1. Определение мандатного контроля целостности (МКЦ)

Мандатный контроль целостности (Mandatory Integrity Control — MIC) — это распределение информации в системе или её компонентах по некоторым явно заданным уровням и назначение прав доступа на основе заданных уровней.

При реализации политики мандатного контроля целостности субъектам и сущностям задаются уровни целостности — совокупность неиерархических уровней (категорий) целостности и иерархических (линейных) уровней целостности.

Уровень целостности сущности отражает степень уверенности в целостности содержащейся в ней информации.

Уровень целостности субъекта соответствует его полномочиям по доступу к сущности, в зависимости от их уровней целостности, а также отражает степень уверенности в корректности его функциональности.

Мандатный контроль целостности в основном предназначен для того, чтобы затруднить программным закладкам внедрение в защищаемую ОС и дальнейшее функционирование в ней.

> **ПРИМЕЧАНИЕ**
> Программная закладка — это небольшая по объёму кода программа, которая внедряется в атакуемую систему и предоставляет нарушителю скрытный доступ к ресурсам атакуемой ОС, вносит уязвимость в её подсистему безопасности, противодействует антивирусному ПО, пакетным фильтрам, системам обнаружения атак и т.д. Компьютерные вирусы и сетевые черви являются частными случаями программных закладок.

В качестве побочного эффекта нейтрализуется угроза вывода ОС из строя некорректно работающим инсталлятором или деинсталлятором прикладного или системного ПО, которые ненамеренно повреждают критически важные программные модули ОС.

Степень уязвимости ОС в отношении программных закладок в основном определяется двумя взаимосвязанными факторами:

- насколько легко программной закладке внедрить свой программный код в критически важные (например, системные) области атакуемой ОС;
- насколько большие полномочия может получить внедрённая в ОС программная закладка в практически значимых ситуациях.

2. Уровни целостности и основное правило

МКЦ

Начиная с версии Astra Linux 1.7, используется 32-битная маска метки целостности, и добавлен 1 линейный знаковый байт.

При установке ОС, по умолчанию предлагается максимальным неиерархический уровень целостности (max_ilev) равный 63, а минимальный уровень всегда 0. После инсталляции ОС максимальный уровень целостности в системе можно повысить.

> **ВНИМАНИЕ!**
> При повышении максимального уровня целостности в ОС выше значения 63, заданного при установке ОС, необходимо убедиться в повышении уровня целостности администратора ОС.

Непривилегированным пользователям по умолчанию присваивается нулевой уровень целостности, администратору присваивается максимальный уровень целостности 63, за системными службами зарезервированы четыре изолированных уровня целостности.

> **ПРИМЕЧАНИЕ**
> Учётная запись непривилегированного пользователя не имеет полномочий по управлению средством защиты информации — ГОСТ Р 59453.1-2021.

Чем выше уровень целостности сущности, тем важнее данная сущность для обеспечения корректного функционирования ОС, и тем выше требования доверия к процессу, модифицирующему данную сущность.

В ОС по умолчанию выделены: нулевой, четыре ненулевых и несравнимых между собой (далее — изолированных) неиерархических уровня целостности и максимальный уровень целостности, который не меньше всех остальных в системе.

Уровень	Значение	Битовая маска	Описание
1	001	0000 0001	Уровень задействован для сетевых служб
2	002	0000 0010	Уровень задействован для виртуализации
3	003	0000 0100	Уровень задействован для специального ПО

4	008	0000 1000	Уровень задействован для графического сервера

В текущей реализации, с учетом 32-битной маски, количество изолированных уровней целостности может быть увеличено до 32.

> **ВНИМАНИЕ!**
> Для супер пользователя root установлен низкий уровень МКЦ.

Субъект с определенным уровнем целостности может получить доступ на запись к сущности, если его уровень целостности не ниже уровня целостности сущности.

Процесс, выполняющийся на низком уровне целостности, не имеет возможности:

- получать доступ к процессам, выполняющимся на более высоких уровнях целостности, в том числе, не может направлять управляющие сообщения их окнам;
- порождать процессы, выполняющиеся от имени другой учётной записи пользователя, с использованием механизмов su, sudo, suid/sgid;
- порождать процессы, выполняющиеся на высоком уровне целостности.

Выбор уровня целостности для корневого процесса пользовательской сессии осуществляется в начале сеанса. Если для сессии выбран низкий уровень целостности, то все процессы, выполняющиеся в ней, гарантированно выполняются на низком уровне целостности. Высокий уровень целостности следует выбирать только в том случае, если пользователь решает задачи администрирования системного ПО, настройки или конфигурирования ОС в целом. Сессии с высоким уровнем целостности не должны использоваться чаще, чем это необходимо. Большинство пользовательских сессий должны стартовать на низком уровне целостности.

3. Управление мандатным контролем целостности

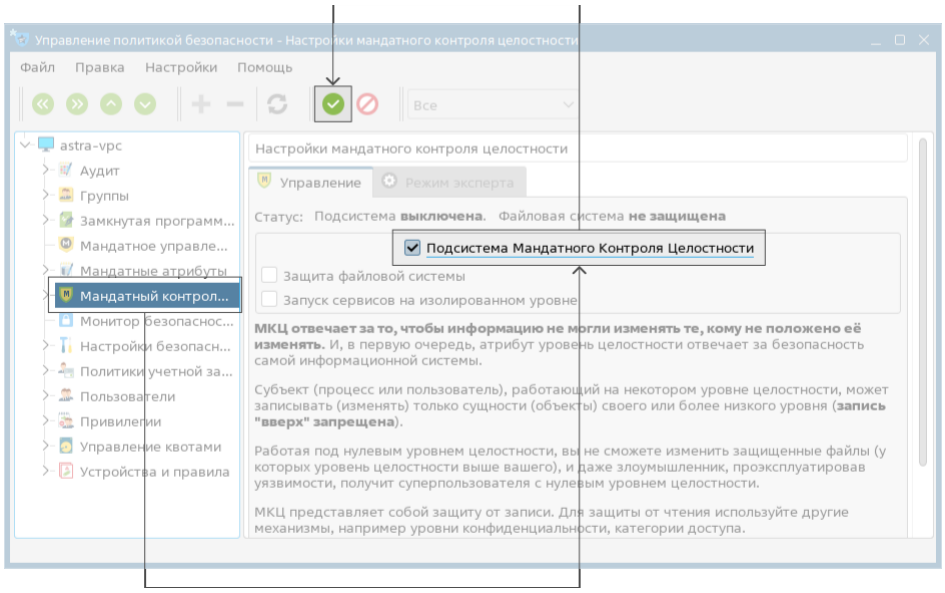
Включение МКЦ уже после установки ОС можно выполнить в Управление политикой безопасности. Для запуска Пуск → Панель управления → Безопасность → Политика безопасности. Чтобы включить МКЦ вокне программы требуется выполнить следующие шаги:

☐. На панели навигации выбрать категорию Мандатный контроль целостности

целостности.

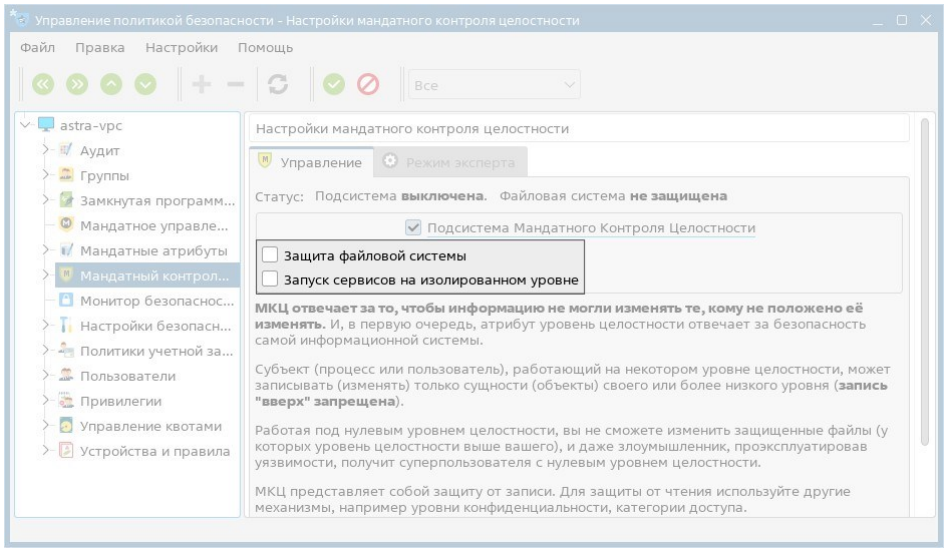
☐. Установить флаг в поле Подсистема Мандатного Контроля Целостности

☐. На панели инструментов нажать кнопку Применить изменения.



После включения МКЦ необходимо перезагрузить ОС.

На вкладке управления МКЦ можно активировать защиту файловой системы и запуск сервисов на изолированном уровне.



При включении МКЦ для системного параметра ядра parsec.max_ilev в загрузчике ОС устанавливается значение 63 — максимальный уровень целостности по умолчанию. Все процессы, начиная от init и до утилиты графического входа в систему fly-dm, будут запускаться на данном уровне целостности.На объектах файловой системы устанавливаются принятые по умолчанию значения целостности (высокий уровень целостностина каталогах /dev, /proc, /run, /sys).

Графический сервер Xorg по умолчанию работает от имени учётной записи пользователя на выделенном

уровне целостности8.

ПРИМЕЧАНИЕ

- Непривилегированный пользователь может выполнять вход в систему только на низком уровне целостности. Привилегированный пользователь, приналичии соответствующего права, может входить в систему на высоком уровне целостности только для выполнения задач по конфигурированию ОС.
- Администратор, созданный при установке ОС, можетвыполнять вход в систему с высоким уровнем целостности (по умолчанию 63) или с низким уровнем целостности.
- Графический рабочий стол на высоком уровне целостности имеет красный фон.

Для домашних каталогов пользователей с ненулевым уровнемцелостности устанавливается соответствующий максимально доступный уровень целостности этого пользователя.
Создаваемому файлу (каталогу) назначается уровень целостности, равный уровню целостности того каталога, в котором он создается.

Непосредственный запуск процесса запрещён в том случае, еслиисполняемый файл, из которого запускается процесс, имеет уровень целостности меньше или несравнимый с уровнем целостности процесса родителя.

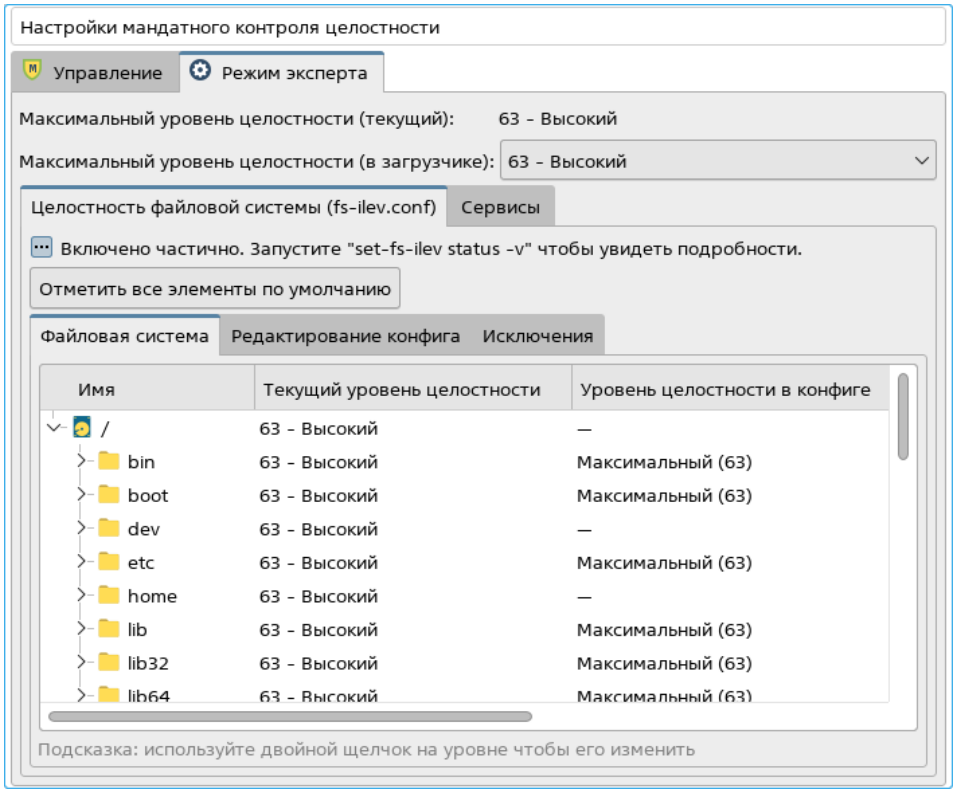
После выключения МКЦ и перезагрузки целостность на объектахфайловой системы сбрасывается на нулевые значения.

ВНИМАНИЕ!
Перед выключением МКЦ рекомендуется предварительновыключить МКЦ на файловой системе.

Начиная с обновления 1.7.2, в ОС доступен расширенный режимМКЦ, который позволяет:

- просмотреть информацию об уровне целостности файлов икаталогов;
- изменить значение уровня целостности для файлового объекта в конфигурационном файле;
- установить значения уровней целостности, заданные по умолчанию, для всех файловых объектов;
- изменить полный путь к файловому объекту;
- добавить или удалить строку в конфигурационном
- файле; просмотреть конфигурационный файл во внешнем редакторе;

- настроить перечень файловых объектов, целостность которыхпроверяться не будет;
- установить максимально допустимый уровень целостности всистеме;
- включить или выключить МКЦ для защищенного комплекса программ печати и маркировки документов (CUPS);
- включить или выключить функцию запуска на низком уровнецелостности для сетевых служб apache2, dovecot и exim4, а также программного обеспечения Docker.



ВНИМАНИЕ!
Для успешного запуска внешнего редактора необходимо,чтобы в системе для редактирования файлов с расширением *.conf по умолчанию использовалась программа без графического интерфейса (например, инструмент командной строки Vim).

4. Режим киоска

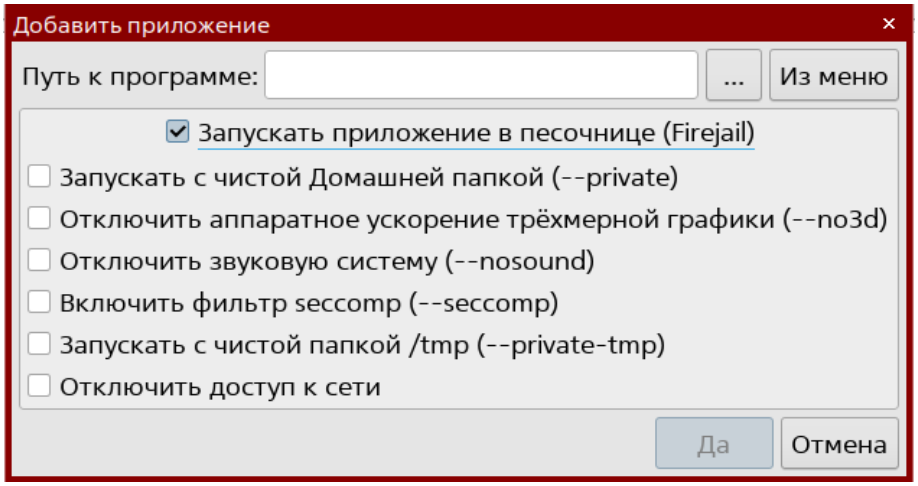
В ОС Astra Linux SE имеется возможность включить режимы графического и системного киоска. Графический киоск позволяет ограничить запуск программ локальным пользователям. Системный киоск (режим Киоск-2) — это инструмент системы PARSEC для ограничения возможностей, предоставляемых непривилегированным пользователям.

Графический киоск ограничивает доступ на уровне графической среды. Включение режима графического киоска ограничивает работу пользователя только с приложениями из списка при следующих условиях:

- если в списке одно приложение, то режим включается при работе с этим приложением;
- если в списке несколько приложений, то запускается рабочий стол с этими приложениями;
- все доступные каталоги, ярлыки и т.д. устанавливаются в соответствии с предоставленным доступом.

При работе с графическим киоском доступен Firejail — инструмент обеспечения изолированного выполнения графических и консольных приложений, который позволяет:

- определять файлы и каталоги, к которым разрешен или запрещен доступ;
- предоставлять доступ к файлам или каталогам только для чтения;
- подключать для данных временные ФС (tmpfs);
- совмещать каталоги через bind-mount и overlayfs.



Системный киоск ограничивает пользователя на уровне ядра системы (ограничение происходит на уровне доступа к конкретным файлам). Ограничения осуществляются на основе профилей:

- профили пользователей служат для применения ограничений действий пользователей (установка ограничений только для одного пользователя):
  - если при включенном режиме Киоск 2 отсутствует профиль пользователя, то права данного пользователя в ОС не ограничиваются;
  - если для пользователя создан пустой профиль, то данному пользователю запрещены любые действия.
- системные профили также служат для применения ограничений действий пользователей. Системный профиль можно добавить в профили нескольких пользователей, тогда для всех этих пользователей будет доступно использование приложения в соответствии с ограничениями в правах доступа и владельцах, указанных в системном профиле данного приложения.

Графический киоск настраивается в программе управления политикой безопасности и может быть включен для отдельного пользователя и/или для группы пользователей. Системный киоск настраивается в отдельной программе, доступной в категории **Безопасность** панели управления.