МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
 «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**ОТЧЁТ**

**по лабораторной работе №11**

**«**Настройка механизмов организации замкнутой программной среды.Контроль целостности комплекса средств защиты.**»**

Выполнил: студент гр. ВКБ41

Якушевский С.С.

Проверил:

доц. Скляров А.В.

асс. Кацай А.М.

**Цель:** изучить принципы и технологии контроля целостности данных (в том

числе комплекса средств защиты – КСЗ), реализованных в ОССН. Освоить умения,

необходимые для решения задач подсчёта носителей контрольных сумм файлов и

оптических носителей, контроля соответствия дистрибутиву, регламентного

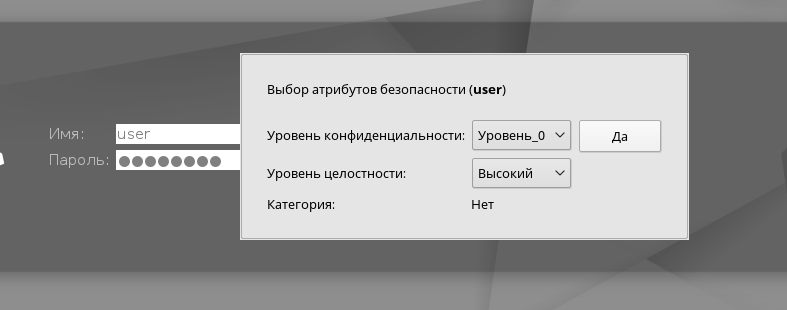
контроля целостности и создания замкнутой программной среды..

Ход работы:

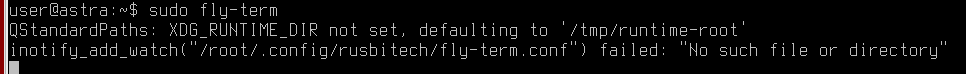
**1.** Начать работу со входа в ОССН в графическом режиме с учётной

привилегированного пользователя пользователя, например: user (уровень доступа

— 0, неиерархические категории — нет, уровень целостности — «Высокий»)



и запустить терминал Fly в «привилегированном» режиме командой sudo flyterm.

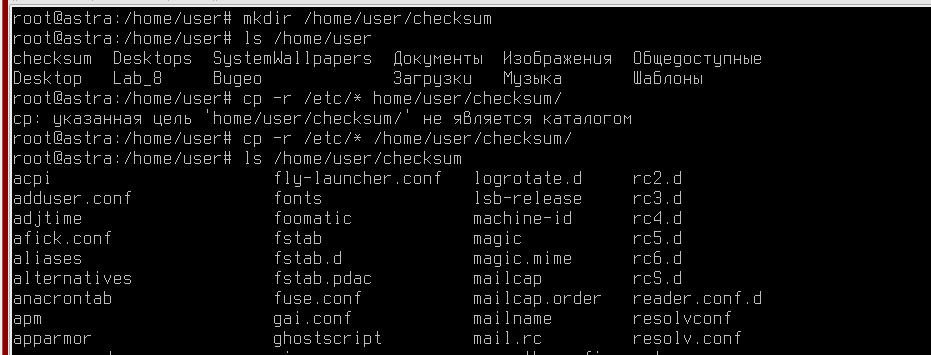


**2.** В домашнем каталоге создать подкаталог checksum и скопировать в

него все файлы (включая вложенные каталоги) из каталога /etc.

mkdir /home/user/checksum

cp -r /etc/\* home/user/checksum/



**3.** Используя алгоритм MD5, вычислить контрольные суммы всех файлов в

каталоге /home/user/checksum и перенаправить результат их вычисления в

файл /home/user/md5.check, а поток с перечнем ошибок в файл

/home/user/error.md5, командой

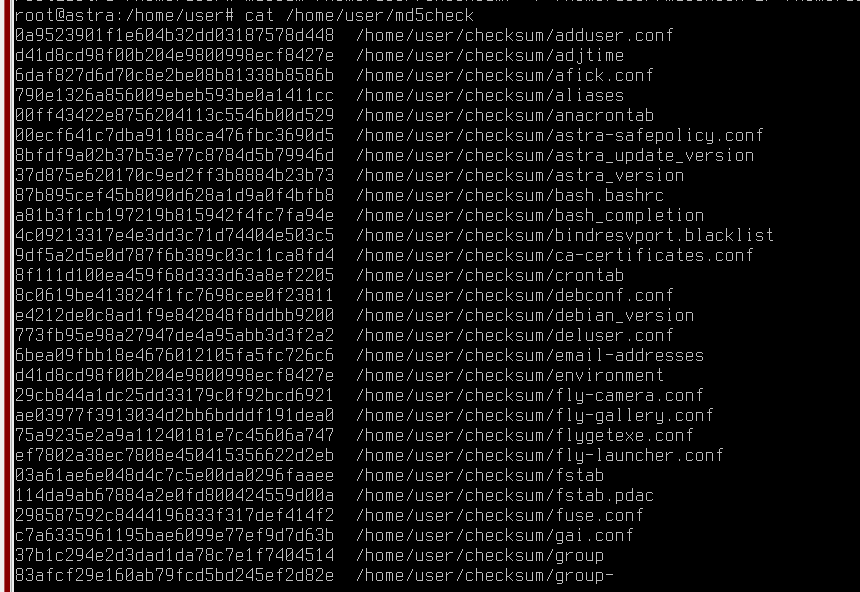
md5sum /home/user/checksum/\* > /home/user/md5check 2> /home/user/error.md5



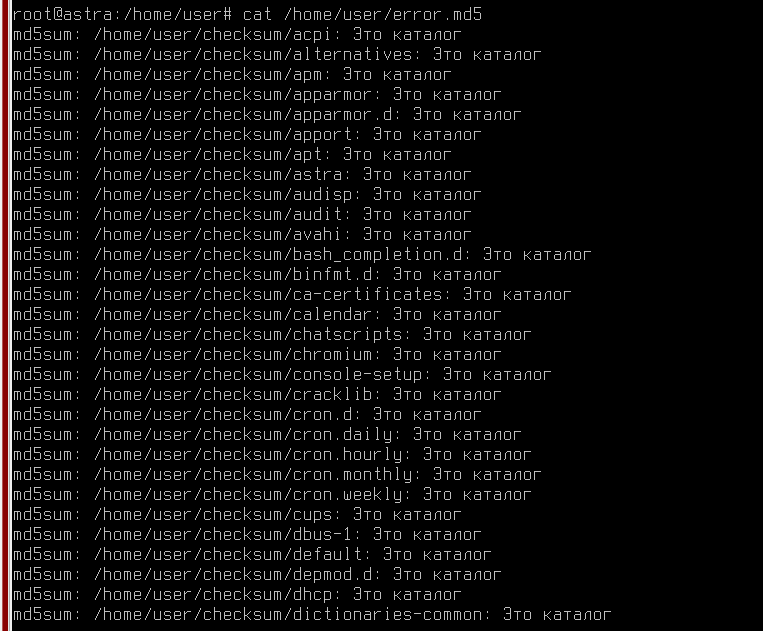
**4.** Вывести в терминал содержимое файлов /home/user/md5check и

/home/user/error.md5 цепочкой команд

cat /home/user/md5check



cat /home/user/error.md5

и указать, для каких объектов в каталоге

/home/user/checksum контрольные суммы не были созданы.

Контрольные суммы не были созданы для каталогов.

5. Используя алгоритм SHA-512/256, вычислить контрольные суммы всех

файлов в каталоге /home/user/checksum и перенаправить результат вычислений в файл /home/user/sha512256check командой

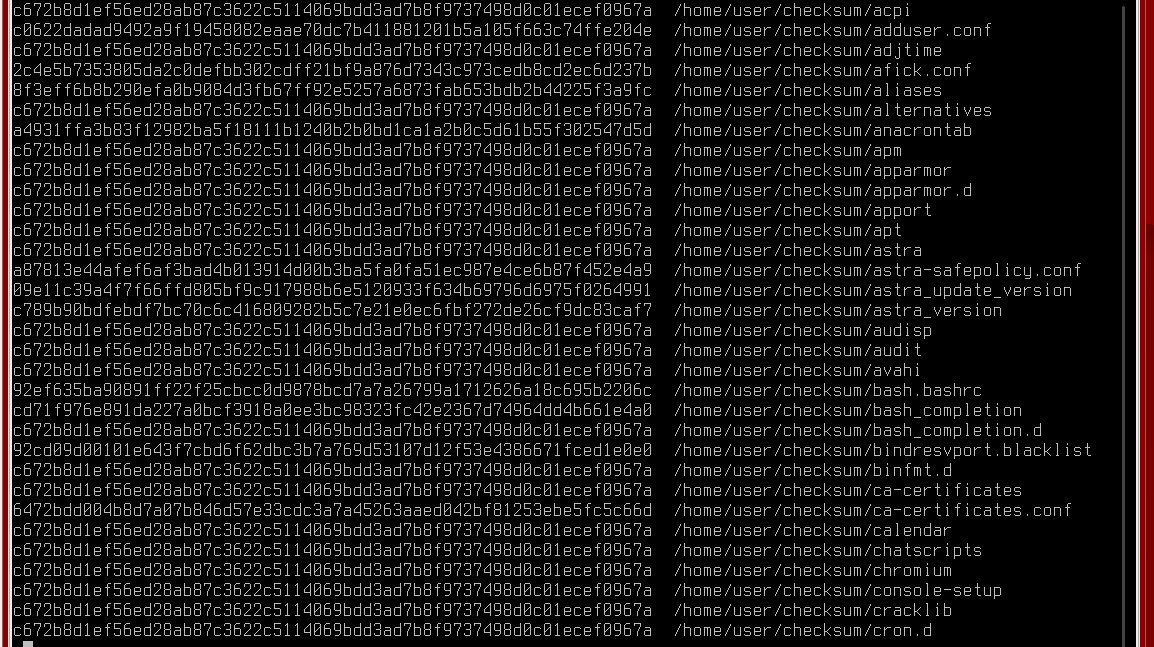
shasum -a 512256 /home/user/checksum/\* > /home/user/sha512256check



Вывести на экран содержимое файла /home/user/sha512256check

командой

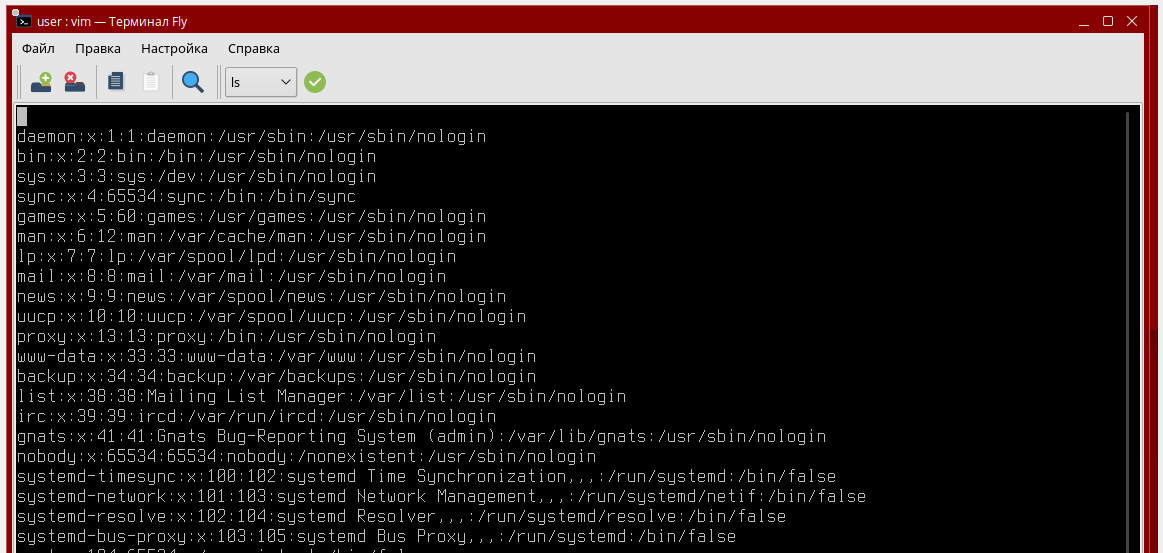
less /home/user/sha512256check



**6.** Используя редактор *vim*, изменить содержимое файла

/home/user/checksum/passwd, удалив из него учётную запись

суперпользователя (строку root: x: 0:0:root: /root: /bin/bash).



**(чтобы выйти и записать из vim : esc -> написать :wq)**

**7.** Используя алгоритм MD5, проверить контрольные суммы всех файлов в

каталоге /home/user/checksum и перенаправить результат проверки в файл

/home/user/fullcheck командой

md5sum -с /home/user/md5check > /home/user/fullcheck

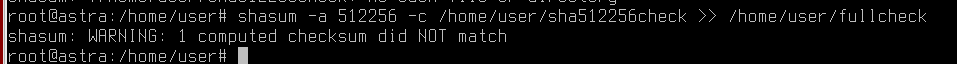


**8.** Используя алгоритм SHA512/256, проверить контрольные суммы всех

файлов в каталоге /home/user/checksum и перенаправить результат проверки (с

добавлением) в файл /home/user/full-check командой

shasum -a 512256 -c ./home/user/sha512256check >> /home/user/fullcheck



**9.** Найти в файле /home/user/fullcheck строки, указывающие на

файлы с нарушением целостности (содержащие слова ПОВРЕЖДЁН и FAILED),

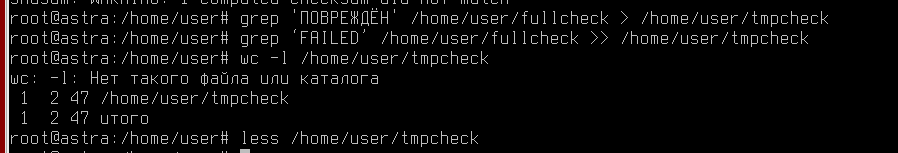
вывести в терминал их содержимое и число цепочкой команд

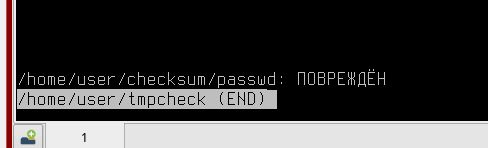
grep 'ПОВРЕЖДЁН' /home/user/fullcheck > /home/user/tmpcheck

grep ‘FAILED’ /home/user/fullcheck >> /home/user/tmpcheck

wc –l /home/user/tmpcheck

less /home/user/tmpcheck



****

**10.** Используя алгоритм ГОСТ P 34. 11-2012 (256 битов), вычислить

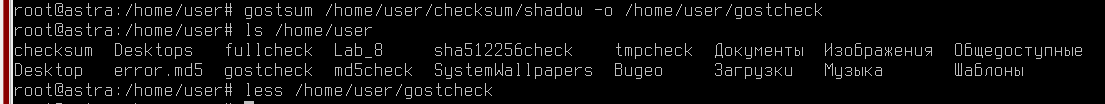
контрольную сумму файла /home/user/checksum/shadow, перенаправить результат

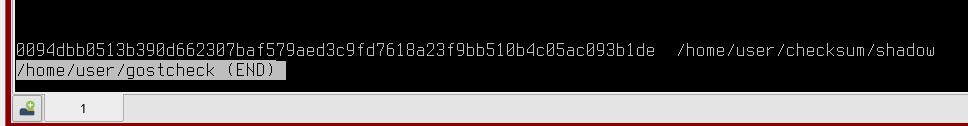
проверки в файл /home/user/gostcheck и вывести в терминал содержимое

файла /home/user/gostcheck цепочкой команд

gostsum /home/user/checksum/shadow -o /home/user/gostcheck

less /home/user/gostcheck.



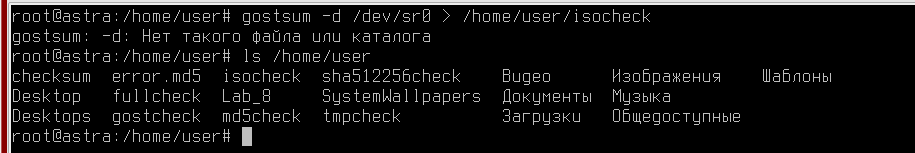


**11.** Установить оптический диск с дистрибутивом ОССН

и, используя алгоритм ГОСТ Р 34. 11-2012 (256 битов), вычислить его контрольную сумму (по умолчанию файл устройства оптического диска /dev/sr0) и перенаправить результат вычисления в файл /home/user/isocheck командой

gostsum –d /dev/sr0 > /home/user/isocheck

(выполнение команды занимает длительное время).



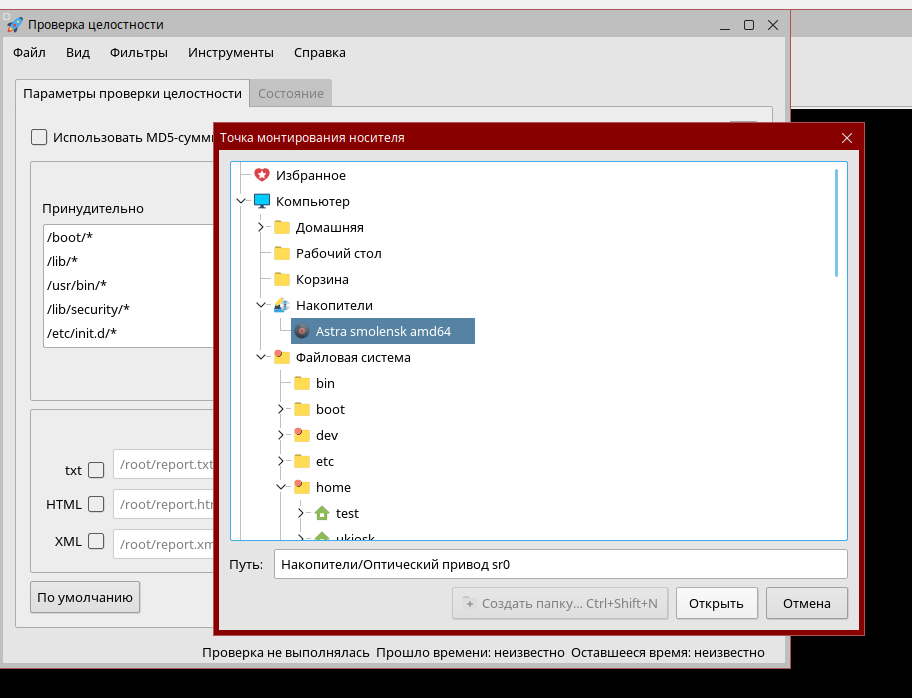
**12.** Запустить графическую утилиту fly-admin-int-check и во вкладке

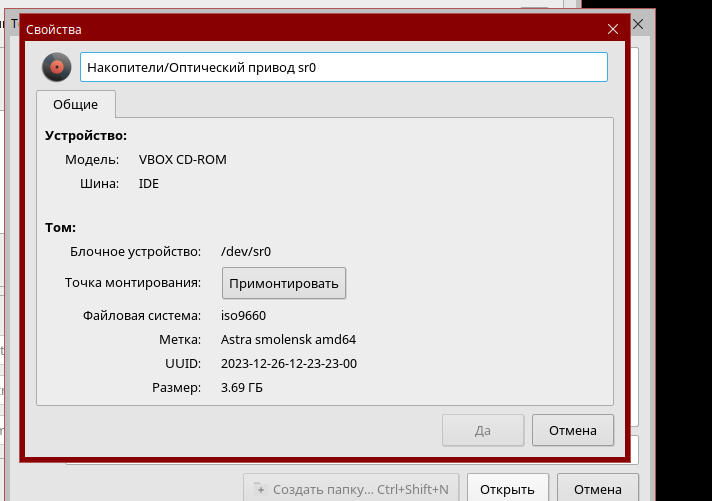
«Параметры проверки целостности»:

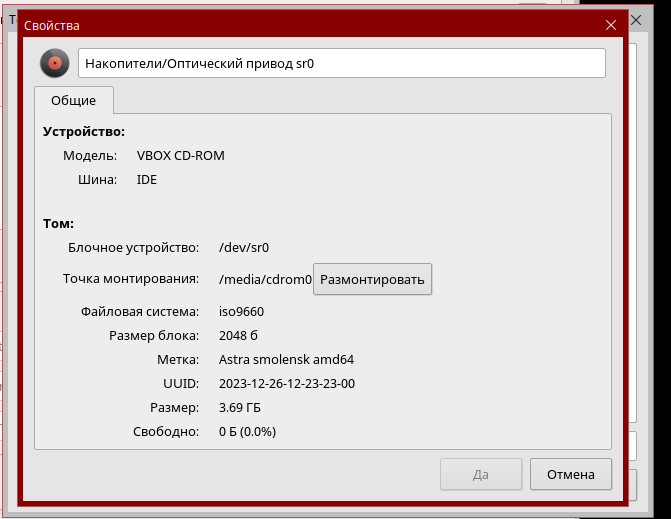
- выбрать точку монтирования устройства «Astra Smolensk amd64» (поад

умолчанию это, чаще всего, каталоги /media/cdrom или /media/cdrom0) и

выполнить монтирование;







- настроить фильтр проверки целостности в разделе «Принудительно», добавив

регулярное выражение, содержащее абсолютный путь ко всем файлам каталога

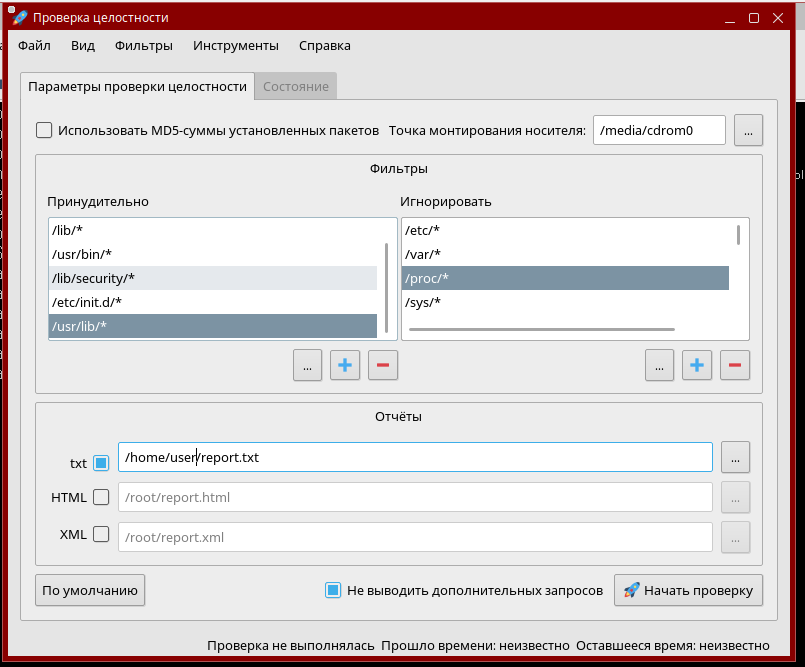
**/usr/lib**: /usr/lib/\*;

- настроить фильтр проверки целостности в разделе «Игнорировать», удалив

регулярное выражение, содержащее абсолютный путь к каталогу /tmp;

- в разделе « Отчёты» задать только текстовый формат файла отчёта, определив

путь размещения файла report.txt в каталоге /home/user/report;



- изменить содержимое файла /usr/share/doc/libcap2/copyright

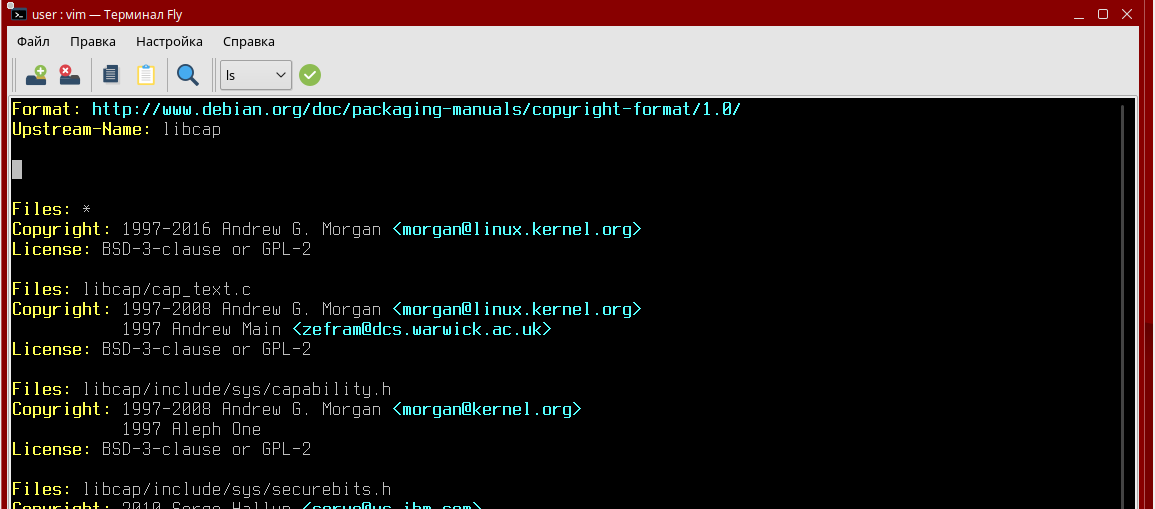
командой vim /usr/share/doc/libcap2/copyright, удалив в нем две

первые строки:

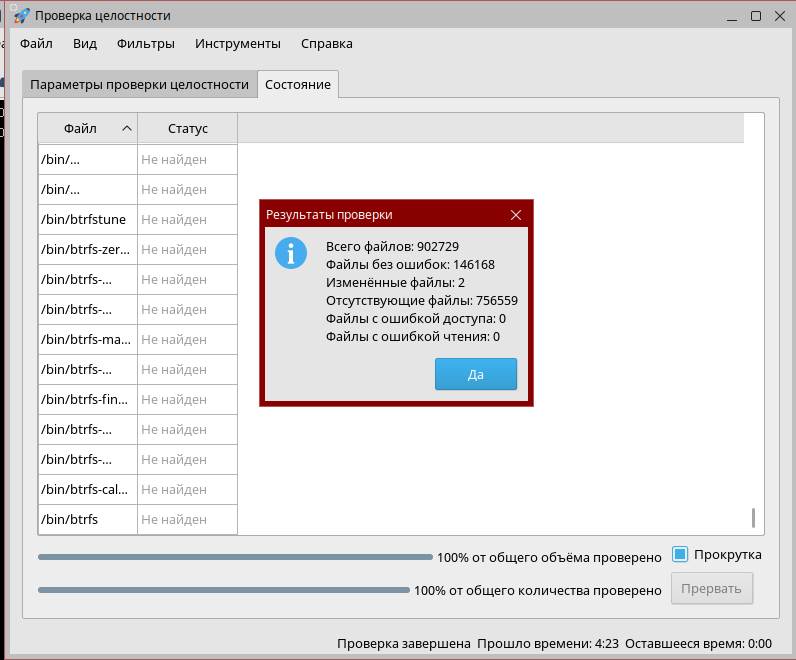
Upstream-Contact: Andrew G. Horgan morgan@kernel. org

Source: https://www.kernel.org/pub/linux/libs/security/linuxprivs/

libcap2/:d2



- начать проверку и зафиксировать предполагаемое время проверки, перейти во вкладку «Состояние» и проконтролировать статус проверки, после окончания проверки завершить работу графической утилиты;



- в файле /home/user/report/report.txt найти строки, содержащие текст: «Файлы, целостность которых нарушена», «Контр. сумма» и «/usr/share/doc/libcap2/copyright», сохранить результаты поиска в файл /home/user/report-2 цепочкой команд:

grep 'Файлы, целостность которых нарушена' /home/user/report/report.txt -A 4 > /home/user/report-2;

grep 'Контр. сумма' /home/user/report/report.txt -A 4 >> /home/user/report-2;

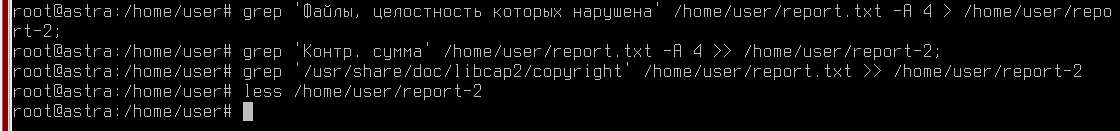
grep '/usr/share/doc/libcap2/copyright' /home/user/report/report.txt >> /home/user/report-2

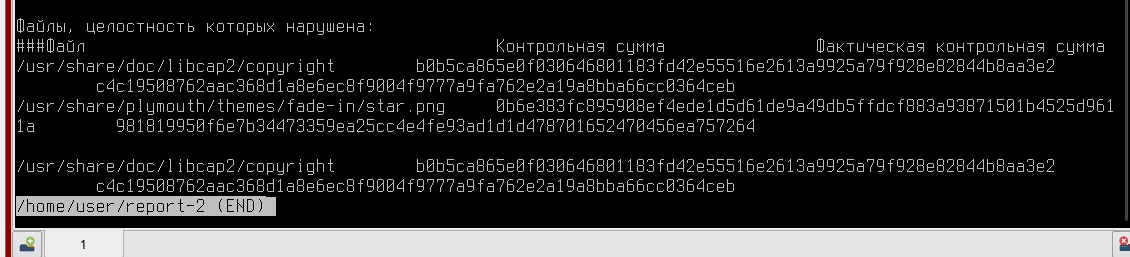
й

grep 'Файлы, целостность которых нарушена' /home/user/report.txt -A 4 > /home/user/report-2;

grep 'Контр. сумма' /home/user/report.txt -A 4 >> /home/user/report-2;

grep '/usr/share/doc/libcap2/copyright' /home/user/report.txt >> /home/user/report-2



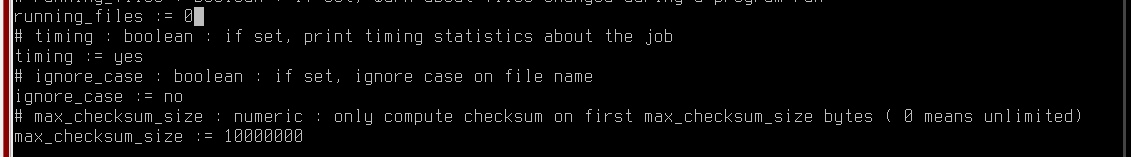


**13.** Отредактировать секцию directives конфигурационного файла /etc/afick.conf системы AFICK, отменив проверку выполняющихся приложений: исходный вариант секции:

directives: running\_files: = yes,

отредактированный вариант секции:

directives: running\_files: = 0.



**14.** Отредактировать секцию alias конфигурационного файла

/etc/afick.conf системы AFICK:

изменить правило ЕТС, удалив из него проверку размера файловых сущностей и добавив проверку времени их модификации:

**исходный вариант правила:**

ETC = р+d+i+u+g+s+md5,

**отредактированный вариант правила:**

ЕТС = р+d+i+u+m+c+a+md5;

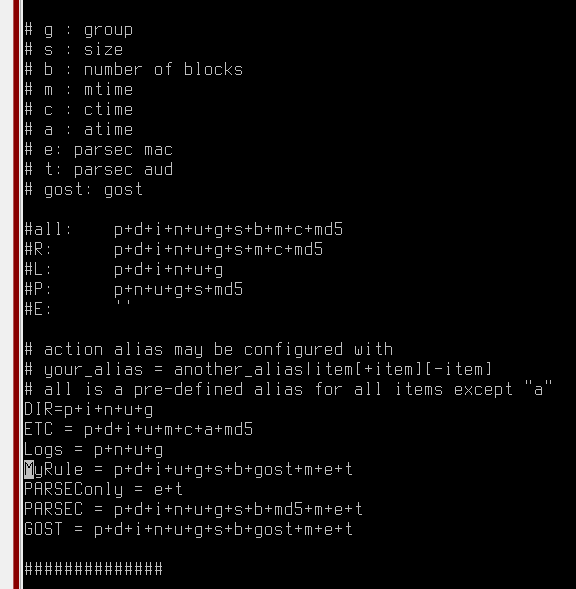
отредактировать правило MyRule, удалив из него проверку для файловых сущностей количества ссылок на них и добавив проверку контроля целостности мандатных меток безопасности, контроля целостности данных системы аудита безопасности и контроля целостности с использованием криптографического алгоритма ГОСТ Р 34. 11-2012 вместо алгоритма MD5:

**исходный вариант правила:**

MyRule = p+d+i+n+u+g+s+b+md5+m,

**отредактированный вариант правила:**

MyRule = p+d+i+u+g+s+b+gost+m+е+t



**15.** Отредактировать секцию file section конфигурационного файла

/etc/afick.conf.

заменить для каталога /boot правило проверки GOST на правило

проверки PARSEC:

**исходный вариант:**

/boot GOST,

**отредактированный вариант:**

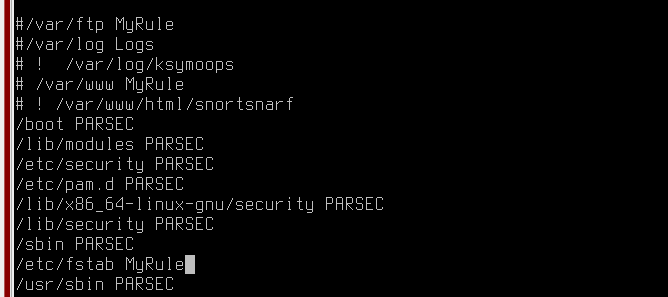
/boot PARSEC

добавить для файловой сущности /etc/fstab правило проверки

MyRule:

**отредактированный вариант:**

/etc/fstab MyRule,



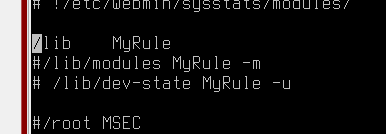
активировать правило проверки по умолчанию для каталога /lib:

**исходный вариант:**

#/lib MyRule,

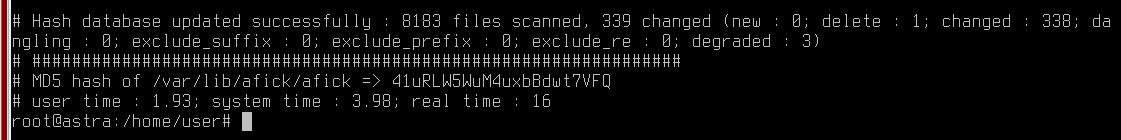
**отредактированный вариант:**

/lib MyRule.



**16.** Обновить базу данных системы AFICK с учётом выполненных изменений в

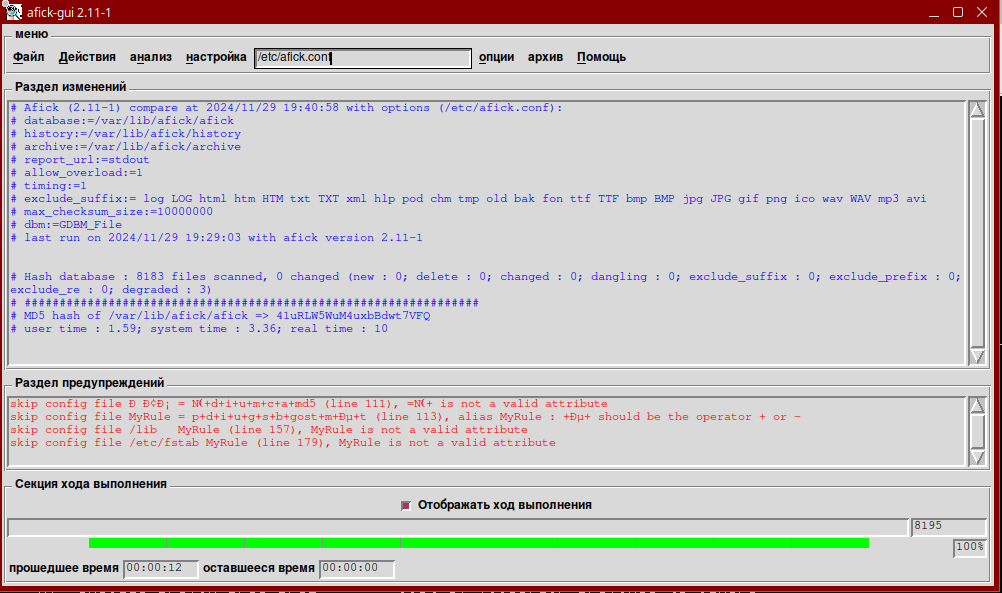
секции file section командой afick -u.



**17.** Изменить содержимое файла /etc/fstab, удалив в нем две первые строки.

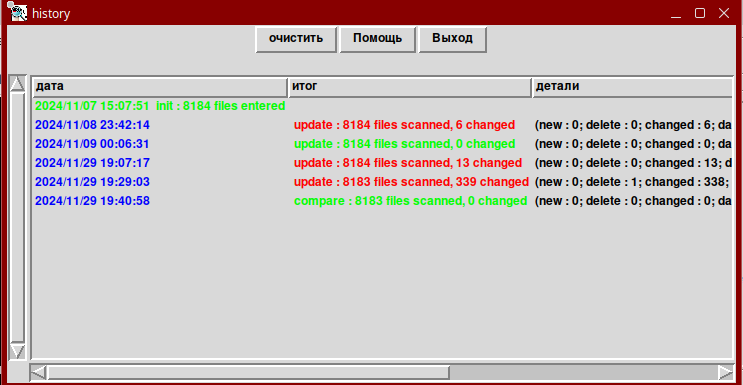


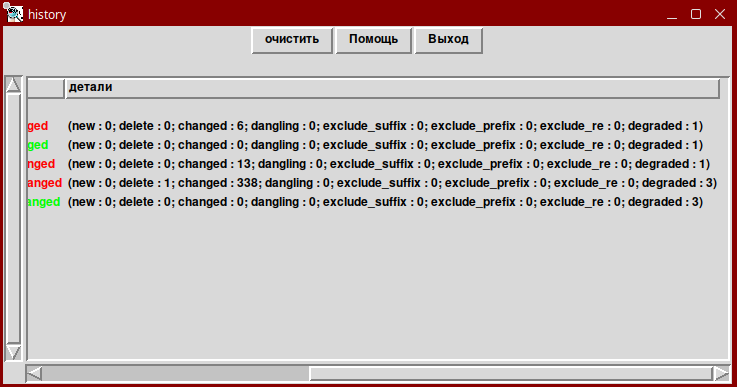
**18.** Запустить графическую утилиту «Контроль целостности файлов» (afick-tk) управления AFICK из меню «Системные» главного пользовательского меню и выполнить принудительную проверку целостности, выбрав действие — сравнение с базой.



**19.** После завершения контроля целостности:

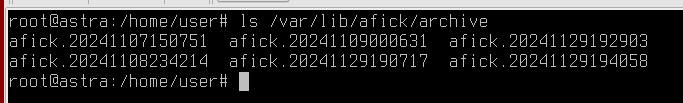
в меню утилиты afick-tk «Файл — история» определить дату и время последнего принудительного контроля целостности;



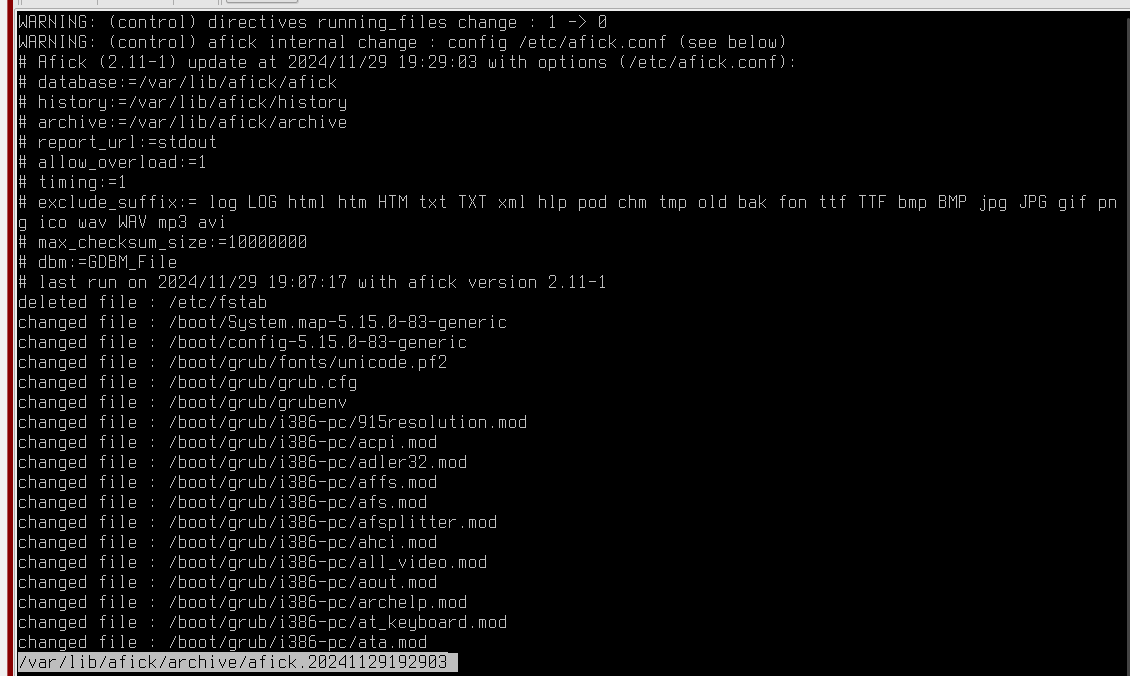


найти в каталоге /var/lib/afick/archive log-файл,

соответствующий выполненной принудительной проверке (значение YYYYMMDDHHMMSS в имени log-файла должно совпадать с найденными в предыдущем пункте датой и временем проверки);



просмотреть найденный log-файл с помощью команды less и в его секции #detaled changes найти запись о нарушении целостности файловой сущности /etc/fstab (раздел changed file:/etc/fstab);



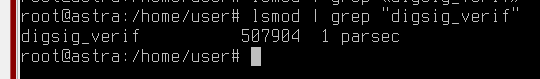
проанализировать найденную запись о нарушении целостности и определить параметры, соответствующие действиям (action) нарушения целостности, и их текущие значения.

**20.** Запустить терминал Fly в «привилегированном» режиме командой sudo flyterm.



**21.** Просмотреть загруженные модули ядра ОССН и вывести в терминал данные

о невыгружаемом модуле digsig\_verif конвейером команд lsmod | grep «digsig\_verif».



Вывод покажет:

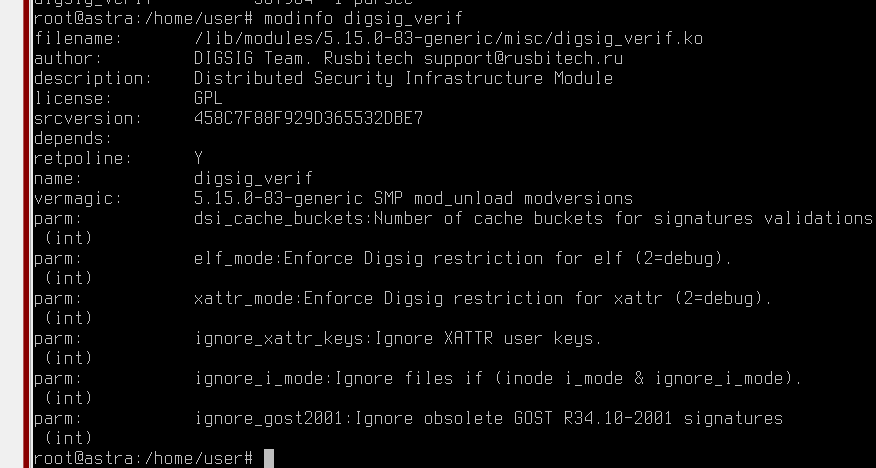
* Имя модуля.
* Используемую память.
* Количество других модулей, которые зависят от него.

Просмотреть информацию о модуле digsig\_verif командой

modinfo digsig\_verif

Определить расположение модуля digsig\_verif и

информацию о разработчике.

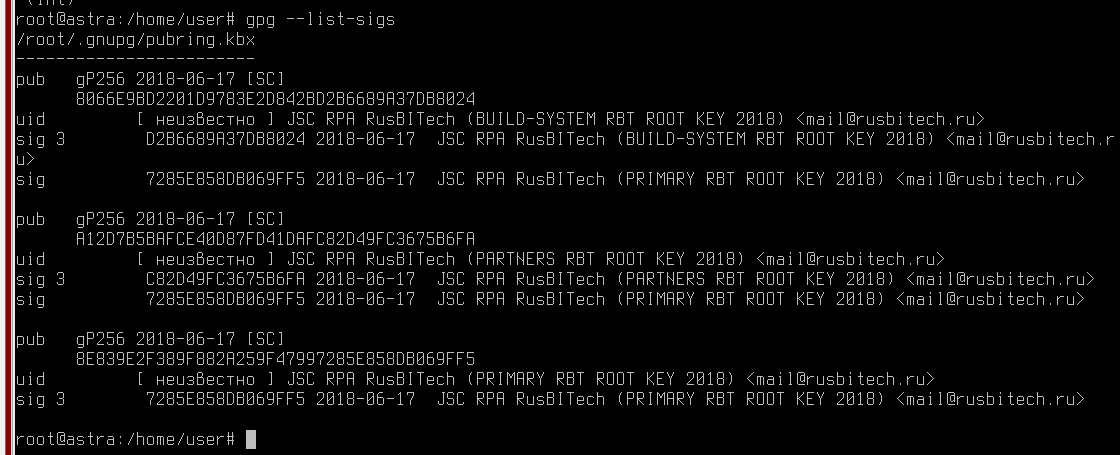


Выполнить импорт открытых ключей, используемых для проверки ЭП файлов.

Для этого выполнить следующие действия:

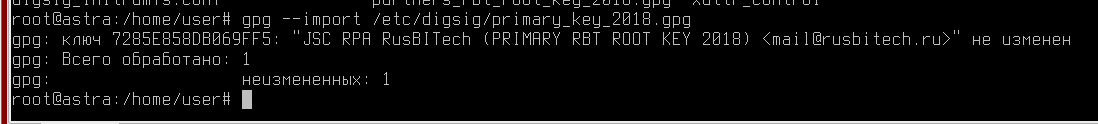
инициализировать каталог /root/.gnupg при просмотре текущих

ключей командой gpg --list-sigs;



импортировать открытый мастер-ключ «JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018)» командой

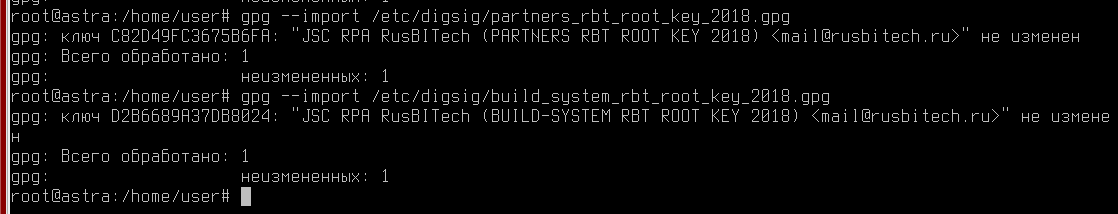
gpg --import /etc/digsig/primary\_key\_2018.gpg



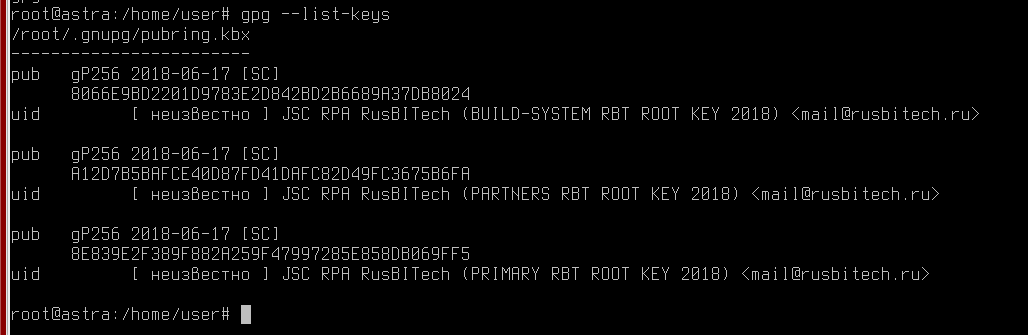
импортировать открытые ключи partners\_rbt\_root\_key\_2018.gpg

и build\_system\_rbt\_root\_key\_2018.gpg (данный ключи используется для подписи файлов ОССН), командой gpg --import /etc/digsig/partners\_rbt\_root\_key\_2018.gpg

gpg --import /etc/digsig/build\_system\_rbt\_root\_key\_2018.gpg



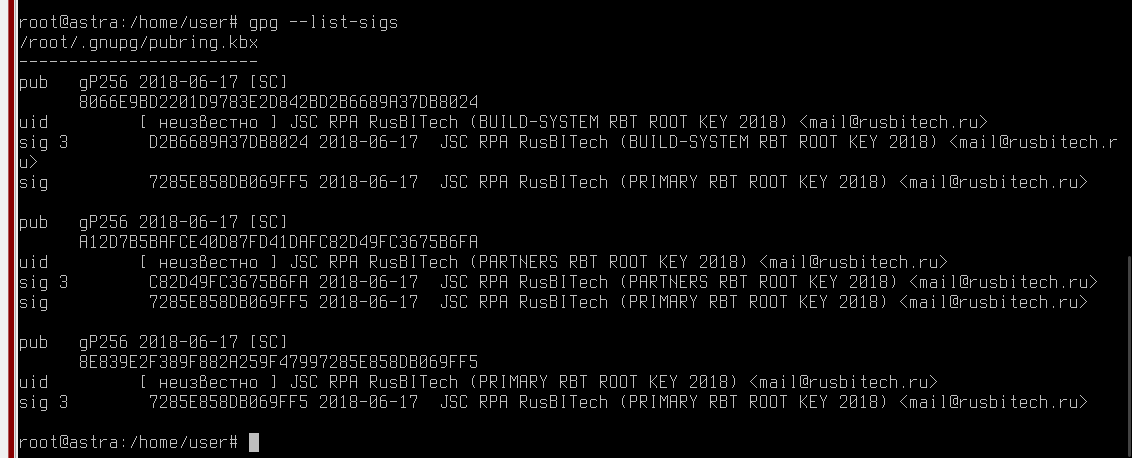
Вывести перечень используемых ключей командой gpg --list-keys



Вывести текущие ключи командой gpg --list-sigs. Определить

идентификатор мастер-ключа «JSC RPA RusBITech (PRIMARY RBT ROOT KEY

2018)». Используется ли он для подписи других загруженных ранее ключей?



Она отображает список ключей в локальном хранилище, включая их подписи. В выводе вы увидите:

* Основную информацию о ключах (например, идентификатор ключа, владельца, email).
* Список подписей, которые были сделаны этим ключом для других ключей.

сам себя и потом других.

Проверить корректность ЭП файла /bin/dash командой bsign -w$(which dash). Определить, каким ключом был подписан данный файл по его

идентификатору в строке «signer: ».

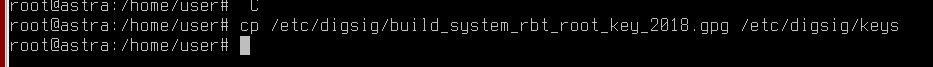


JSC RPA RusBITech (BUILD-SYSTEM RBT ROOT KEY 2018) <mail@rusbitech.ru>

Переписать открытый ключ /etc/digsig/build\_system\_rbt-rootkey\_

2018.gpg в каталог /etc/digsig/keys командой

cp /etc/digsig/build\_system\_rbt\_root\_key\_2018.gpg /etc/digsig/keys



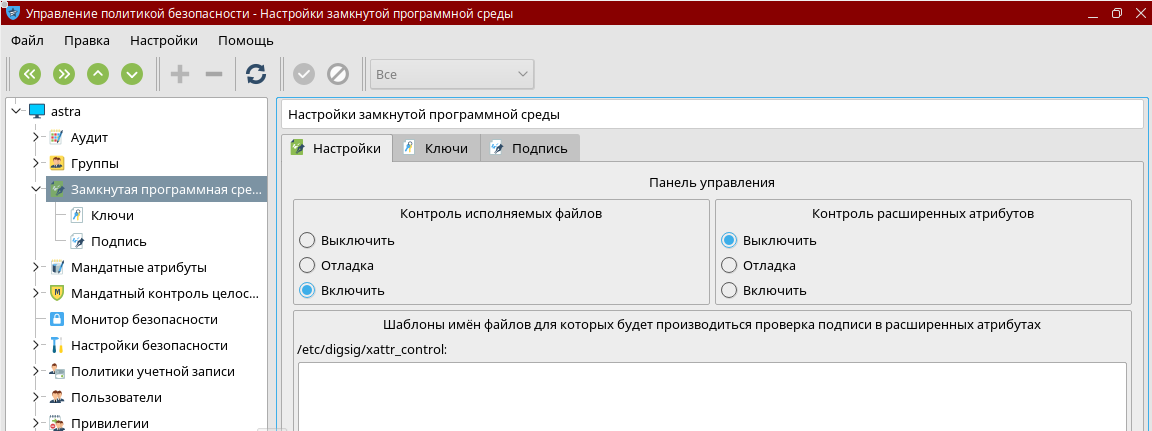
Перейти в каталог /etc/digsig и изменить файл

digsig\_initramfs.conf (значение DIGSIG\_ELF\_MODE установить равным 1).

nano /etc/digsig/digsig\_initramfs.conf



Проверить корректность установки данного параметра путём открытия настройки «Замкнутой программной среды» в «Панели управления».



Создать дополнительный ключ ЭП команд.

В диалоге команды gpg:

выбрать пункт 15 «GOST R 34. 10-2012»;

указать длину ключа – 1024;

указать неограниченный срок действия дополнительного ключа ЭП, выбр

значение 0

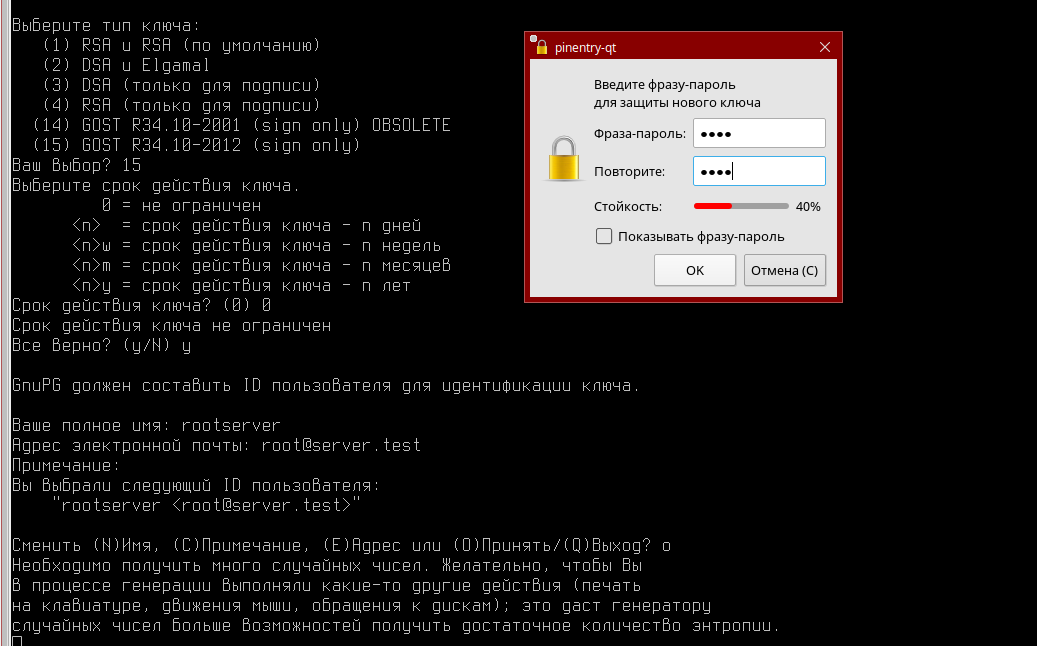
указать параметры:

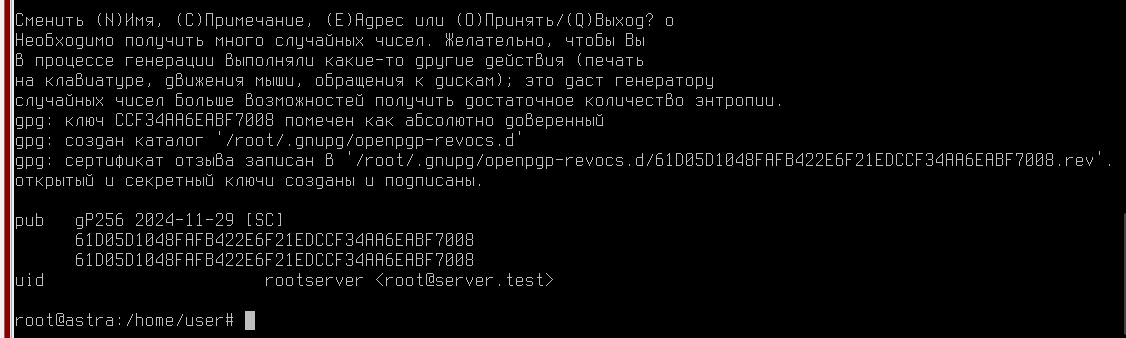
указать полное имя: rootserver, адрес электронной почты:

root@server.test и получить User ID: "rootserver root@server.test”.

Вывести текущие ключи командой gpg --list-sigs и определить

идентификатор ключа "rootserver [root@server.test](mailto:root@server.test)”.





Скопировать файл /bin/dash в каталог /root, указав при этом новое имя

файла 1.elf.

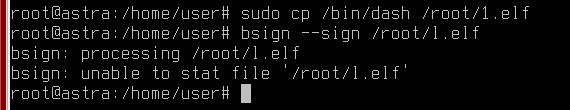
sudo cp /bin/dash /root/1.elf

Подписать файл l.elf новым ключом «rootserver

<root@server.test>» командой

gpg --default-key CCF34AA6EABF7008

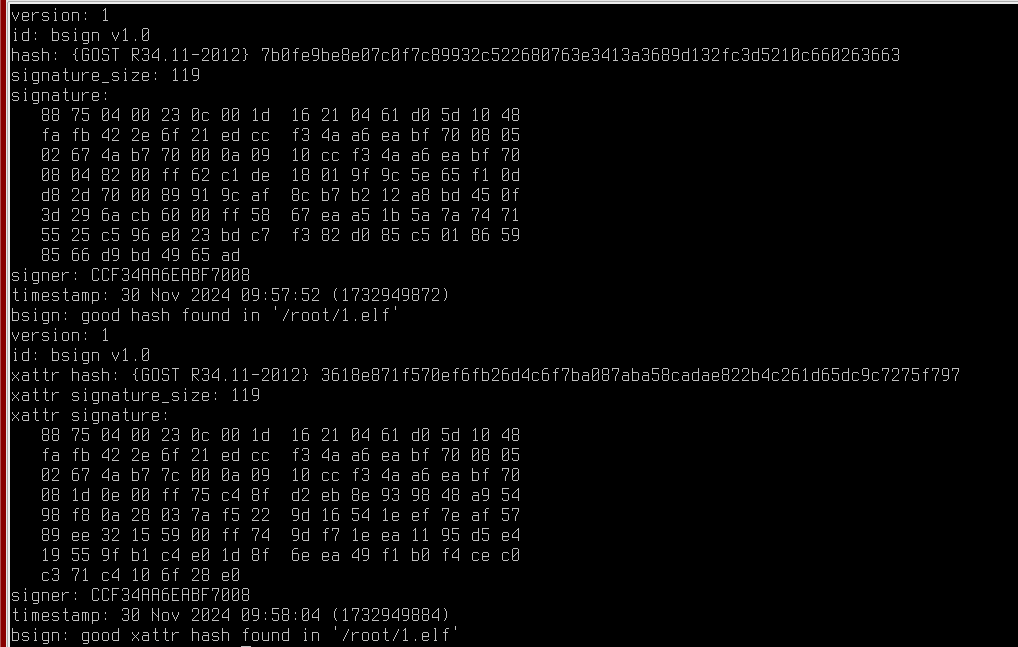
bsign --sign /root/l.elf



Вывести новую подпись файла командой bsign -w /root/1.elf и

проверить соответствие идентификатора ключа ЭП в строке «signer. » данным

ключа «rootserver <root@server.test>».



файл был подписан дважды: один раз в теле файла (в основной подписи) и второй раз в атрибутах файла (xattr).

В дополнение к обычной подписи файла, утилита bsign также может добавлять подпись в расширенные атрибуты (xattr) самого файла. Это позволяет подписывать не только сам файл, но и его метаданные, такие как права доступа, дата изменения и другие параметры.

1. **Обычная подпись**: Первая подпись, которая отображается как signature, — это основная подпись файла, которая создаётся на основе его содержимого.
2. **Подпись в расширенных атрибутах (xattr)**: Вторая подпись — это подпись, которая добавляется к расширенным атрибутам файла (xattr). Эта подпись используется для проверки целостности файла в его метаданных, в том числе защиты информации о том, как файл был подписан.

Включить штатный режим проверки ЭП с использованием модуля

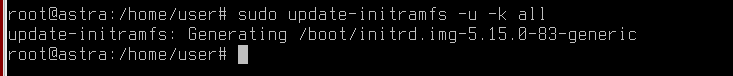
digsig\_verif, установив значение ключа DIGSIG\_ELF\_MODE = 1 в

конфигурационном файле /etc/digsig/digsig\_initramfs.conf.

Активировать настройки командой

sudo update-initramfs -u -k all

, затем выполнить перезагрузку и повторный вход в ОССН.



Запустить терминал Fly в «привилегированном» режиме командой sudo

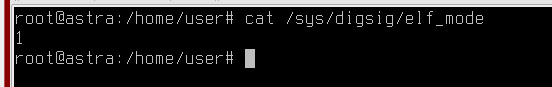
fly-term.

Проверить включение штатного режим функционирования модуля

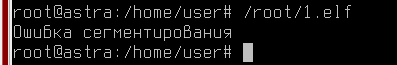
digsig\_verif (в файле /sys/digsig/elf\_mode должно быть установлено

значение «1») командой

cat /sys/digsig/elf\_mode



Выполнить попытку запуска файла /root/1.elf, который был подписан с использованием ключа «rootserver <root@кщserver. test>» (данный ключ не был подписан мастер-ключом «JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018)»), и проанализировать выводимые ошибки.



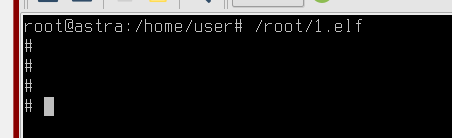
Установить значение ключа DIGSIG\_ELF\_MODE=0 в конфигурационном файле /etc/digsig/digsig\_initramfs.conf, активировать настройки командой sudo update-initramfs -u -k all,

куизатем выполнить

перезагрузку и повторный вход в ОССН

В «привилегированном» режиме терминала Fly выполнить команду

/root/1.elf и проанализировать вывод.



 Выйти из запущенного интерпретатора «dash» (файл 1.elf) командой exit.

Активировать настройки командой sudo update-initramfs -u -k all,

затем выполнить перезагрузку и повторный вход в ОССН.

 Создать ключи и выполнить подпись файла конфигурации:

 запустить терминал Fly от имени учётной записи привелигированного

пользователя командой fly-term;

- скопировать файлы /etc/passwd и /bin/dash в каталог ~ и сменить

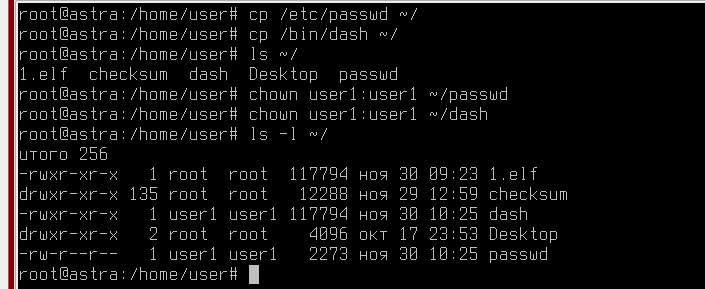
владельца на user1;

cp /etc/passwd ~/

cp /bin/dash ~/

chown user1:user1 ~/passwd

chown user1:user1 ~/dash



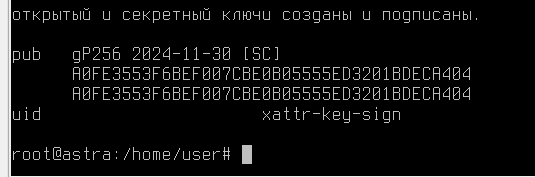
 выполнить команду генерации мастер-ключа для подписи в xattr командой

gpg --full-generate-key, выбрать алгоритм (15) и установить имя: xattr-key;



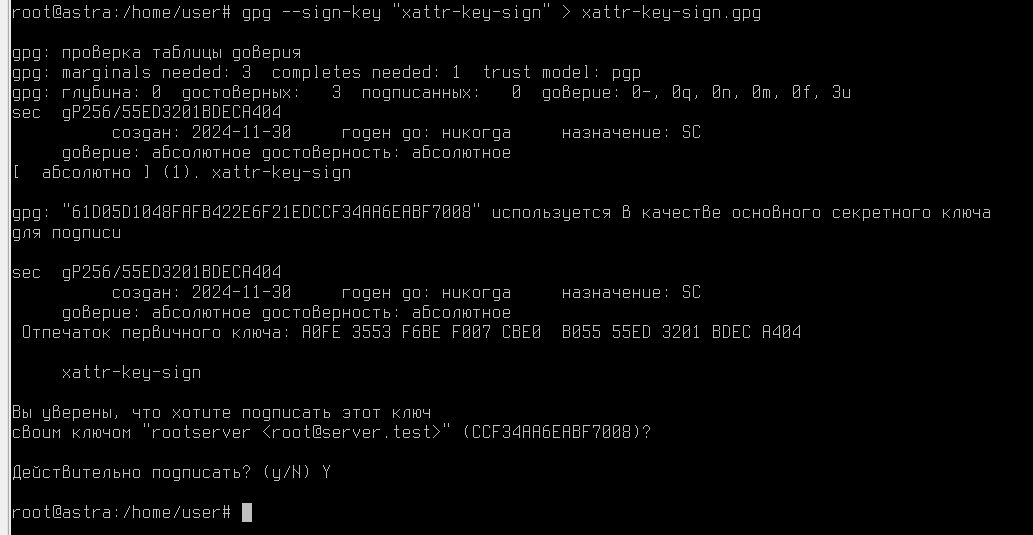
 выполнить команду генерации ключа для подписи в xattr командой gpg --

full-generate-key, выбрать алгоритм (15) и установить имя: xattr-key-sign;



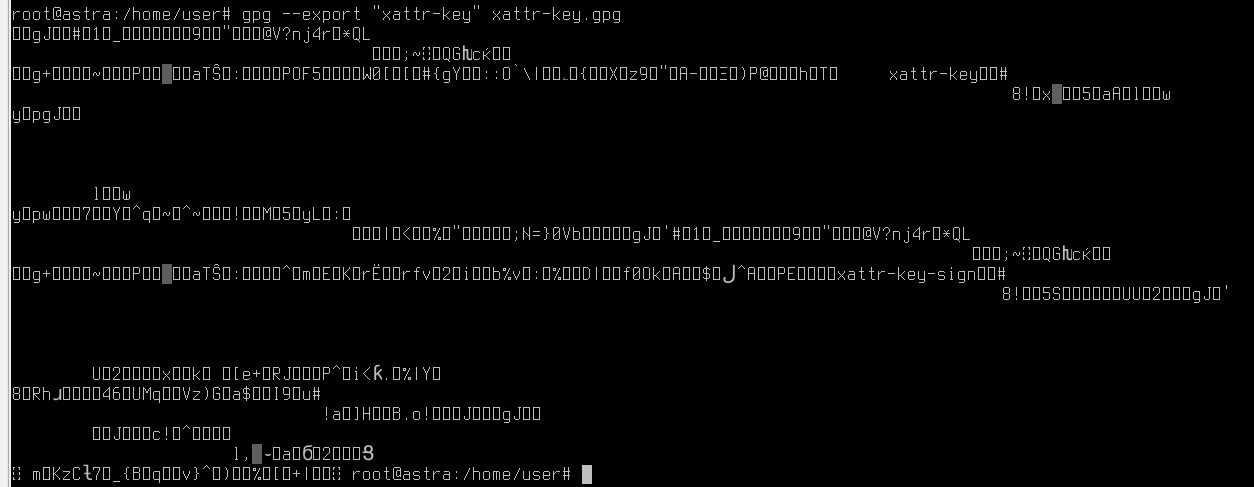
 выполнить подпись ключа «xattr-key-sign» командой

gpg --sign-key "xattr-key-sign" > xattr-key-sign.gpg



 экспортировать ключ «xattr-кеу» командой

gpg --export "xattr-key" xattr-key.gpg

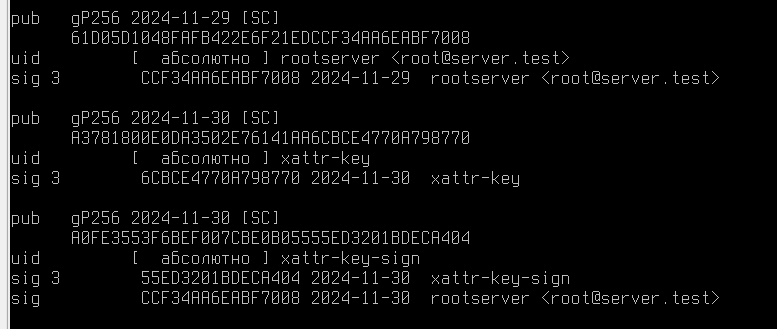
 

 проверить наличие подписанного ключа «xattr-key-sign» командой

gpg --list-sigs

(при этом ключ «xattr-key-sign» должен быть подписан

ключом «xattr-key»);



 запомнить идентификаторы ключей «xattr-кеу» и «xattr-key-sign»

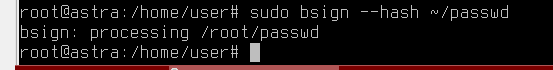
(8 байтов в шестнадцатеричном формате - 16 символов);

 создать хэш файла ~/passwd и записать его в расширенные атрибуты

командой sudo bsign --hash ~/passwd (обратить внимание, что никаких

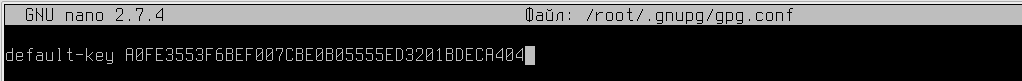
ключей разблокировки секретного ключа при этом не запрашивается у

пользователя);

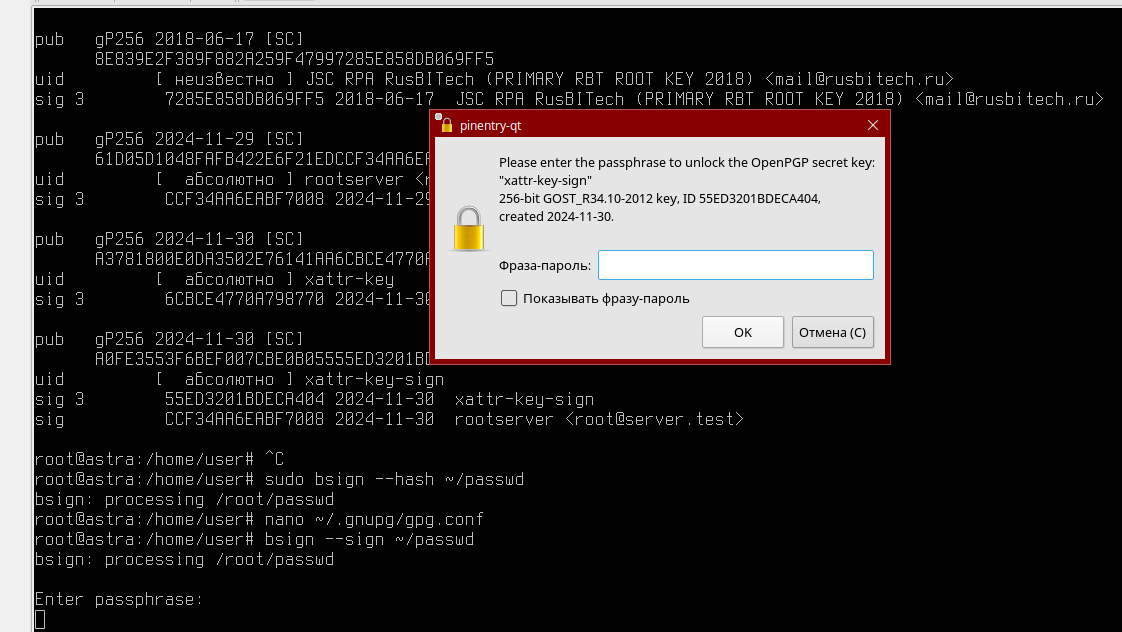


 создать файл ~/.gnupg/gpg.conf с содержимым: default-key

идентификатор\_ключа\_xattr-key-sign;

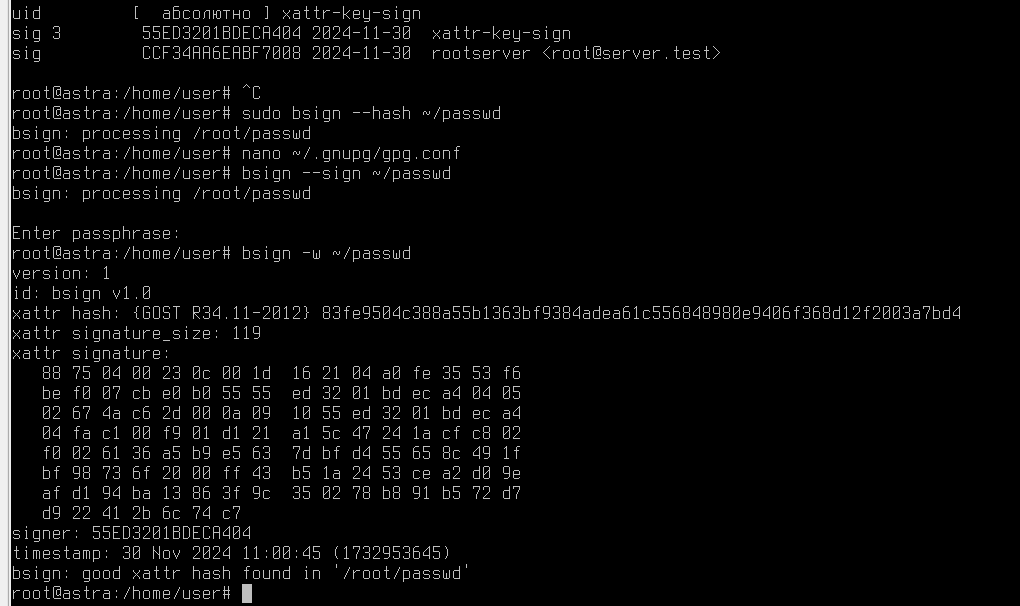


 выполнить подпись файла passwd командой bsign --sign ~/passwd;



 выполнить проверку подписи файла passwd командой bsign -w

~/passwd;



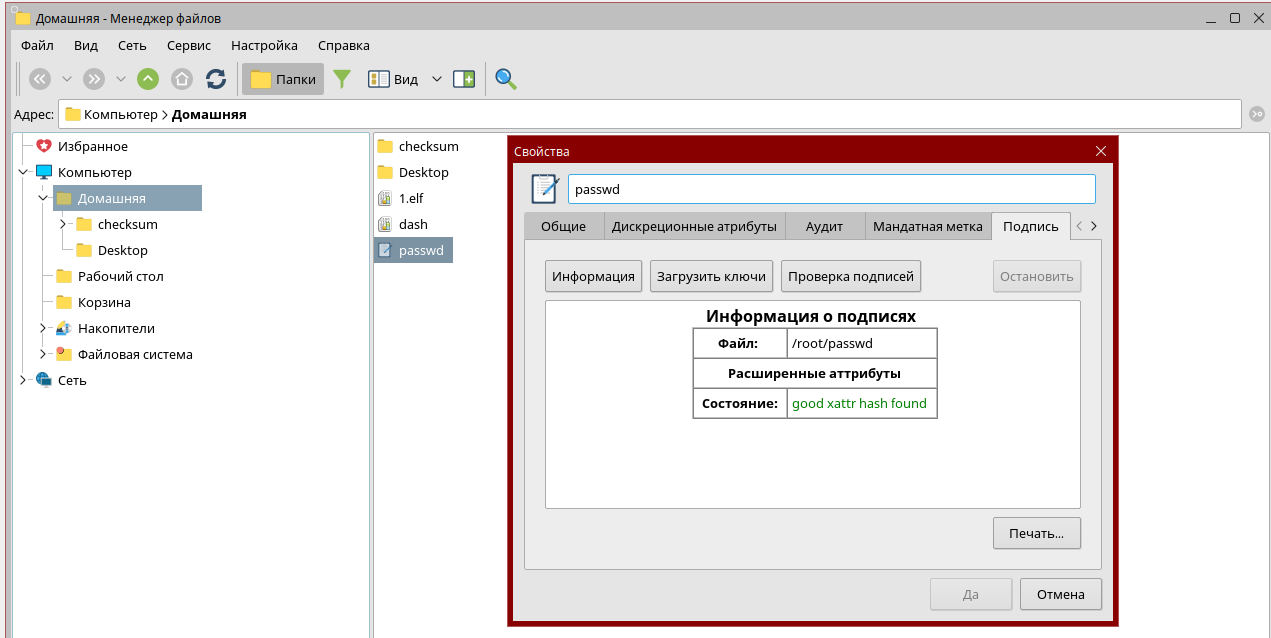
 скопировать ключи (xattr-key-sign.gpg и xattr-key.gpg) для работы

с подписями файлов в каталог /etc/digsig/xattr\_keys;



 в графическом файловом менеджере fly-fm перейти в каталог «Домашний»

и открыть в контекстном меню «Свойства», «Подпись» файла passwd;



 нажать кнопки «Загрузить ключи» и «Информация», при этом проверить

корректность созданного хэш и наличие подписи.

