Безопасность в Linux: как сделать круче, чем SELinux и Apparmor

МЫЛИЦЫН РОМАН НИКОЛАЕВИЧ,
РУКОВОДИТЕЛЬ ЦЕНТРА КОМПЕТЕНЦИИ
АО «НПО РУСБИТЕХ» В УРФО

ТЕАТР НАЧИНАЕТСЯ С ВЕШАЛКИ

А LINUX — С ЯДРА:

«HARDENED ЯДРО»

ОГРАНИЧЕНИЯ ПО РАБОТЕ С ПАМЯТЬЮ

– запрет записи в область памяти, помеченную как исполняемая;

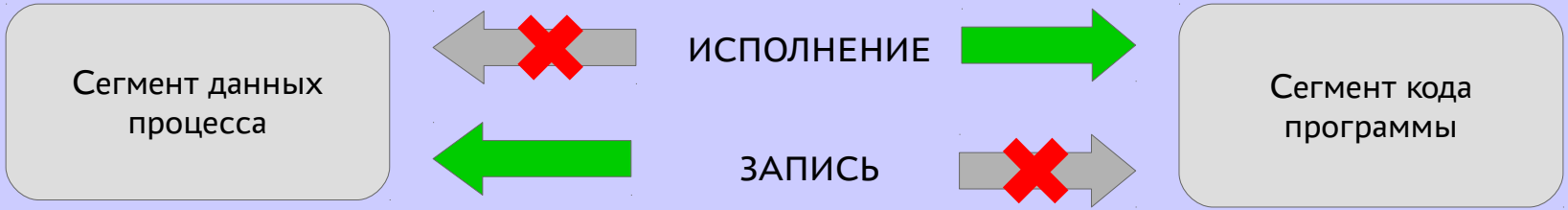
– запрет создания исполняемых областей памяти;

– запрет перемещения сегмента кода;

– запрет создания исполняемого стека;

– случайное распределение адресного пространства процесса;

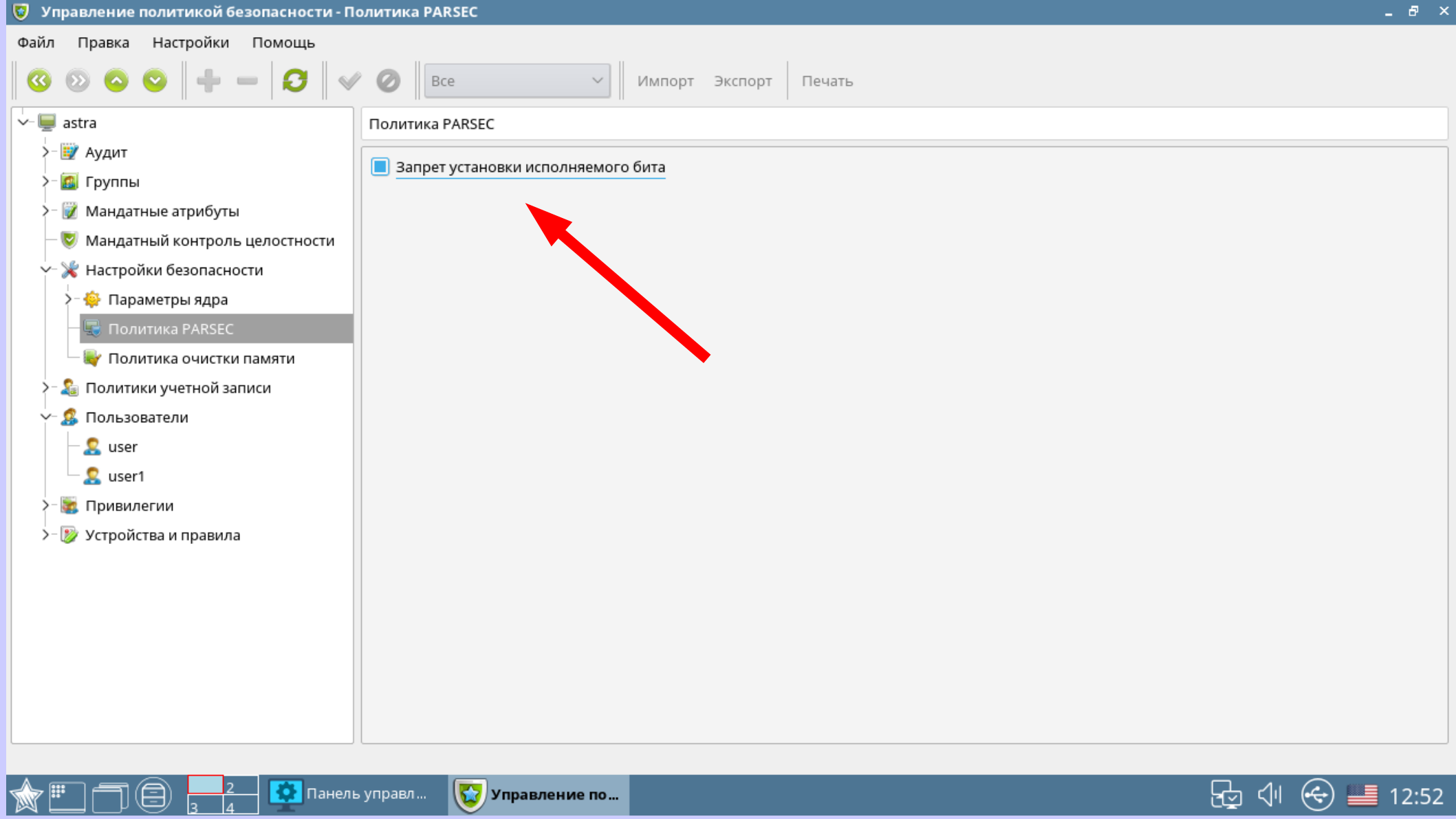
– очистка остаточной информации из стека ядра после системных вызовов.



ПАТЧ ЯДРА PAX

Использование аппаратной реализации в процессоре неисполняемого бита (NX-бит) для предотвращения выполнения произвольного кода.

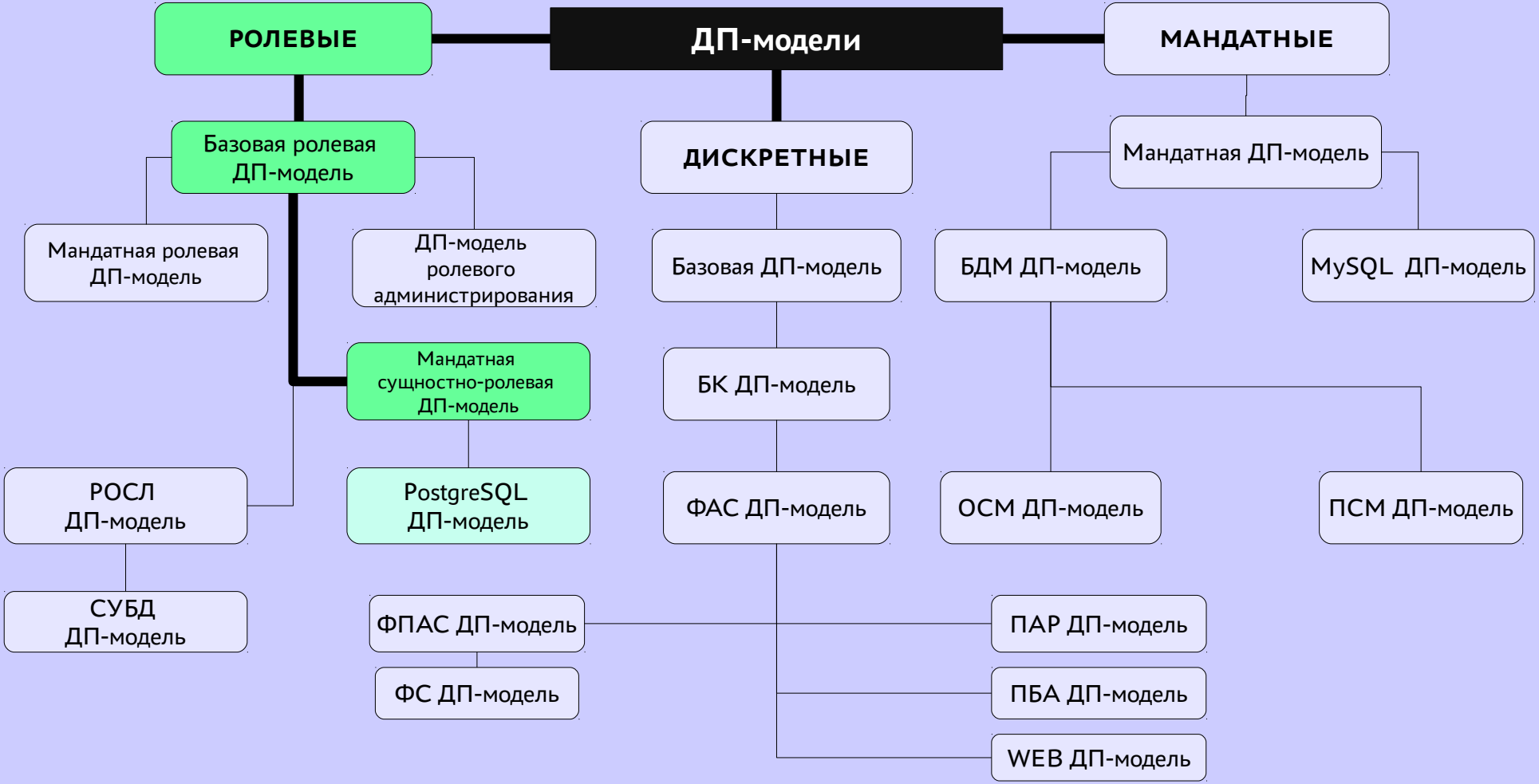
Создание новых исполняемых файлов в системе после включения этой опции невозможно.


Управление политикой безопасности - Политика PARSEC
Файл
Правка
Настройки
Помощь
Все
Импорт
Экспорт
Печать
astra
Аудит
Группы
Мандатные атрибуты
Мандатный контроль целостности
Настройки безопасности
Параметры ядра
Политика PARSEC
Политика очистки памяти
Политики учетной записи
Пользователи
user
user1
Привилегии
Устройства и правила
Политика PARSEC
Запрет установки исполняемого бита
Панель управл...
Управление по...
12:52

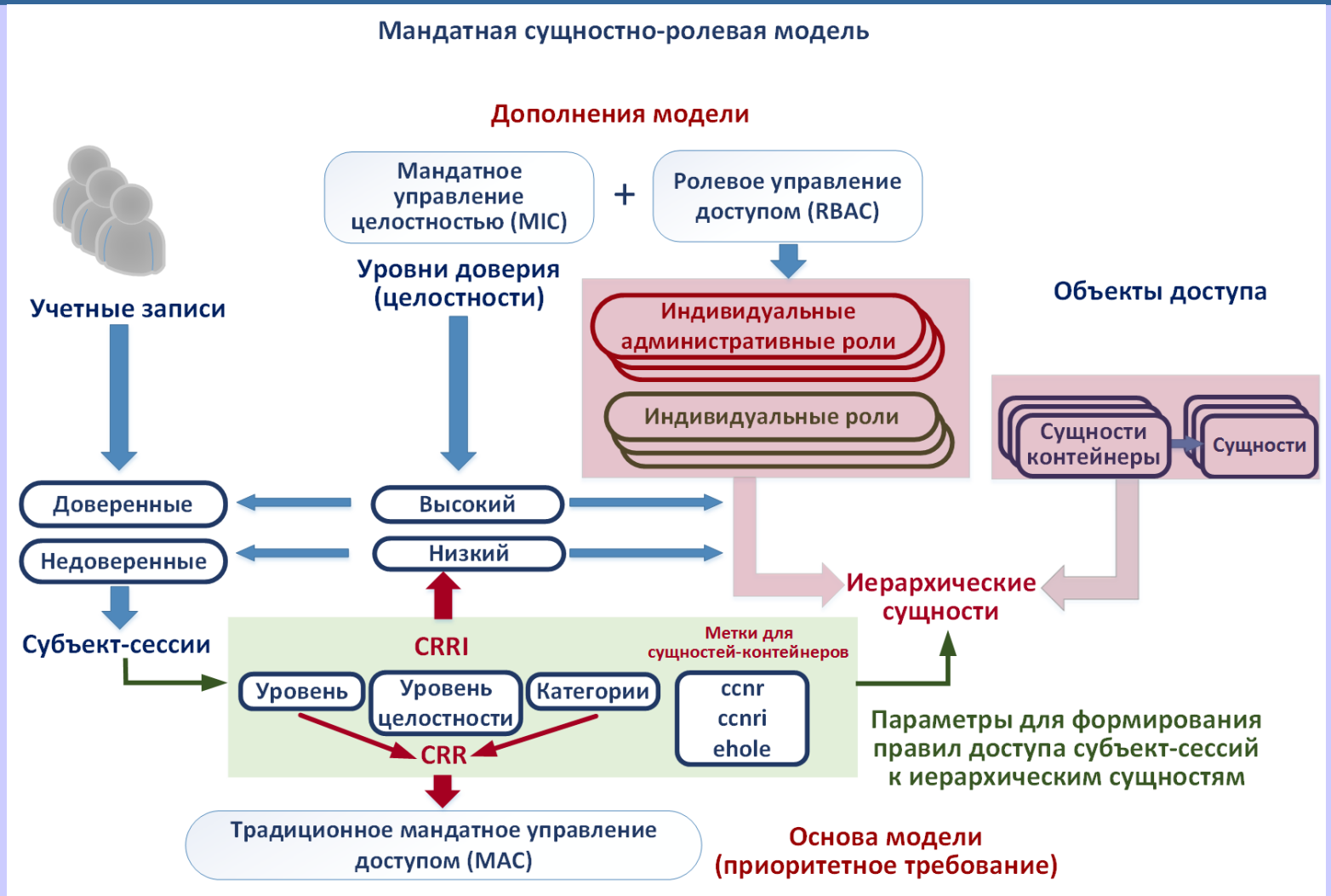
МРОСЛ ДП МОДЕЛЬ

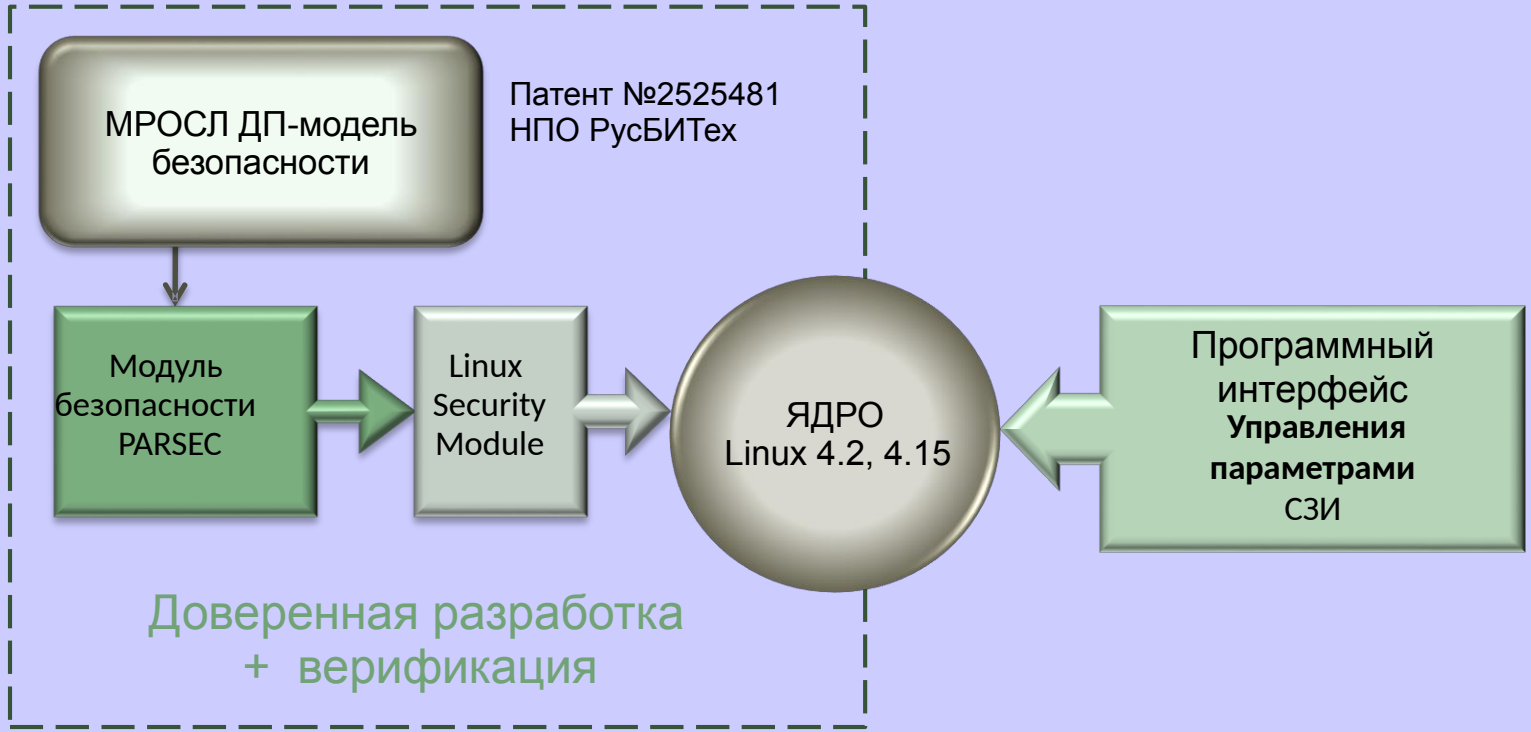
РАЗГРАНИЧЕНИЕ ДОСТУПА И ПОТОКОВ

МРОСЛ-ДП МОДЕЛЬ

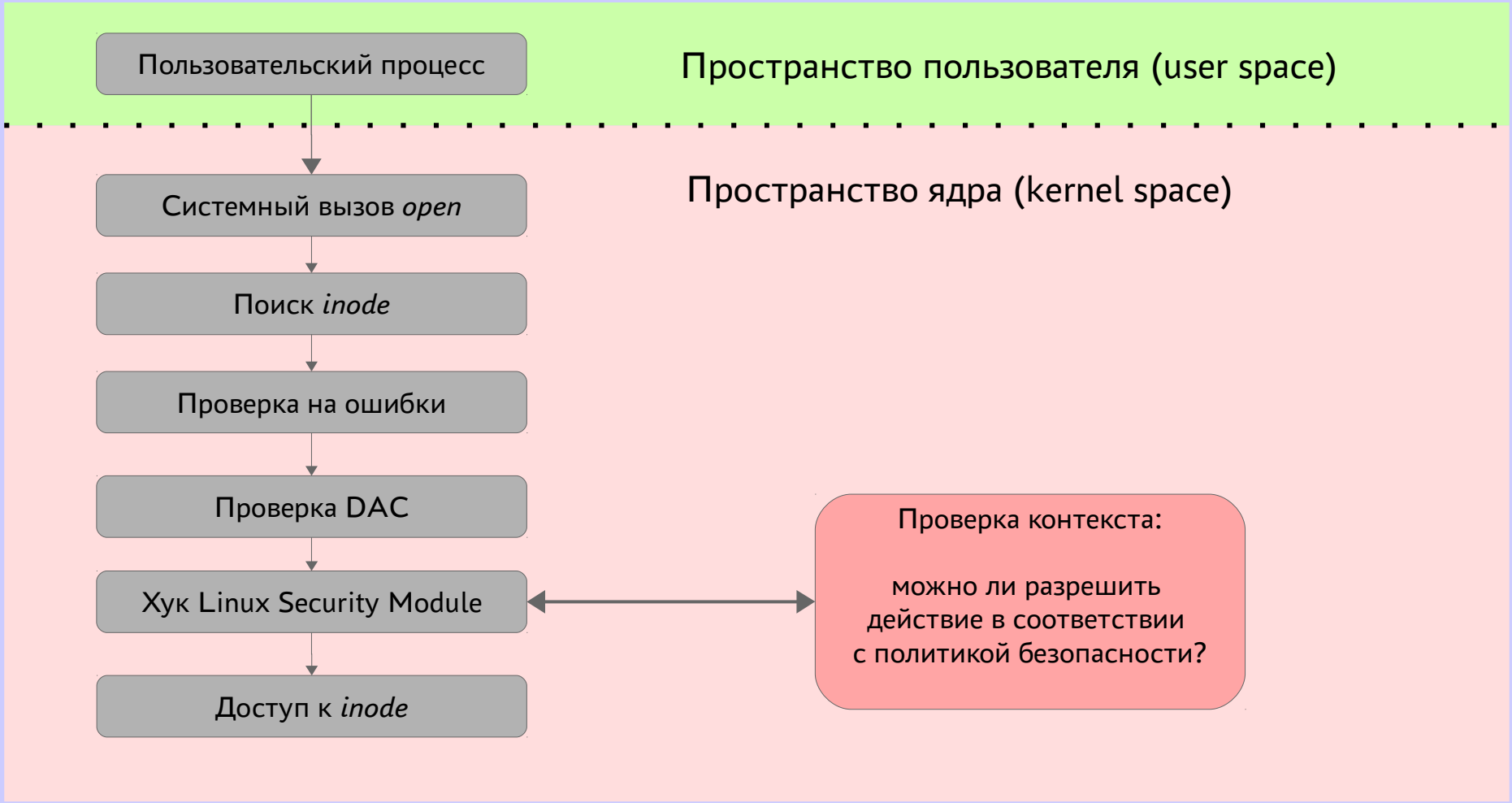


МРОСЛ ДП-МОДЕЛЬ



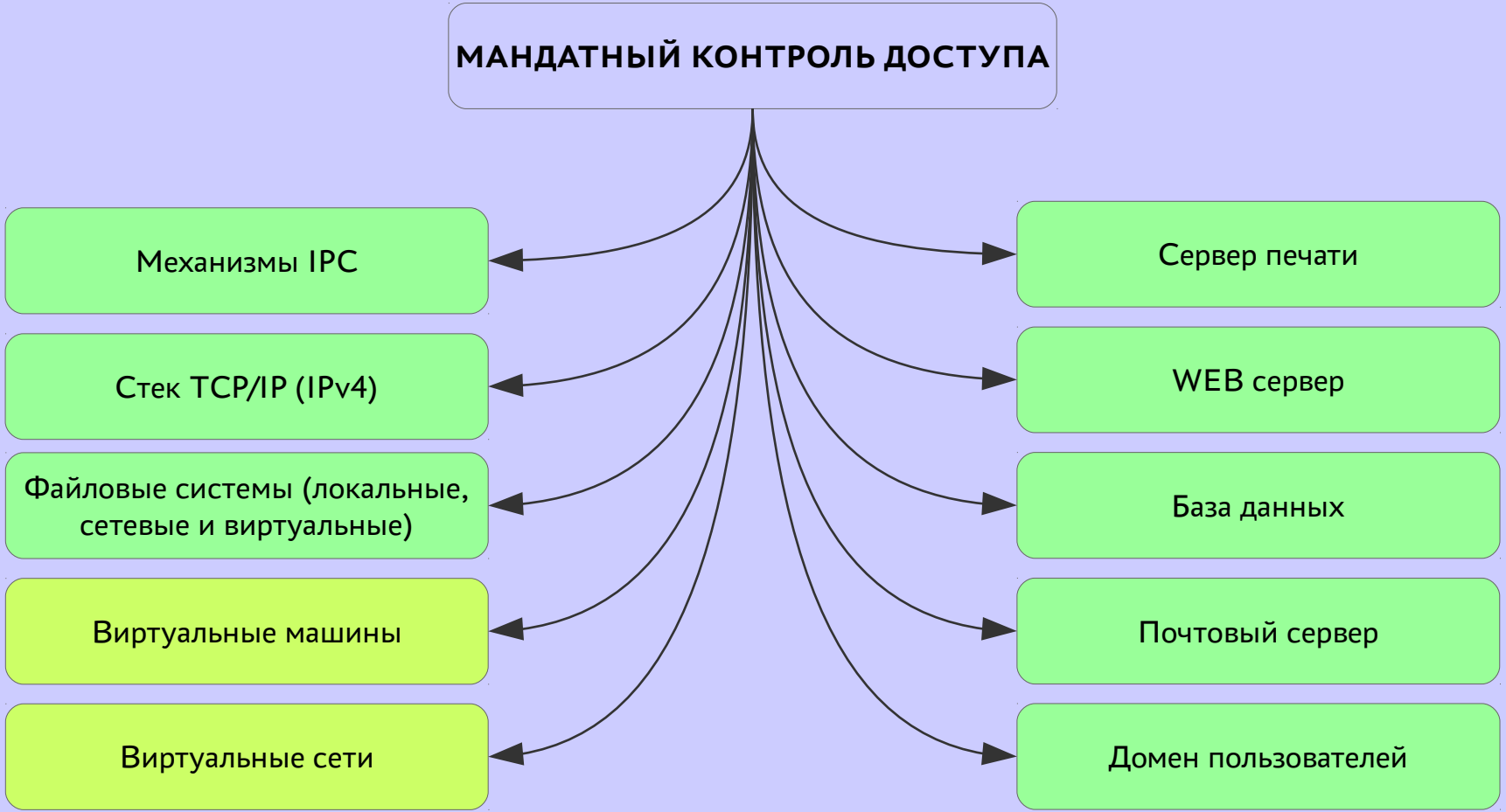


Научное сопровождение работ:
Институт системного программирования РАН и Академия ФСБ России


Пользовательский процесс
Пространство пользователя (user space)
Системный вызов *open*
Пространство ядра (kernel space)
Поиск *inode*
Проверка на ошибки
Проверка DAC
Хук Linux Security Module
Доступ к *inode*
Проверка контекста:
можно ли разрешить
действие в соответствии
с политикой безопасности?

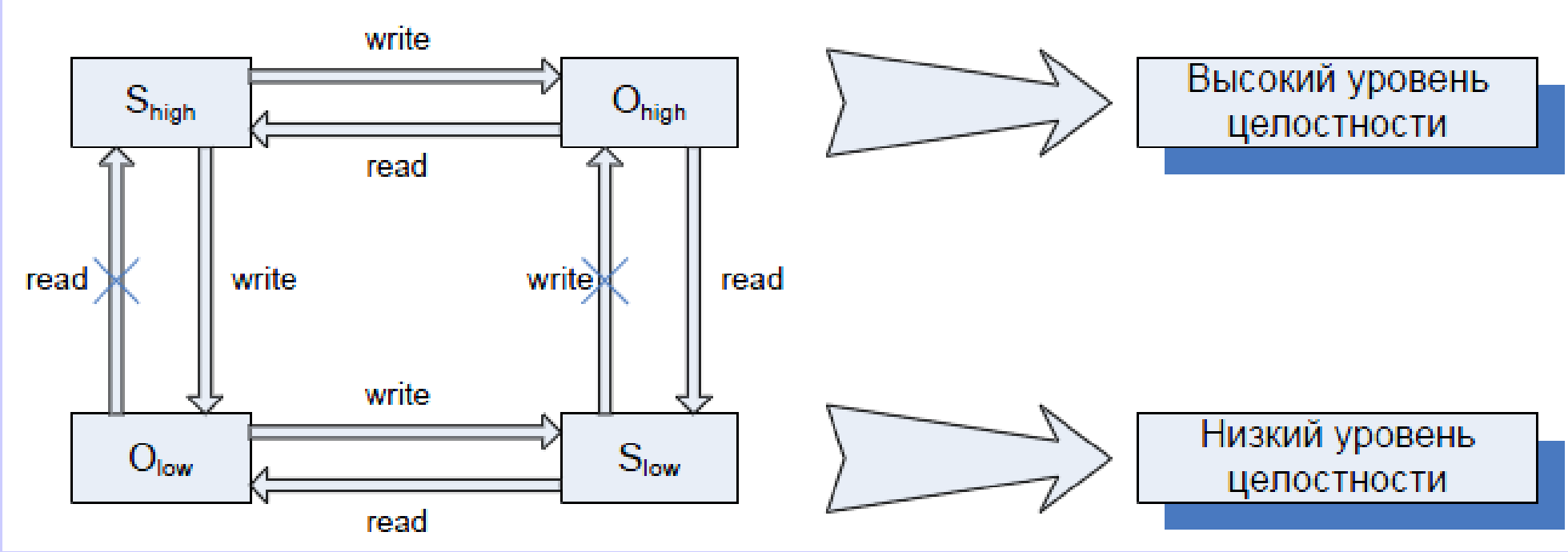
КОНТРОЛЬ ДОСТУПА

МАНДАТНЫЙ КОНТРОЛЬ ДОСТУПА



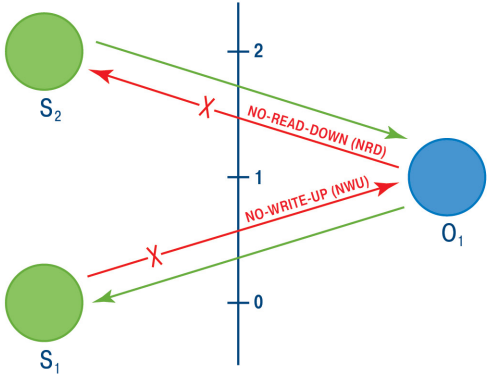
КОНТРОЛЬ ЦЕЛОСТНОСТИ

МЕХАНИЗМ ИЗОЛЯЦИИ ПРОЦЕССОВ СОГЛАСНО РАЗГРАНИЧЕНИЮ ПО НЕЗАВИСИМЫМ УРОВНЯМ ЦЕЛОСТНОСТИ (ДОВЕРИЯ).

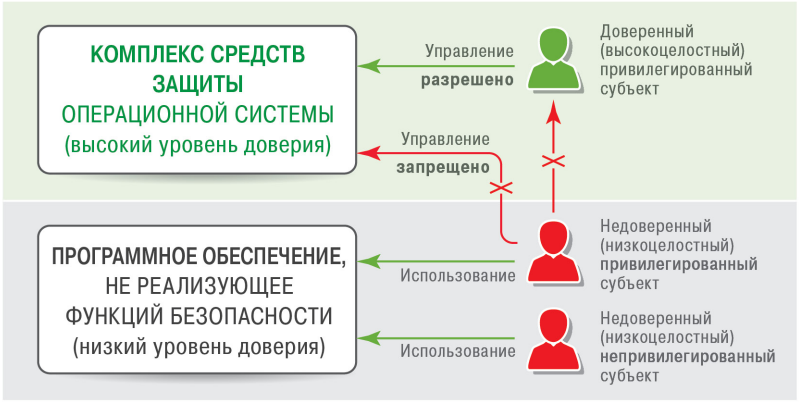


МАНДАТНЫЙ КОНТРОЛЬ ЦЕЛОСТНОСТИ

ТЕОРЕМА БИБА (**МКЦ**)

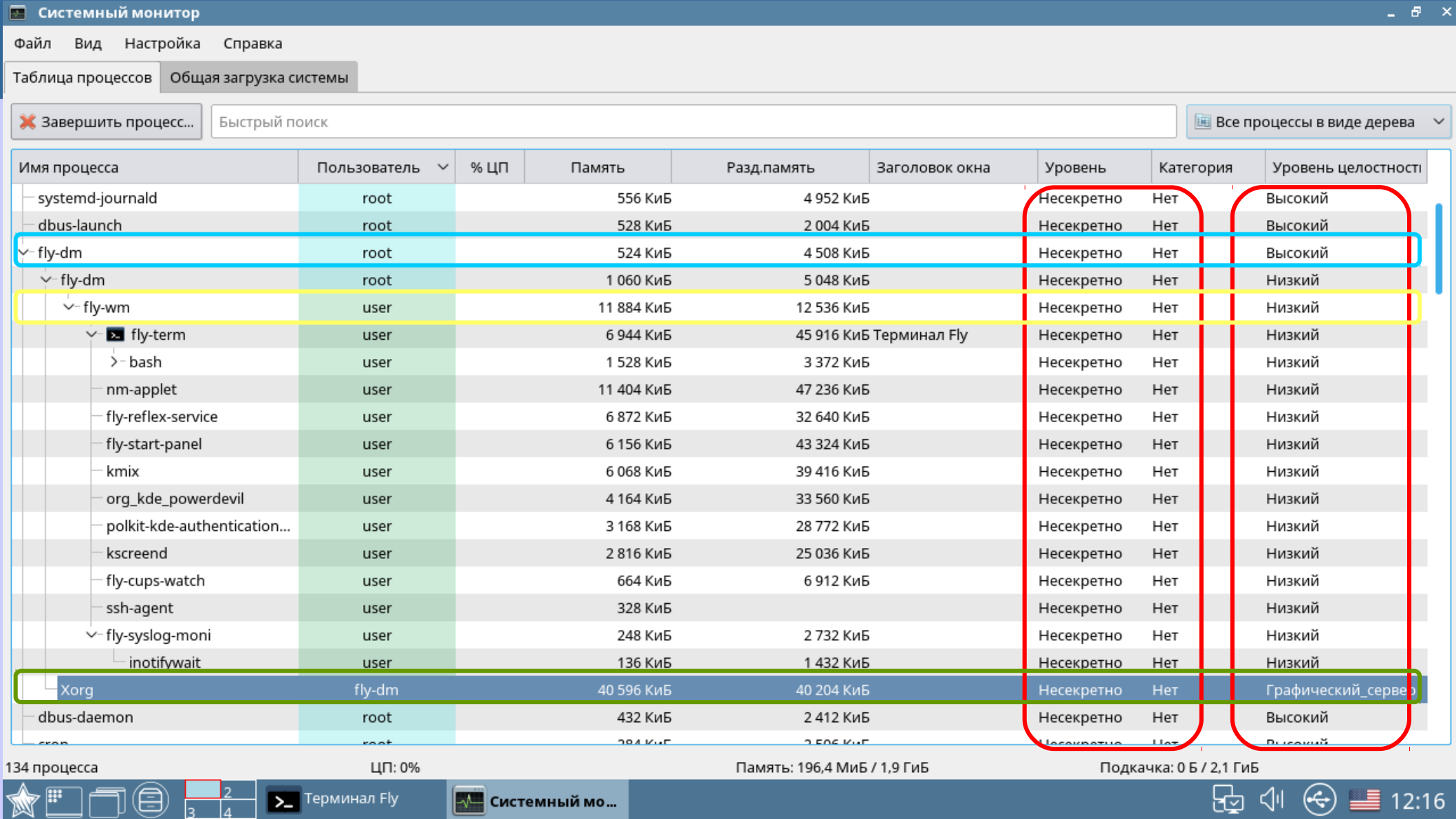


ОБЕСПЕЧЕНИЕ ДОВЕРИЯ К КОМПЛЕКСУ СРЕДСТВ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ **МКЦ**



РОЛЬ И МЕСТО **МКЦ** В ВЕКТОРЕ АТАКИ

- обнаружение уязвимости «нулевого дня»
- повышение привилегий (получение прав привилегированного субъекта)
- управление КСЗ: изменение параметров КСЗ, нарушение целостности ПО КСЗ
- **Контроль над системой защиты информации**


Системный монитор
Файл
Вид
Настройка
Справка
Таблица процессов
Общая загрузка системы
Завершить процесс...
Быстрый поиск
Все процессы в виде дерева
Имя процесса
Пользователь
% ЦП
Память
Разд.память
Заголовок окна
Уровень
Категория
Уровень целостности
systemd-journald root 556 КиБ 4 952 КиБ Несекретно Нет Высокий
dbus-launch root 528 КиБ 2 004 КиБ Несекретно Нет Высокий
fly-dm root 524 КиБ 4 508 КиБ Несекретно Нет Высокий
fly-dm root 1 060 КиБ 5 048 КиБ Несекретно Нет Низкий
fly-wm user 11 884 КиБ 12 536 КиБ Несекретно Нет Низкий
fly-term user 6 944 КиБ 45 916 КиБ Терминал Fly Несекретно Нет Низкий
bash user 1 528 КиБ 3 372 КиБ Несекретно Нет Низкий
nm-applet user 11 404 КиБ 47 236 КиБ Несекретно Нет Низкий
fly-reflex-service user 6 872 КиБ 32 640 КиБ Несекретно Нет Низкий
fly-start-panel user 6 156 КиБ 43 324 КиБ Несекретно Нет Низкий
kmix user 6 068 КиБ 39 416 КиБ Несекретно Нет Низкий
org_kde_powerdevil user 4 164 КиБ 33 560 КиБ Несекретно Нет Низкий
polkit-kde-authentication... user 3 168 КиБ 28 772 КиБ Несекретно Нет Низкий
kscreend user 2 816 КиБ 25 036 КиБ Несекретно Нет Низкий
fly-cups-watch user 664 КиБ 6 912 КиБ Несекретно Нет Низкий
ssh-agent user 328 КиБ Несекретно Нет Низкий
fly-syslog-moni user 248 КиБ 2 732 КиБ Несекретно Нет Низкий
inotifywait user 136 КиБ 1 432 КиБ Несекретно Нет Низкий
Xorg fly-dm 40 596 КиБ 40 204 КиБ Несекретно Нет Графический_серве
dbus-daemon root 432 КиБ 2 412 КиБ Несекретно Нет Высокий
134 процесса
ЦП: 0%
Память: 196,4 МиБ / 1,9 ГиБ
Подкачка: 0 Б / 2,1 ГиБ
Терминал Fly
Системный мо...
12:16

МЕХАНИЗМ ДИНАМИЧЕСКОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ (**ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА**).

ПОДДЕРЖКА **ГОСТ Р 34.11-2012**

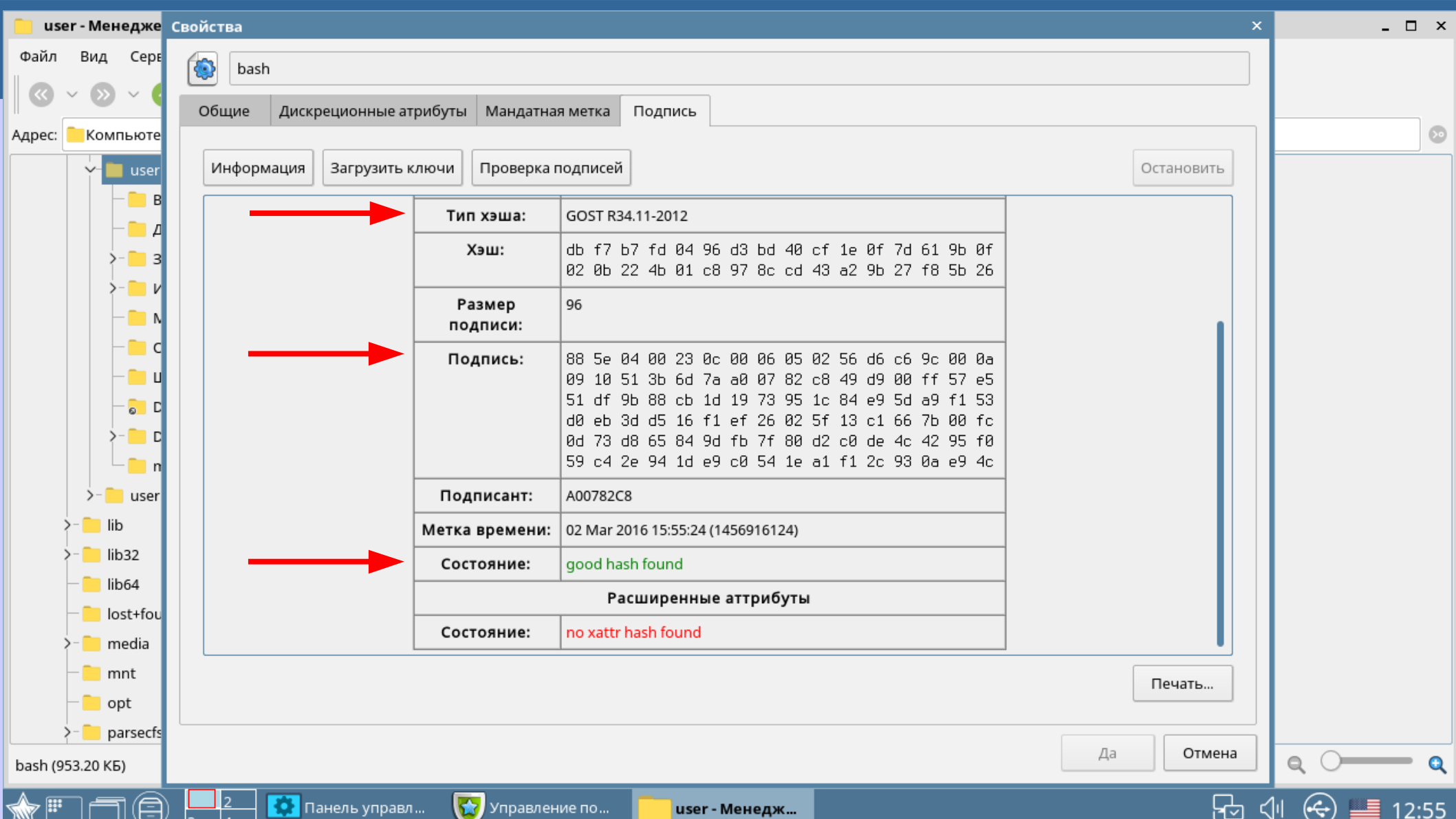
«ФУНКЦИЯ ХЭШИРОВАНИЯ»

ПОДДЕРЖКА **ГОСТ Р 34.10-2012**

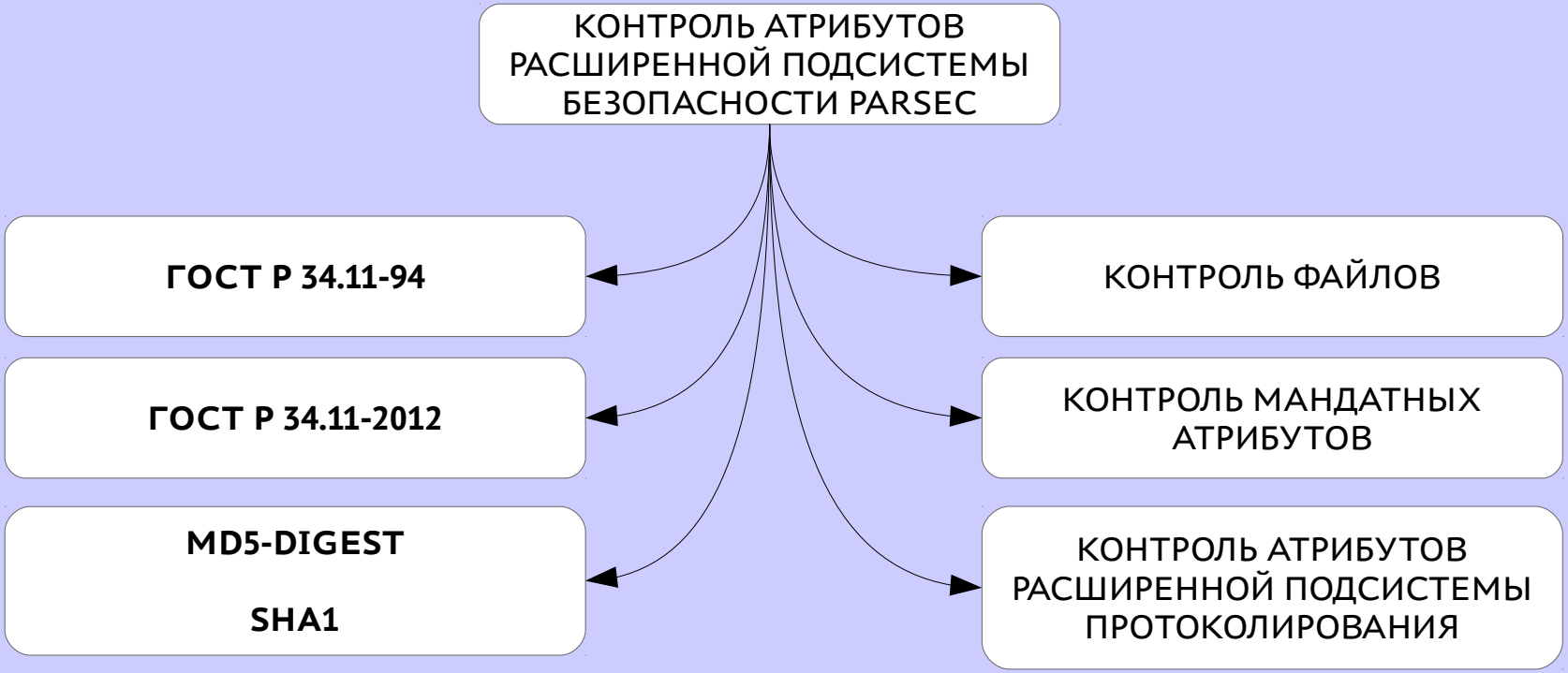
«ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ»

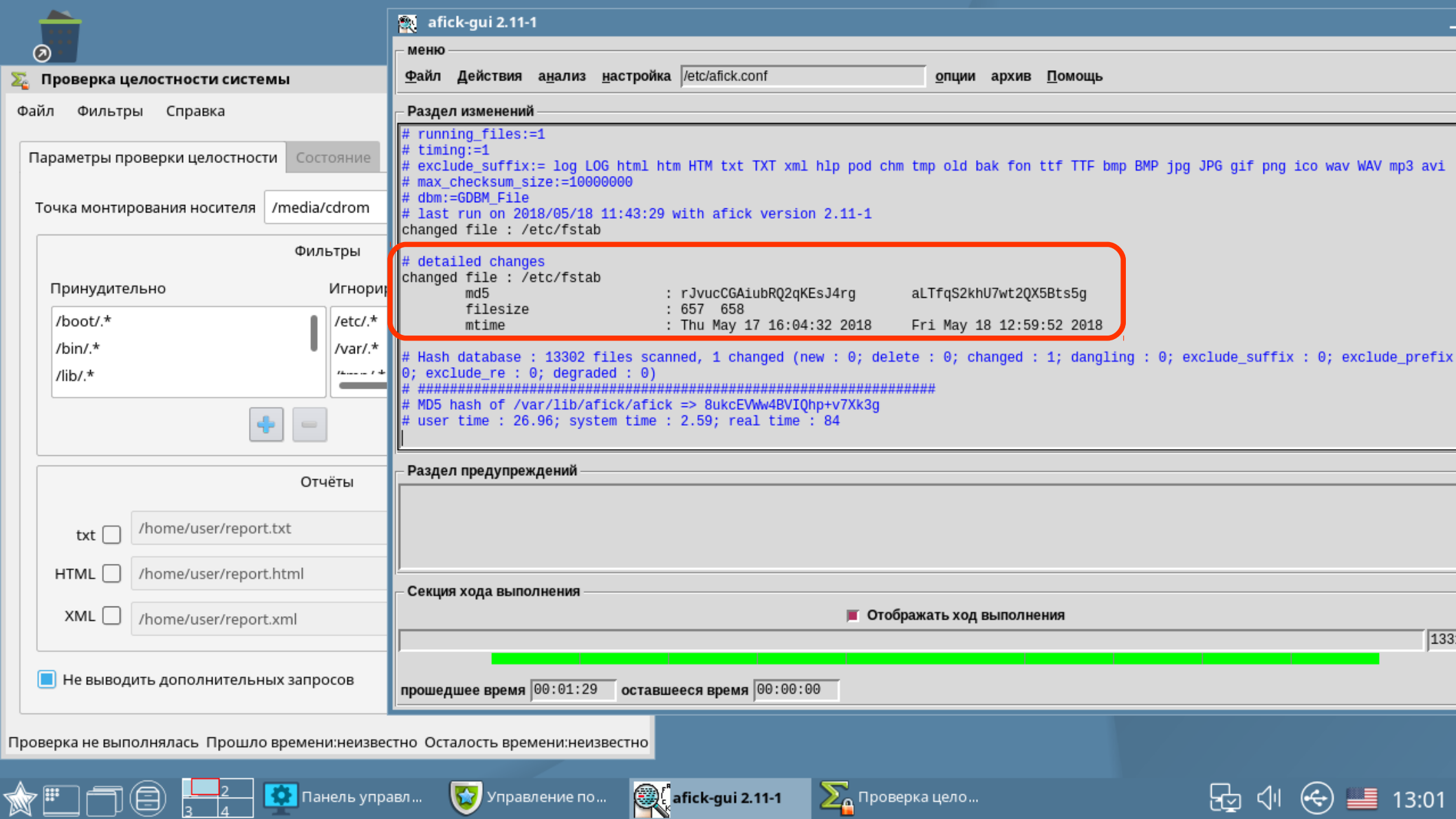
ПОДПИСЬ БИНАРНЫХ ФАЙЛОВ И РАЗДЕЛЯЕМЫХ БИБЛИОТЕК

ПОДПИСЬ СКРИПТОВ И ЛЮБЫХ ФАЙЛОВ


user - Менедже
Файл
Вид
Адрес:
Компьюте
user
lib
lib32
lib64
lost+fou
media
mnt
opt
parsecfs
bash (953.20 КБ)
Свойства
bash
Общие
Дискреционные атрибуты
Мандатная метка
Подпись
Информация
Загрузить ключи
Проверка подписей
Остановить
Тип хэша:
GOST R34.11-2012
Хэш:
db f7 b7 fd 04 96 d3 bd 40 cf 1e 0f 7d 61 9b 0f
02 0b 22 4b 01 c8 97 8c cd 43 a2 9b 27 f8 5b 26
Размер подписи:
96
Подпись:
88 5e 04 00 23 0c 00 06 05 02 56 d6 c6 9c 00 0a
09 10 51 3b 6d 7a a0 07 82 c8 49 d9 00 ff 57 e5
51 df 9b 88 cb 1d 19 73 95 1c 84 e9 5d a9 f1 53
d0 eb 3d d5 16 f1 ef 26 02 5f 13 c1 66 7b 00 fc
0d 73 d8 65 84 9d fb 7f 80 d2 c0 de 4c 42 95 f0
59 c4 2e 94 1d e9 c0 54 1e a1 f1 2c 93 0a e9 4c
Подписант:
A00782C8
Метка времени:
02 Mar 2016 15:55:24 (1456916124)
Состояние:
good hash found
Расширенные аттрибуты
Состояние:
no xattr hash found
Печать...
Да
Отмена
Панель управл...
Управление по...
user - Менедж...
12:55

МЕХАНИЗМ РЕГЛАМЕНТНОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ.

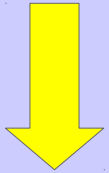



Проверка целостности системы
Файл Фильтры Справка
Параметры проверки целостности
Состояние
Точка монтирования носителя
/media/cdrom
Фильтры
Принудительно
Игнорир
/boot/.*
/bin/.*
/lib/.*
/etc/.*
/var/.*
Отчёты
txt
/home/user/report.txt
HTML
/home/user/report.html
XML
/home/user/report.xml
Не выводить дополнительных запросов
Проверка не выполнялась Прошло времени:неизвестно Осталость времени:неизвестно
afick-gui 2.11-1
меню
Файл Действия анализ настройка
/etc/afick.conf
опции архив Помощь
Раздел изменений
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 2018/05/18 11:43:29 with afick version 2.11-1
changed file : /etc/fstab
detailed changes
changed file : /etc/fstab
md5 : rJvucCGAiubRQ2qKEsJ4rg aLTfqS2khU7wt2QX5Bts5g
filesize : 657 658
mtime : Thu May 17 16:04:32 2018 Fri May 18 12:59:52 2018
Hash database : 13302 files scanned, 1 changed (new : 0; delete : 0; changed : 1; dangling : 0; exclude_suffix : 0; exclude_prefix
0; exclude_re : 0; degraded : 0)
##
MD5 hash of /var/lib/afick/afick => 8ukcEVWw4BVIQhp+v7Xk3g
user time : 26.96; system time : 2.59; real time : 84
Раздел предупреждений
Секция хода выполнения
Отображать ход выполнения
прошедшее время
00:01:29
оставшееся время
00:00:00
Панель управл...
Управление по...
afick-gui 2.11-1
Проверка цело...
13:01

РЕЖИМ КИОСКА

МЕХАНИЗМ ОГРАНИЧЕНИЯ ПРАВ ПОЛЬЗОВАТЕЛЯ В СИСТЕМЕ (РЕЖИМ КИОСКА)

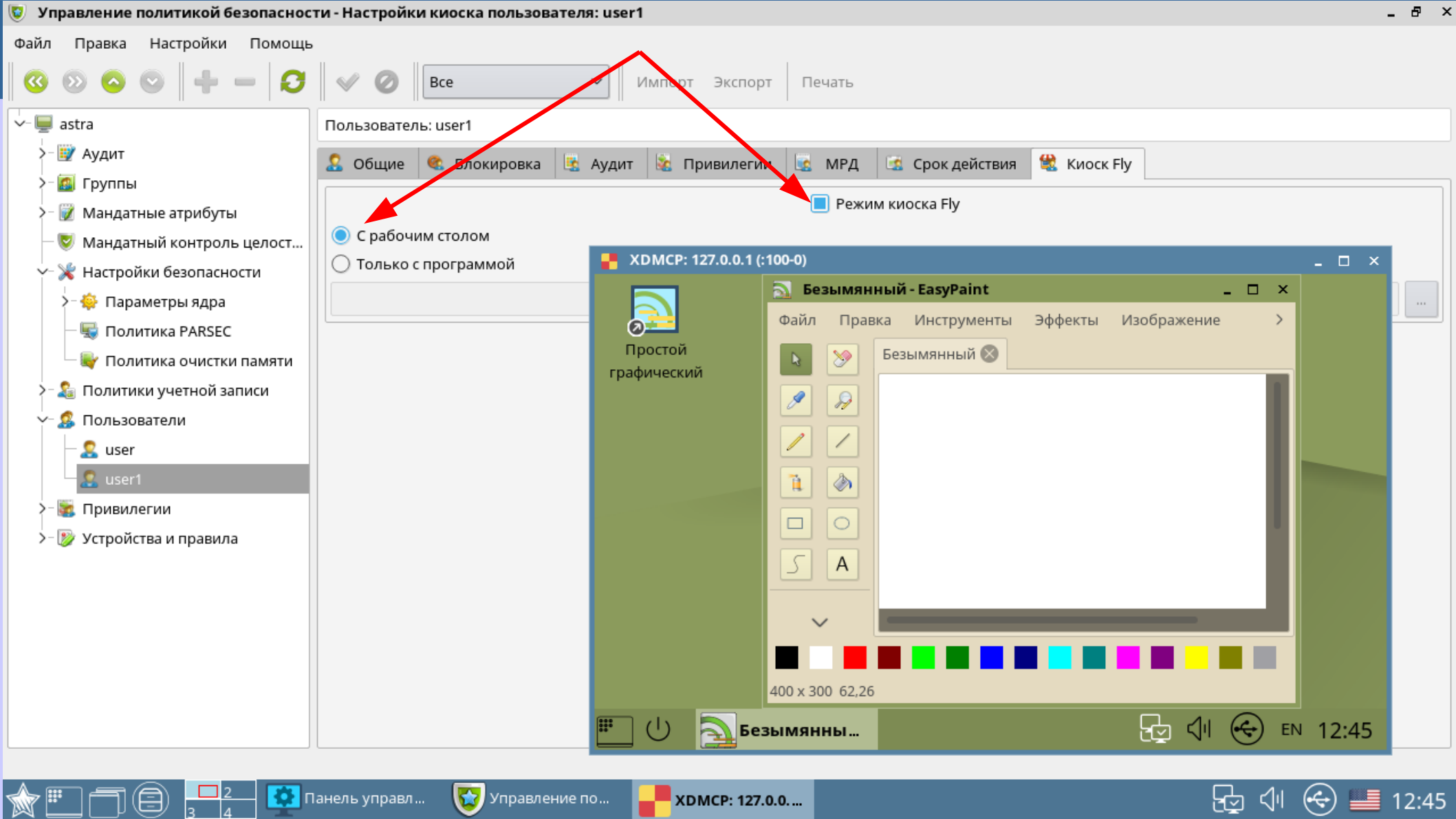
ВЫСОКОУРОВНЕВЫЙ КИОСК

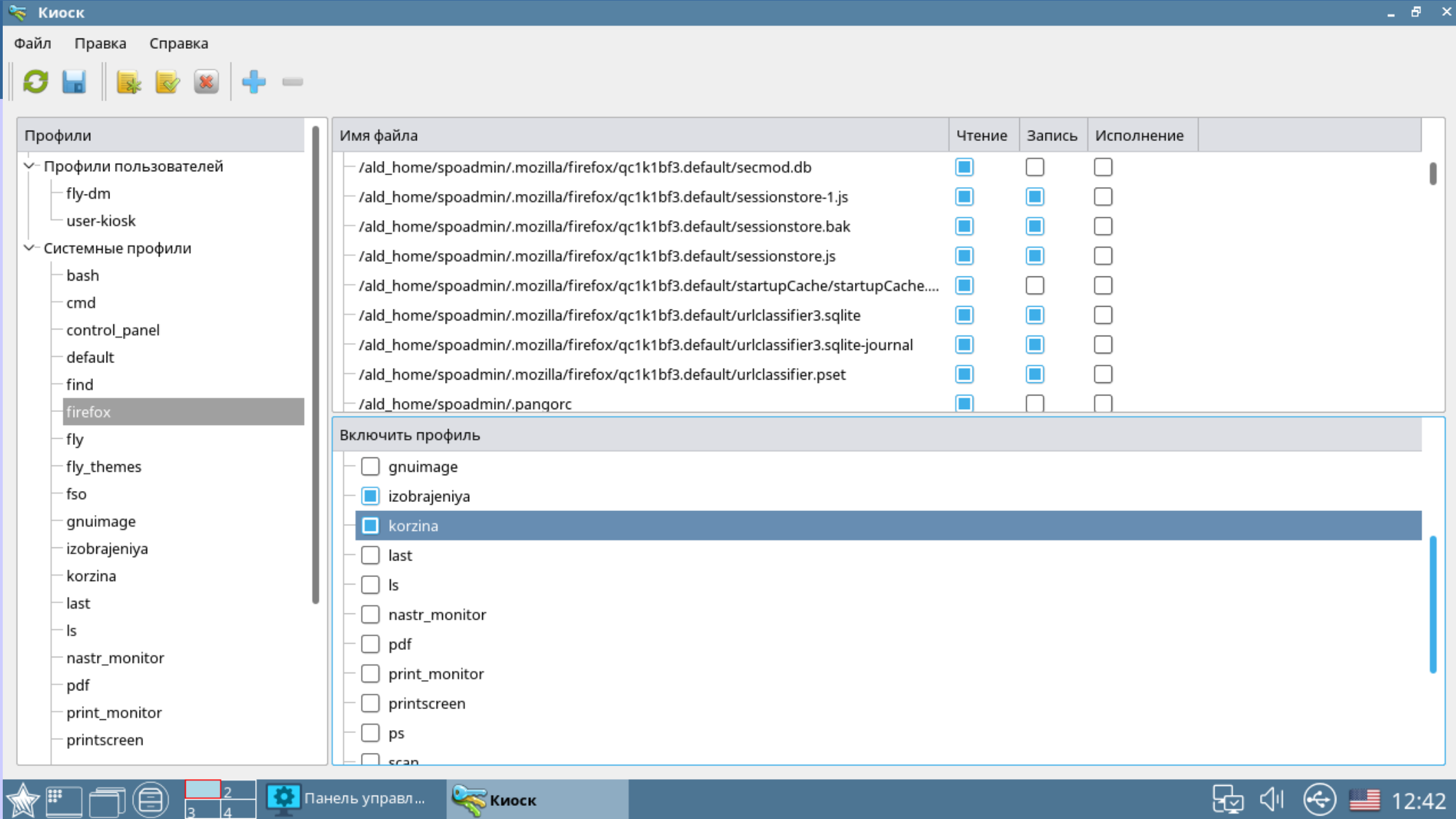


ОГРАНИЧЕНИЕ ПРАВ НА УРОВНЕ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА

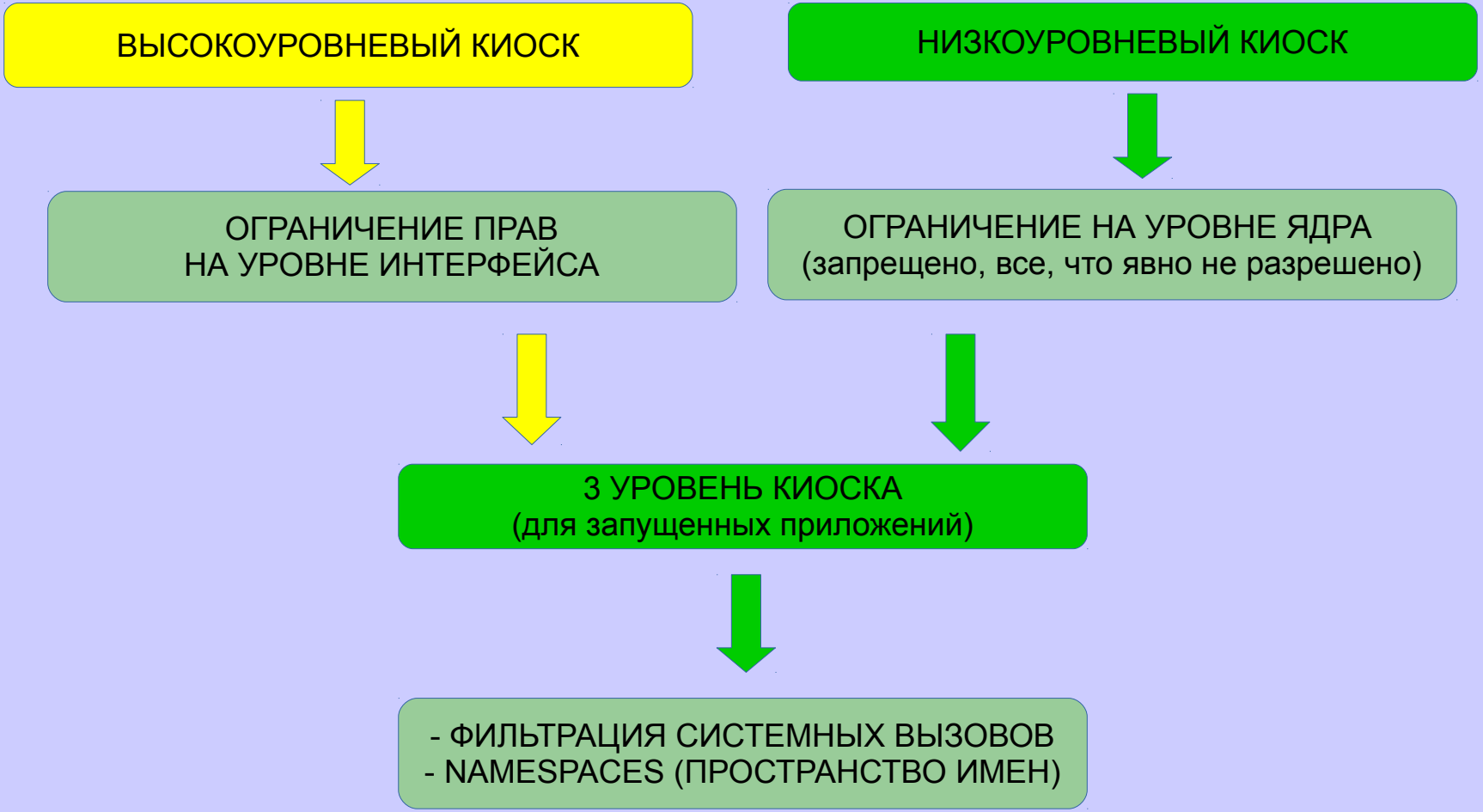
НИЗКОУРОВНЕВЫЙ КИОСК

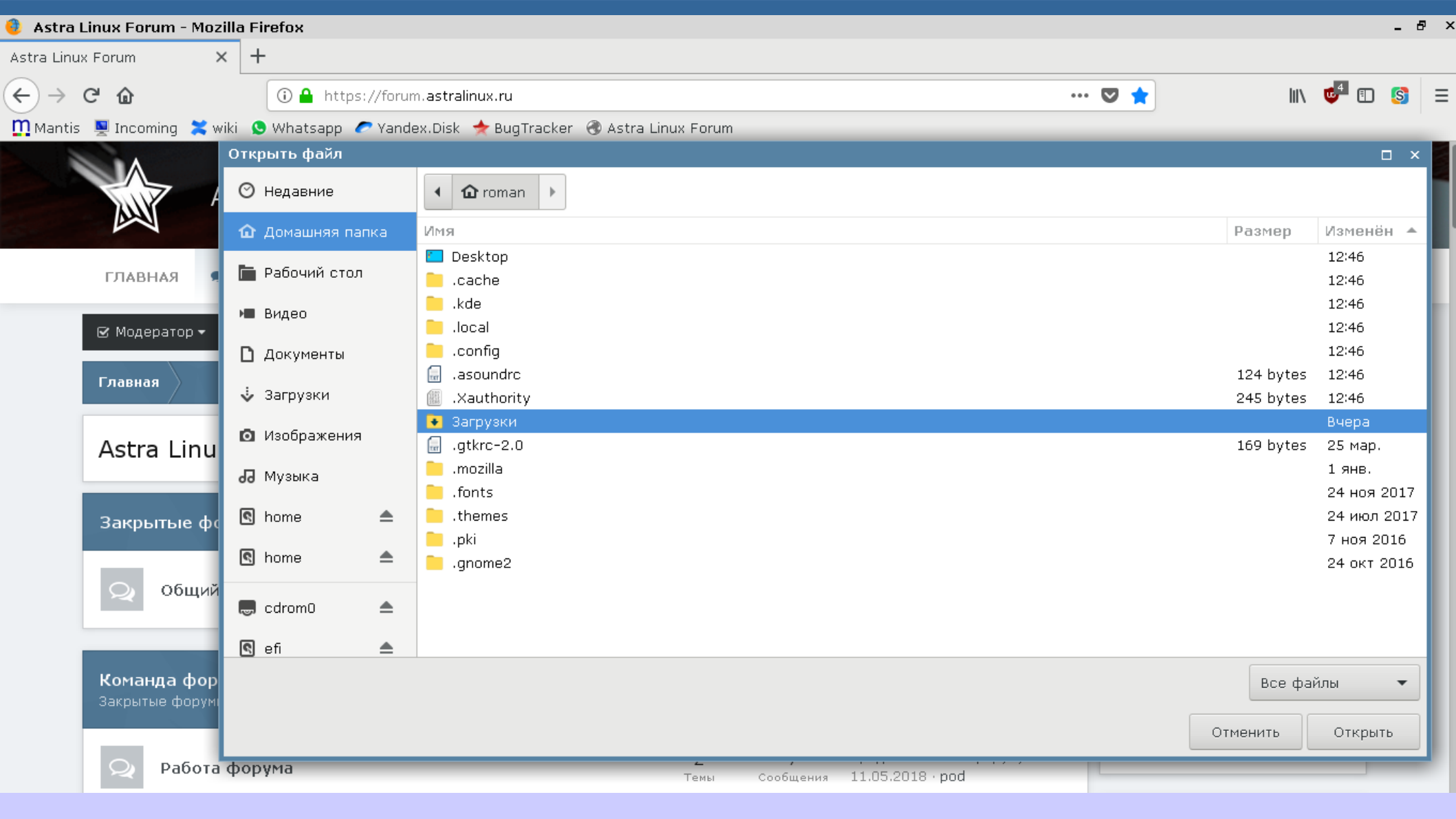
ОГРАНИЧЕНИЕ ПРАВ НА УРОВНЕ ЯДРА СИСТЕМЫ


Управление политикой безопасности - Настройки киоска пользователя: user1
Файл
Правка
Настройки
Помощь
Все
Импорт
Экспорт
Печать
astra
Аудит
Группы
Мандатные атрибуты
Мандатный контроль целост...
Настройки безопасности
Параметры ядра
Политика PARSEC
Политика очистки памяти
Политики учетной записи
Пользователи
user
user1
Привилегии
Устройства и правила
Пользователь: user1
Общие
Блокировка
Аудит
Привилегии
МРД
Срок действия
Киоск Fly
Режим киоска Fly
С рабочим столом
Только с программой
XDMCP: 127.0.0.1 (:100-0)
Простой графический
Безымянный - EasyPaint
Файл
Правка
Инструменты
Эффекты
Изображение
Безымянный
400 x 300 62,26
Безымянны...
EN
12:45
Панель управл...
Управление по...
XDMCP: 127.0.0....
12:45


Киоск
Файл
Правка
Справка
Профили
Профили пользователей
fly-dm
user-kiosk
Системные профили
bash
cmd
control_panel
default
find
firefox
fly
fly_themes
fso
gnuimage
izobrajeniya
korzina
last
ls
nastr_monitor
pdf
print_monitor
printscreen
Имя файла
Чтение
Запись
Исполнение
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/secmod.db
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/sessionstore-1.js
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/sessionstore.bak
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/sessionstore.js
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/startupCache/startupCache....
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/urlclassifier3.sqlite
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/urlclassifier3.sqlite-journal
/ald_home/spoadmin/.mozilla/firefox/qc1k1bf3.default/urlclassifier.pset
/ald_home/spoadmin/.pangorc
Включить профиль
gnuimage
izobrajeniya
korzina
last
ls
nastr_monitor
pdf
print_monitor
printscreen
ps
Панель управл...
Киоск
12:42

РЕЖИМ КИОСКА




Astra Linux Forum - Mozilla Firefox
Astra Linux Forum
https://forum.astralinux.ru
Mantis
Incoming
wiki
Whatsapp
Yandex.Disk
BugTracker
Astra Linux Forum
ГЛАВНАЯ
Модератор
Главная
Astra Linu
Закрытые фо
Общий
Команда фор
Закрытые форум
Работа форума
Темы
Сообщения
11.05.2018 · pod
Открыть файл
Недавние
Домашняя папка
Рабочий стол
Видео
Документы
Загрузки
Изображения
Музыка
home
home
cdrom0
efi
roman
Имя
Размер
Изменён
Desktop 12:46
.cache 12:46
.kde 12:46
.local 12:46
.config 12:46
.asoundrc 124 bytes 12:46
.Xauthority 245 bytes 12:46
Загрузки Вчера
.gtkrc-2.0 169 bytes 25 мар.
.mozilla 1 янв.
.fonts 24 ноя 2017
.themes 24 июл 2017
.pki 7 ноя 2016
.gnome2 24 окт 2016
Все файлы
Отменить
Открыть

РОЛЕВОЕ УПРАВЛЕНИЕ ДОСТУПОМ

МЕХАНИЗМ РОЛЕВОГО УПРАВЛЕНИЯ ДОСТУПОМ

НАЗНАЧЕНИЕ КОМПЛЕКСА ПРАВ И ОГРАНИЧЕНИЙ (МАНДАТНОГО ДОСТУПА И ЦЕЛОСТНОСТИ) ПОСРЕДСТВОМ МЕХАНИЗМА РОЛЕЙ

ПЛАНИРУЕТСЯ К ВКЛЮЧЕНИЮ В ASTRA LINUX SPECIAL EDITION 1.6 В 2018 ГОДУ

ДОПОЛНИТЕЛЬНЫЕ ЭЛЕМЕНТЫ КСЗ

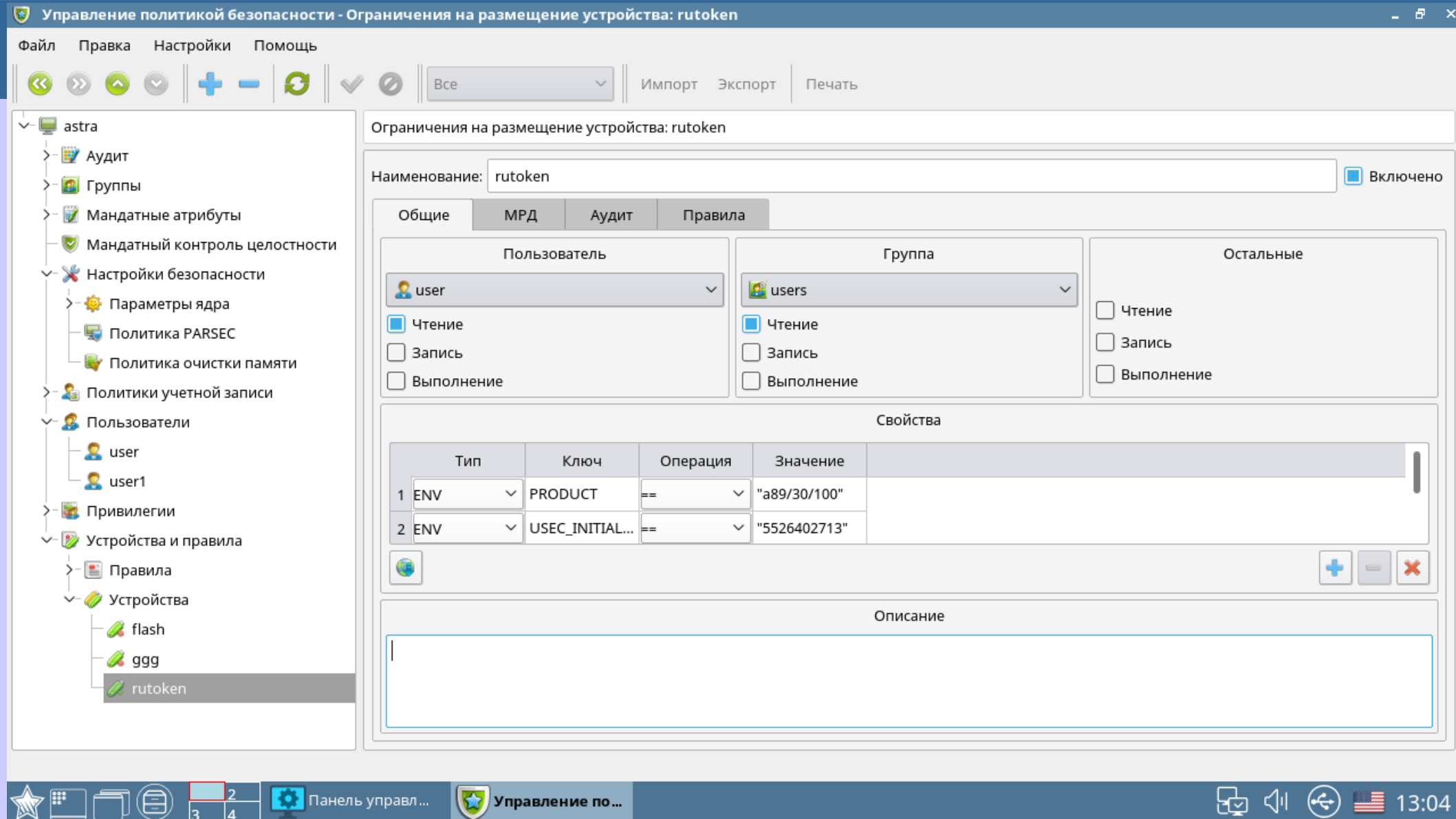
ОЧИСТКА ОБЛАСТЕЙ ПАМЯТИ

ИЗОЛЯЦИЯ ПРИЛОЖЕНИЙ ПОЛЬЗОВАТЕЛЯ

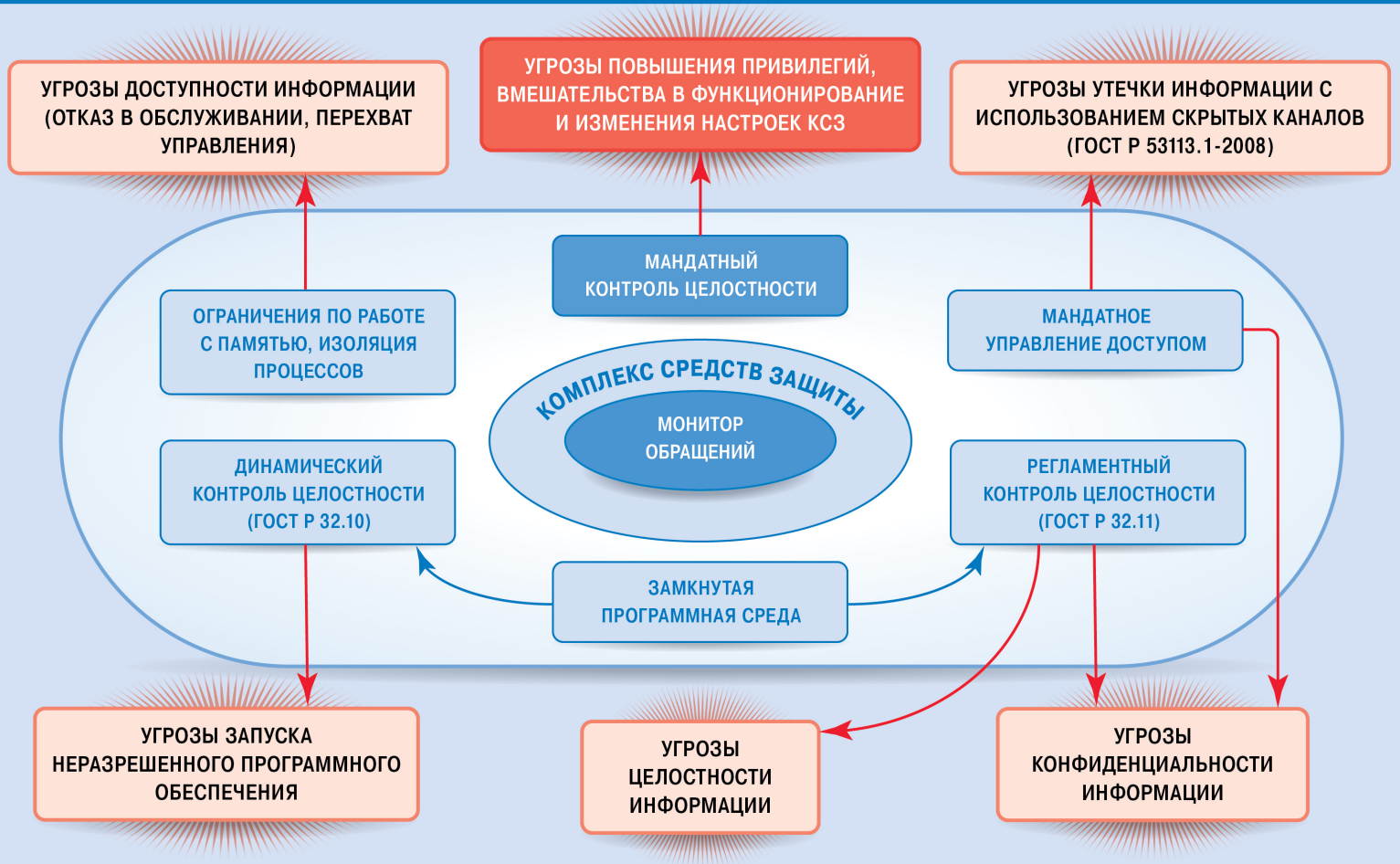
РАСШИРЕННЫЙ АУДИТ СОБЫТИЙ

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ В ДОМЕНЕ ПО ГОСТОВЫМ АЛГОРИТМАМ

И МНОГОЕ ДРУГОЕ...


Управление политикой безопасности - Ограничения на размещение устройства: rutoken
Файл
Правка
Настройки
Помощь
Все
Импорт
Экспорт
Печать
astra
Аудит
Группы
Мандатные атрибуты
Мандатный контроль целостности
Настройки безопасности
Параметры ядра
Политика PARSEC
Политика очистки памяти
Политики учетной записи
Пользователи
user
user1
Привилегии
Устройства и правила
Правила
Устройства
flash
ggg
rutoken
Ограничения на размещение устройства: rutoken
Наименование:
rutoken
Включено
Общие
МРД
Аудит
Правила
Пользователь
user
Чтение
Запись
Выполнение
Группа
users
Чтение
Запись
Выполнение
Остальные
Чтение
Запись
Выполнение
Свойства
Тип
Ключ
Операция
Значение
1
ENV
PRODUCT
==
"a89/30/100"
2
ENV
USEC_INITIAL...
==
"5526402713"
Описание
Панель управл...
Управление по...
13:04

АРХИТЕКТУРНЫЙ ПОДХОД



ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К ОПЕРАЦИОННЫМ СИСТЕМАМ

Приказ ФСТЭК России № 17 (с учетом приказа ФСТЭК России от 2017 г. № 27) требует при создании систем защиты информации государственных информационных систем использовать операционные системы соответствующего класса защиты.

«Astra Linux Special Edition» является операционной системой типа «А» и соответствует требованиям документов «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016) и «Профиль защиты операционных систем типа «А» **второго класса** защиты ИТ.ОС.А2.ПЗ» (ФСТЭК России, 2016).

www.rusbitech.ru

www.astralinux.ru

Группа «Security Linux» в Телеграм:

@safelinux