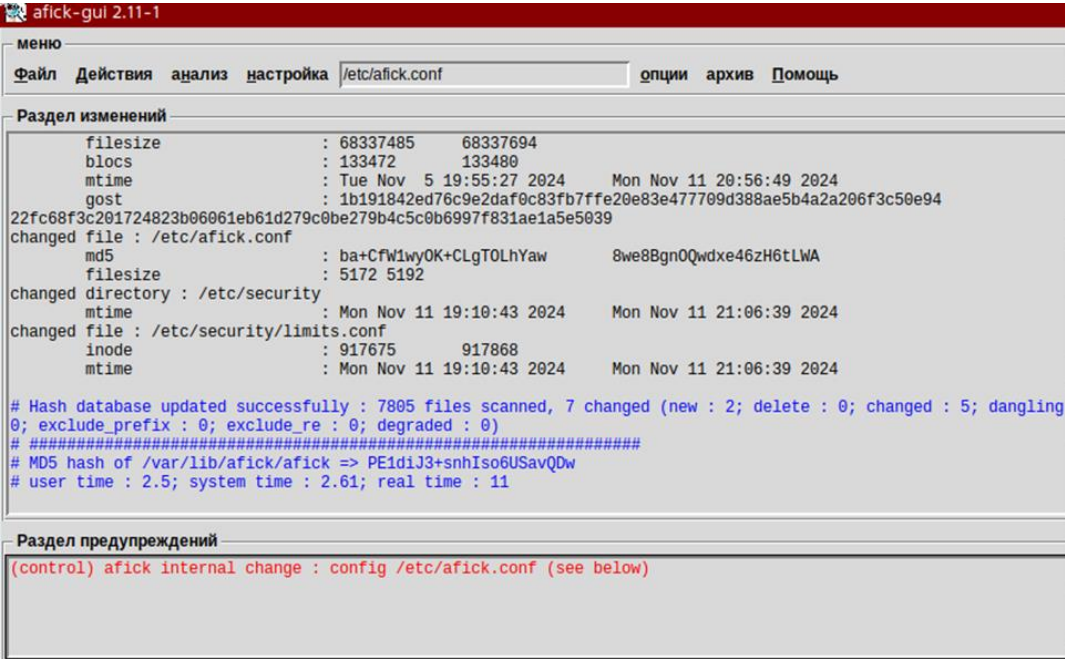


Рис. 20 – Ошибка в конфигурационном файле

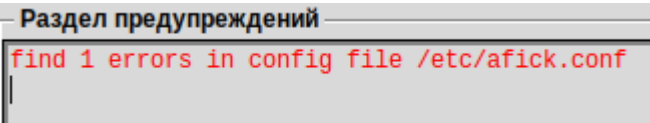


Рис. 21 – Изменение файла

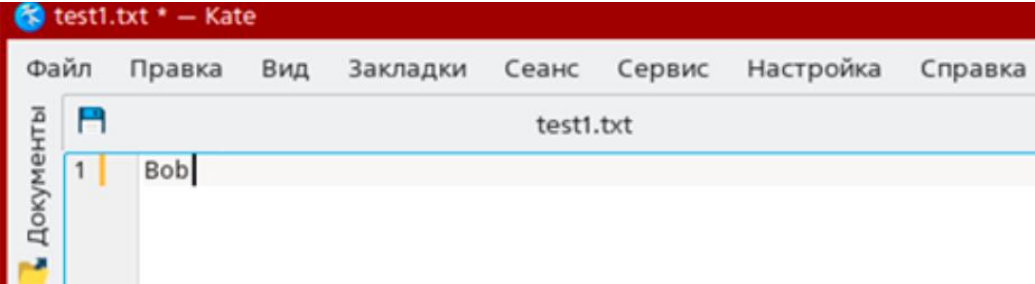


Рис. 22 – Уведомление об изменении файла

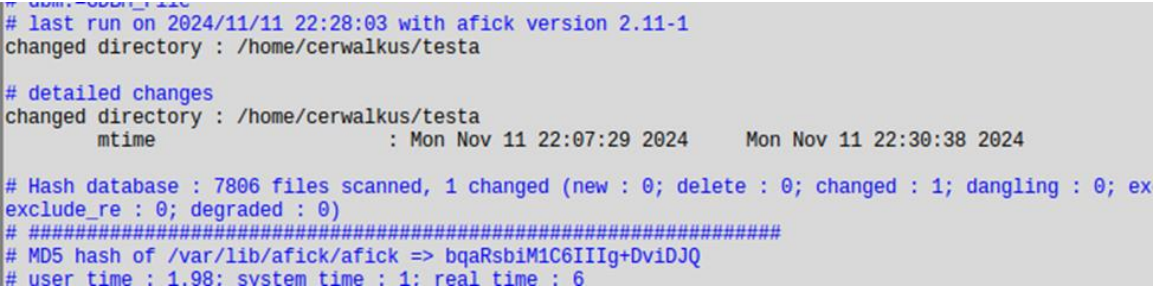


Рис. 23 – Запуск средства контроля gostsum

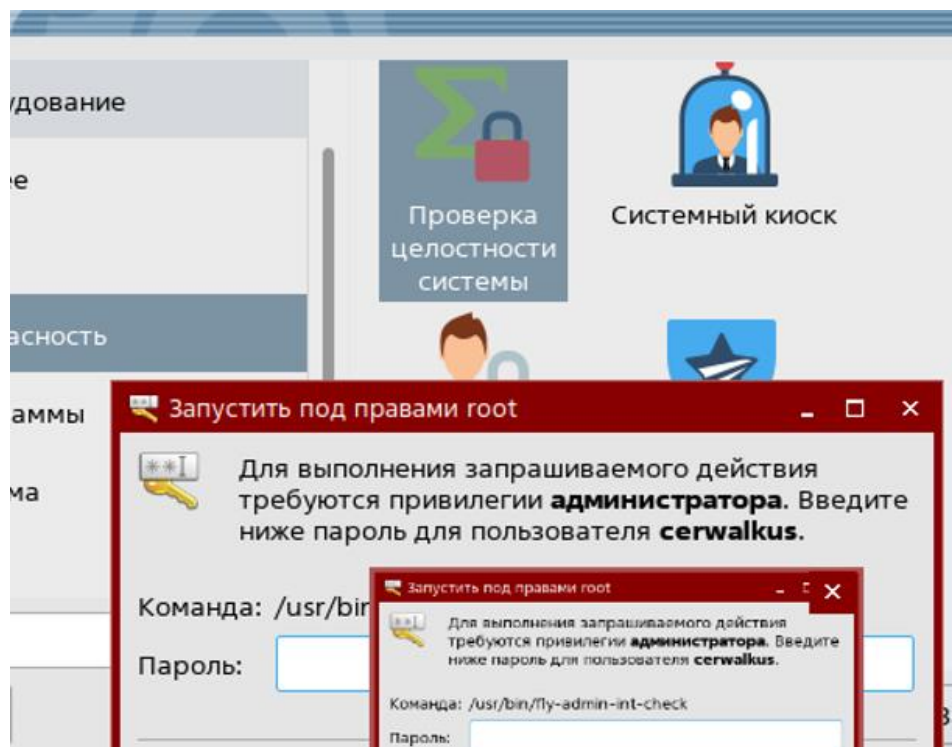


Рис. 24 – Эталонный файл

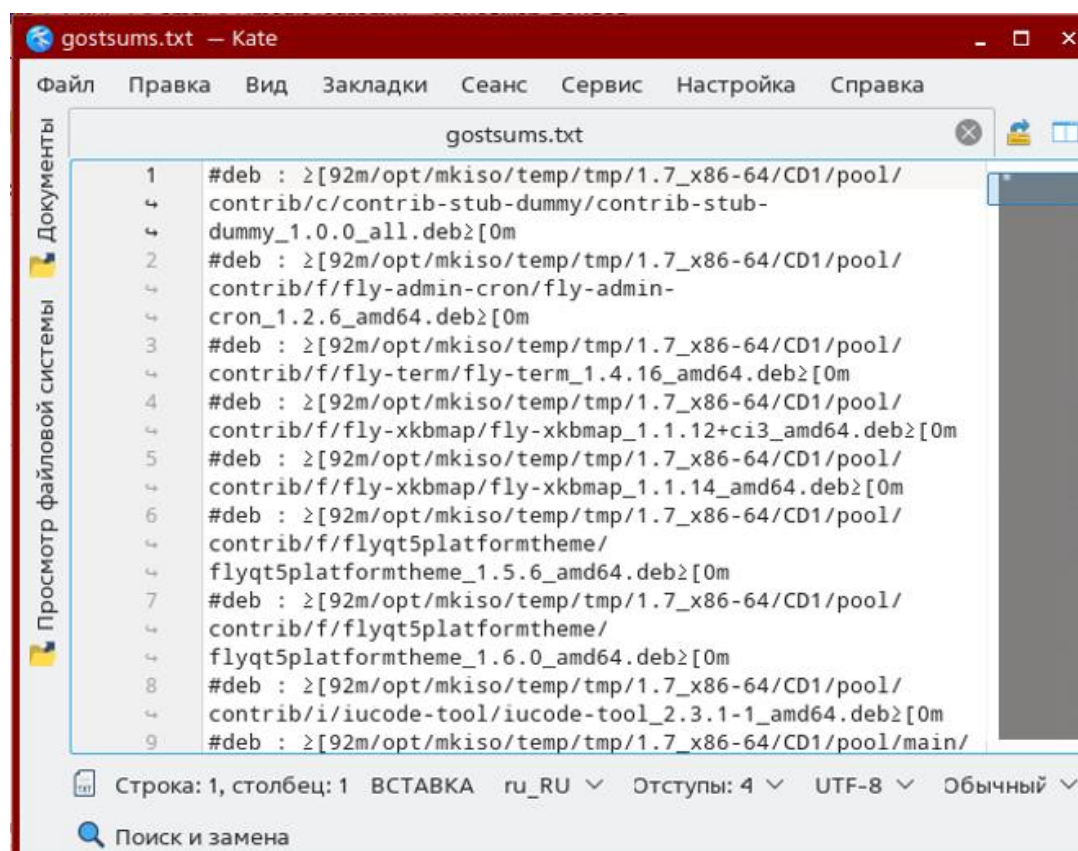


Рис. 25 – Результат проверки

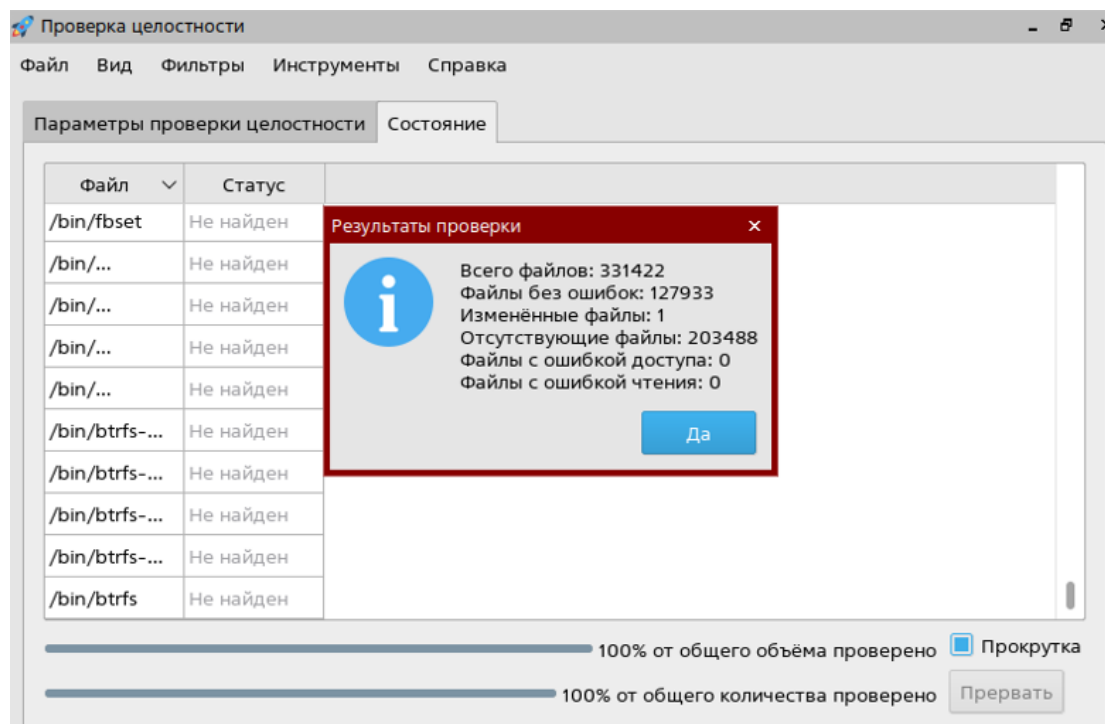


Рис. 26 – Выявленные проблемы

