Лабораторная работа №9.

Базовый комплекс средств защиты информации

Введение

В данной лабораторной работе мы познакомимся с подсистемой безопасности PARSEC, рассмотрим суть понятий мандатного контроля целостности и мандатного управления доступом, научимся работать на низком и высоком уровне целостности, изменять уровни конфиденциальности и категории, назначать метки безопасности на файлы и каталоги, назначать мандатные уровни учетным записям, назначать PARSEC-привилегии, узнаем о средствах ограничения программной среды (режим киосков).

Мандатный контроль целостности

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.

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 суперпользователя 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:

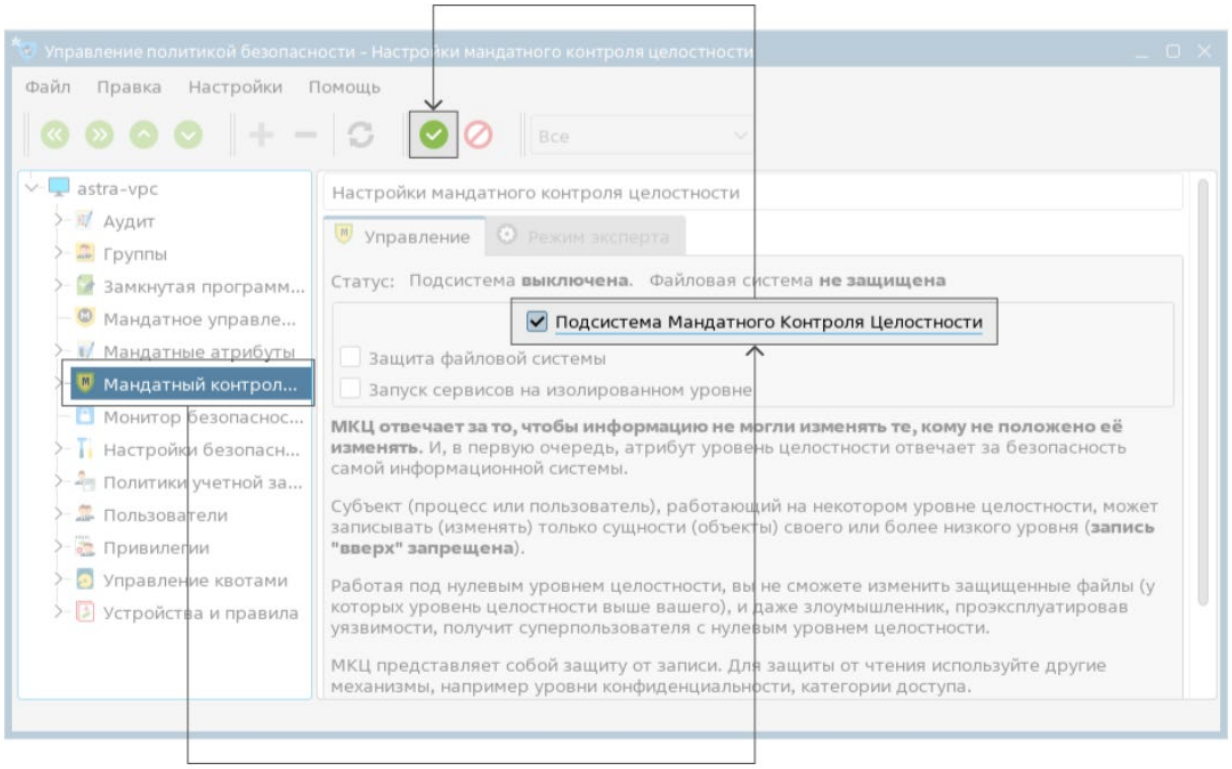
- получать доступ к процессам, выполняющимся на более высоких уровнях целостности, в том числе, не может направлять управляющие сообщения их окнам;
- порождать процессы, выполняющиеся от имени другой учётной записи пользователя, с использованием механизмов `su, sudo, suid/sgid`;
- порождать процессы,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

Управление мандатным контролем целостности

МКЦ уже после установки ОС можно выполнить в приложении Управление политикой безопасности. Для запуска программы следует нажать Пуск → Панель управления → Безопасность → Политика безопасности или из терминала под пользователем root: `fly-admin-smc`. Чтобы включить МКЦ в окне программы требуется выполнить следующие шаги:

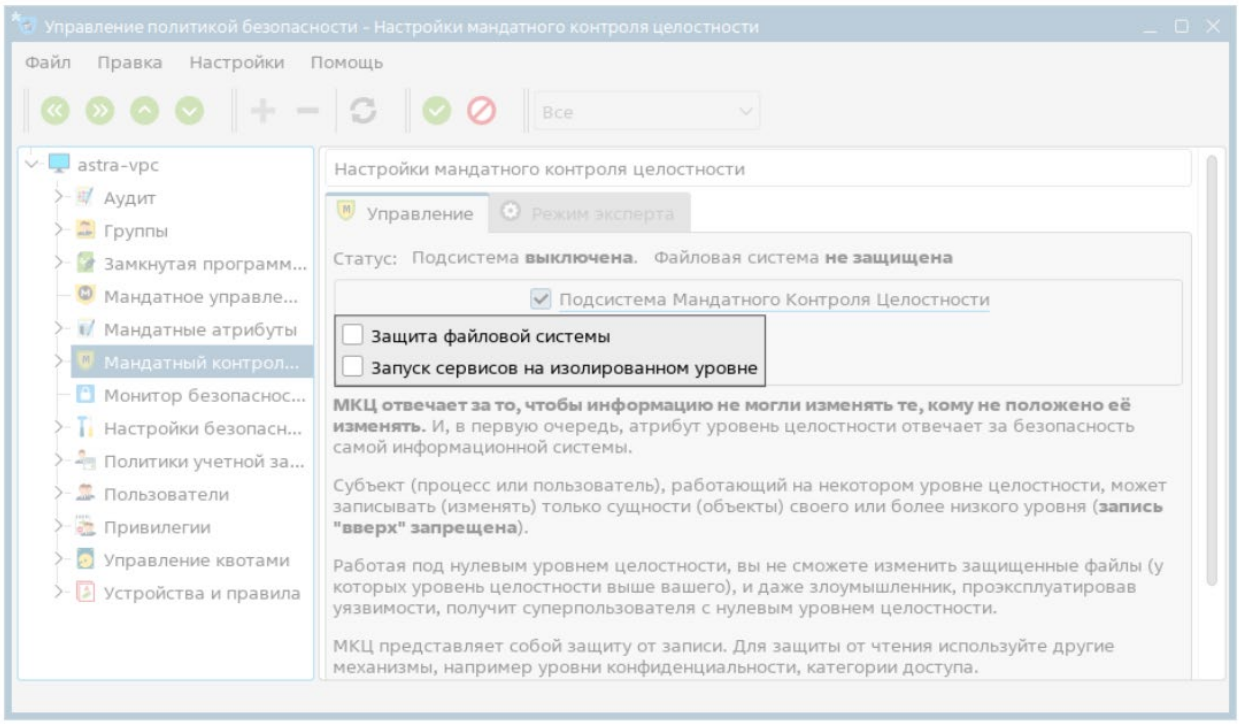
1. На панели навигации выбрать категорию Мандатный контроль целостности.
2. Установить флаг в поле Подсистема Мандатного Контроля Целостности.
3. На панели инструментов нажать кнопку Применить изменения.



Включение МКЦ

После включения МКЦ необходимо перезагрузить ОС.

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



Вкладка управления МКЦ

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 целостности на каталогах `/dev, /proc, /run, /sys`).

Графический сервер Xorg по умолчанию работает от имени учётной записи пользователя на выделенном уровне целостности 8.

Примечание

- Непривилегированный пользователь может выполнять вход в систему только на низком уровне целостности. Привилегированный пользователь, при наличии соответствующего права, может входить в систему на высоком уровне целостности только для выполнения задач по конфигурированию ОС.
- Администратор, созданный при установке ОС, может выполнять 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 уровнем целостности 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, если исполняемый файл, из которого запускается процесс, имеет уровень целостности меньше или несравнимый с уровнем целостности процесса родителя.

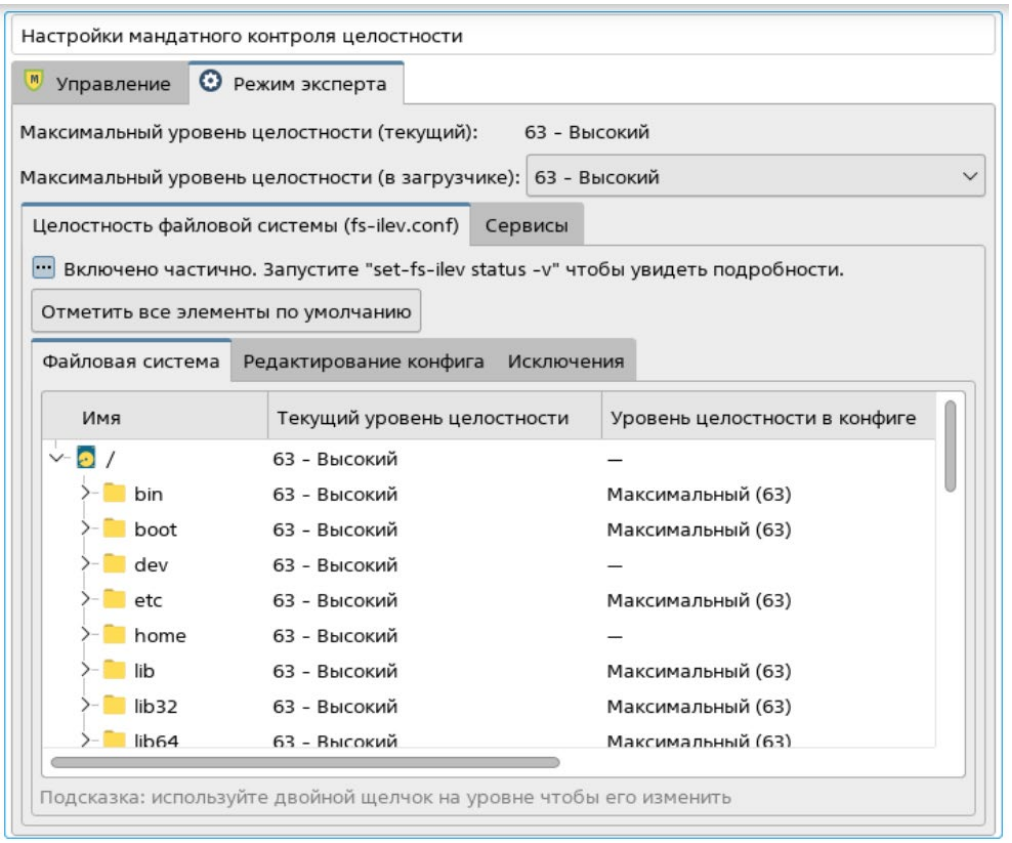
После выключения МКЦ и перезагрузки целостность на объектах файловой системы сбрасывается на нулевые значения.

Внимание

Перед выключением МКЦ рекомендуется предварительно выключить МКЦ на файловой системе.

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

- просмотреть информацию об уровне целостности файлов и каталогов;
- 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 которых проверяться не будет;
- установить максимально допустимый уровень целостности в системе;
- включить или выключить МКЦ для защищенного комплекса программ печати и маркировки документов (CUPS);
- включить или выключить функцию запуска на низком уровне целостности для сетевых служб apache2, dovecot и exim4, а также программного обеспечения Docker.



Настройка мандатного контроля целостности в режиме эксперта

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).

Режим киоска

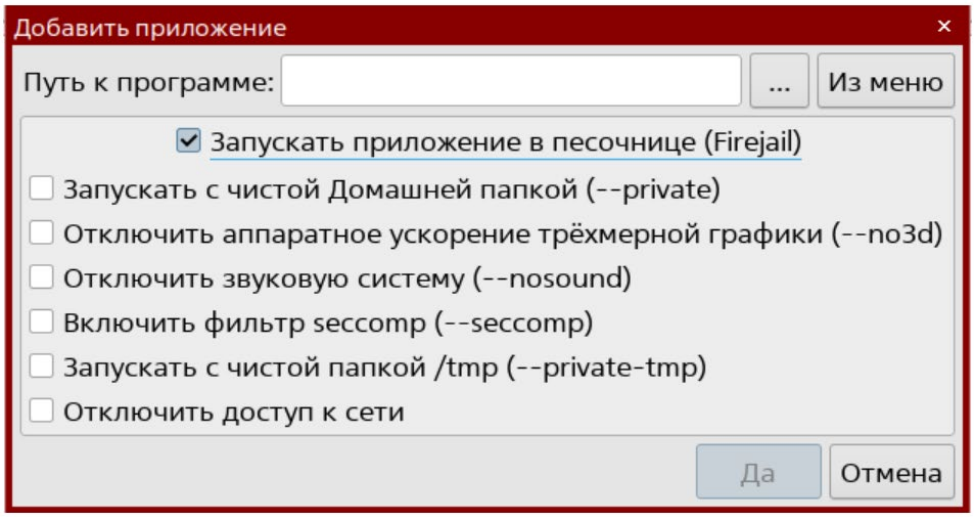
В ОС Astra Linux SE имеется возможность включить режимы графического и системного киоска. Графический киоск позволяет ограничить запуск программ локальным пользователям. Системный киоск (режим Киоск-2) — это инструмент системы PARSEC для ограничения возможностей, предоставляемых непривилегированным пользователям.

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`.

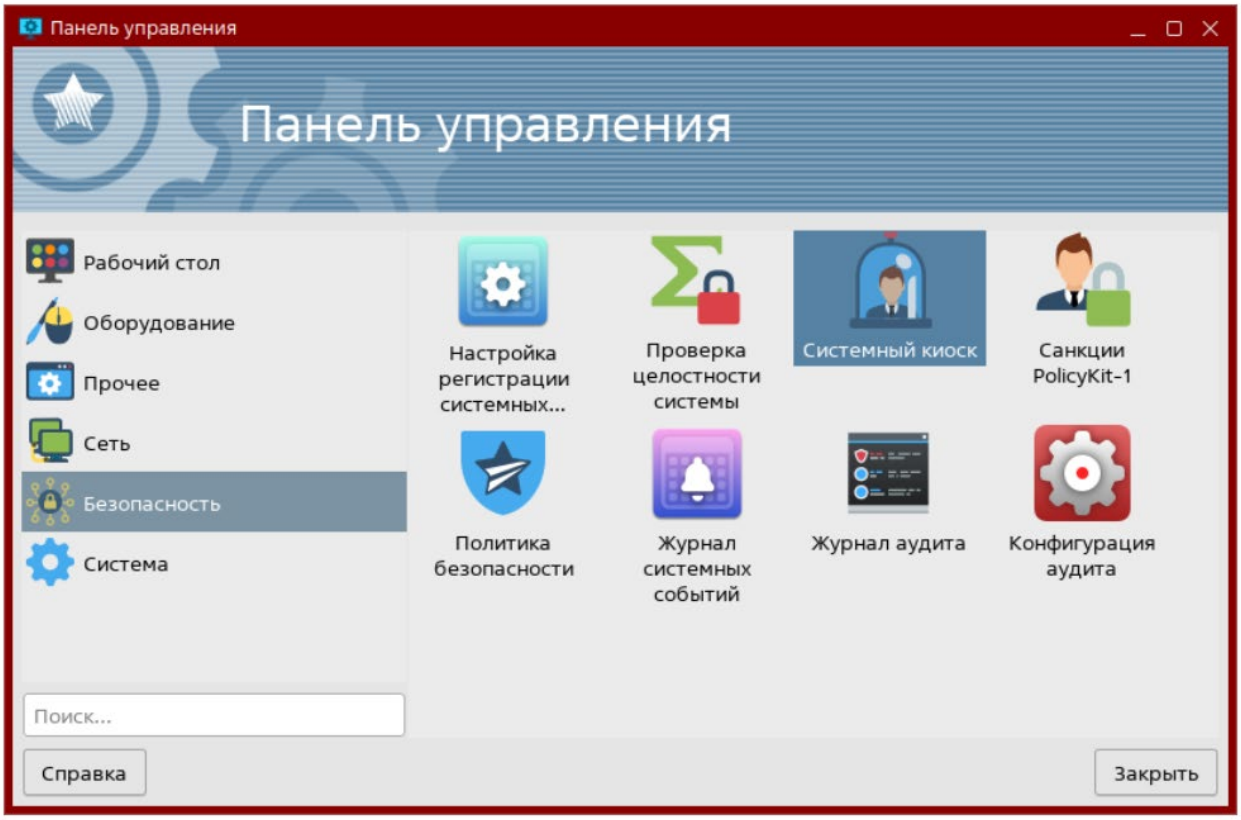


Инструмент Firejail

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.



Мандатное управление доступом

Политика мандатного управления доступом

Мандатное управление доступом подразумевает разграничение доступа в зависимости от уровня конфиденциальности и категории.

То, к чему необходимо ограничить доступ, называют объектом или сущностью (файл, каталог, и т.п.).

Пользователь или процесс, который пытается получить доступ к объекту, называют субъектом.

Также выделяют понятие контейнер — структурированная сущность доступа, т.е. сущность (каталог), которая может содержать другие сущности доступа (каталоги или файлы).

Сущностям и субъектам присваиваются следующие мандатные атрибуты:

- иерархический уровень конфиденциальности - определяет степень секретности документа (сущности) и соответствующий уровень доступа к этому документу, назначенный персоналу (субъекту);
- неиерархическая категория конфиденциальности - разделение по категориям конфиденциальности. Субъект, относящийся к определённой категории может иметь доступ только к сущностям той же категории. Доступ может быть предоставлен одновременно к нескольким категориям;
- дополнительные мандатные атрибуты - являются необязательными и позволяют уточнять или изменять правила мандатного доступа для отдельных контейнеров, субъектов или сущностей.

Мандатные атрибуты субъекта/сущности объединяются в мандатный контекст этого субъекта/сущности.

Классический пример уровней конфиденциальности - это степени повышающейся секретности документов (сущностей) "Не секретно" - "ДСП" - "Секретно" - "Совершенно секретно", и соответствующие им уровни доступа к этим документам, назначенные персоналу (субъектам).

В такой системе персоналу с уровнем доступа, например, "ДСП", разрешено читать только документы уровней "ДСП" и "Не секретно", и запрещено читать документы с более высокими уровнями конфиденциальности ("Секретно" и "Совершенно секретно").

Персоналу с уровнем конфиденциальности, например "Секретно", запрещено передавать (преднамеренно или случайно) персоналу с более низким уровнем доступа "ДСП" документы уровня "Секретно".

Объекту присваивается любое значение из иерархии уровней доступа. Для объекта допускается повышение уровня секретности (изменение до большего значения уровня, чем текущий). Понижение уровня секретности категорически не допускается.

Уровни объекта и субъекта равны
Уровень субъекта выше уровня объекта
Уровень субъекта ниже уровня объекта

Для более точного управления доступом, в дополнение к разделению по уровням конфиденциальности, СЗИ предоставляет возможность разделить материалы по категориям конфиденциальности.

Простой пример категорий конфиденциальности - «Научно-технический отдел» и «Бухгалтерия».

У двух субъектов одинаковый уровень конфиденциальности, но разная категория. Они создают документы на одном уровне секретности но в разных категориях, поэтому документы каждого субъекта недоступны другому.

Категории уровней конфиденциальности

Управление мандатным доступом реализовано на основе подсистемы безопасности PARSEC. Она разработана на основе адаптированной для ОС семейства Linux современной верифицированной формальной модели безопасности управления доступом и информационными потоками (МРОСЛ ДП-модели).

Каждому объекту назначается метка безопасности (мандатная метка).

Каждой учетной записи назначаются допустимые уровни мандатного доступа.

При входе в систему пользователь выбирает, с какими значениями мандатных уровней (мандатный контекст) будет работать пользователь в сеансе. Процессы, запущенные пользователем в рамках сеанса, наследуют мандатный контекст, выбранный пользователем при входе.

Доступ к объекту определяется путем сравнения метки безопасности объекта и мандатного контекста процесса:

- если мандатный контекст субъекта совпадает с меткой безопасности объекта, то субъект может и читать, и изменять содержимое объекта;
- если мандатный контекст субъекта больше метки безопасности объекта, то субъект может только читать содержимое объекта;
- если мандатный контекст субъекта меньше метки безопасности объекта, то субъект не может получить доступ к объекту.

Пользователь не может изменять метки безопасности файлов и каталогов. Только суперпользователь.

Итоговые права доступа к файлам и каталогам определяются совместным применением дискреционных и мандатных прав.

Метка безопасности (мандатная метка) состоит из:

- Классификационной метки;
- Метки целостности;
- Дополнительные необязательные атрибуты (`ccnr, ehole, whole`).

Классификационная метка состоит из:

- Иерархического уровня конфиденциальности (1 байт: 256 уровней);
- Неиерархической категории конфиденциальности (8 байт: 64 категории).

Дочерний процесс полностью наследует метку безопасности родительского процесса.

Когда процесс создает файл, то файл наследует только классификационную метку процесса. Файл получает нулевую метку целостности.

Для каталогов может быть применён дополнительный атрибут — ccnr. Каталог с таким атрибутом может содержать файлы и каталоги с различными классификационными метками, но не большими, чем его собственный.

Для файлов могут быть применены следующие дополнительные атрибуты:

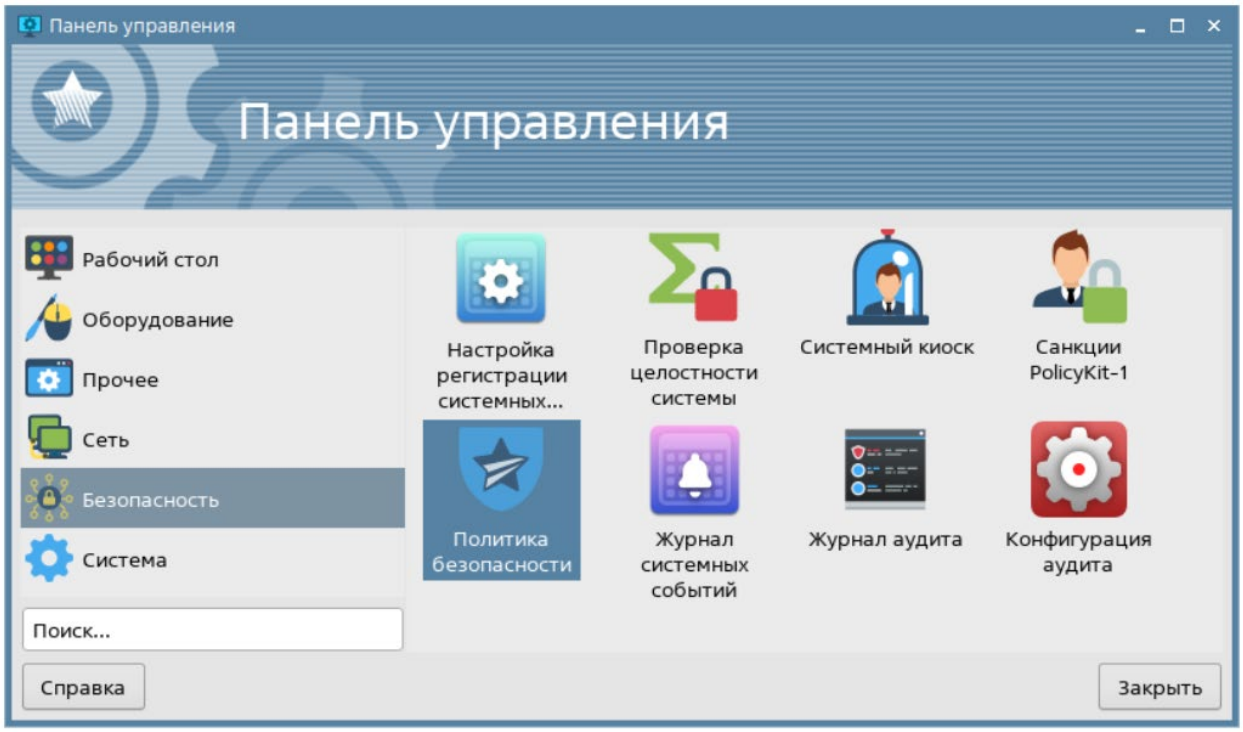
- `ehole` — файл, имеющий минимальную классификационную метку, игнорирует правила управления мандатным доступом к нему, процессы не могут прочитать данные, записанные в такие файлы (пример: `/dev/null`);
- `whole` — файл, имеющий максимальную классификационную метку, разрешает процессам, имеющим более низкую классификационную метку, записывать в них.

Начиная с оперативного обновления 1.7.2 добавлены дополнительные атрибуты:

- `irelax,` применимый к каталогам. В каталог с таким флагом запись может осуществлять процесс с уровнем целостности не выше, чем уровень целостности каталога. Создаваемые файлы получают (наследуют) целостность создающего процесса.
- `silev`— присваивается файлам. Позволяет запускаемому из данного файла процессу назначать уровень целостности файла по маске максимального уровня целостности системы, т.е. максимальное значение уровня целостности одновременно меньшее уровня целостности данного файла и максимального уровня целостности системы. Например, для корректного запуска файла `/usr/bin/passwd,` имеющего высокий уровень целостности, пользователем с низким уровнем целостности.

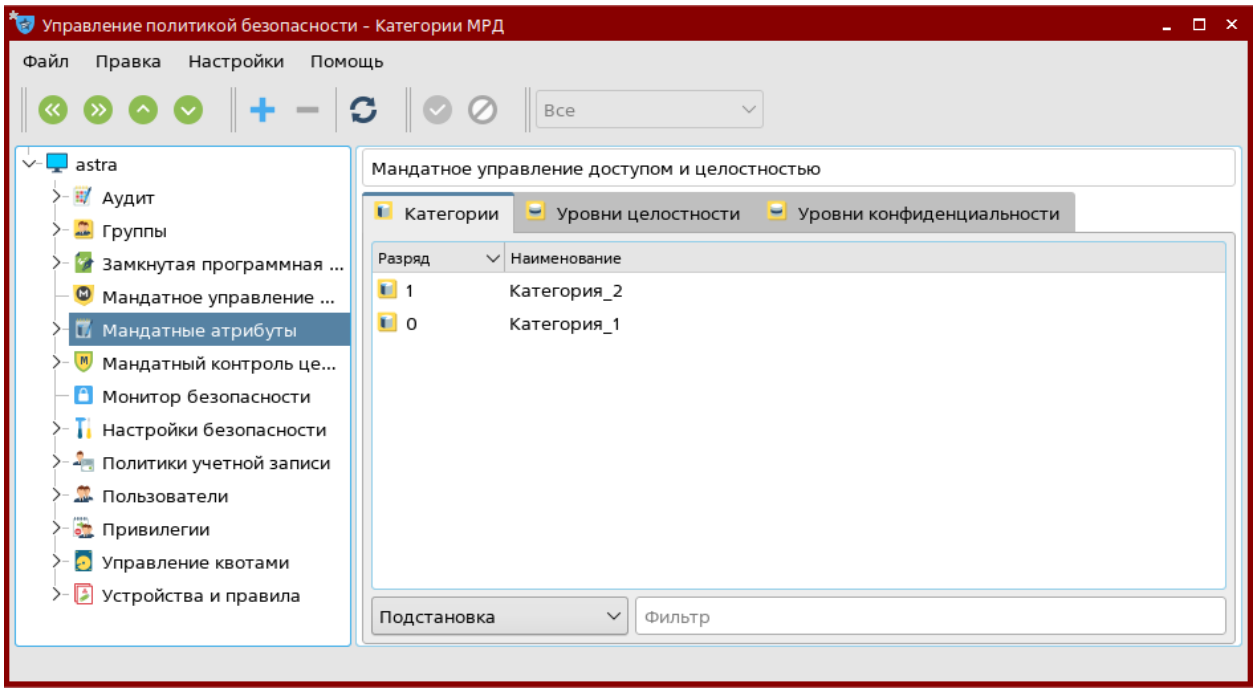
Определение мандатных уровней для учётных записей

Уровень конфиденциальности задаётся в программе Политика безопасности, которую можно запустить из панели управления.



Запуск программы управления политикой безопасности

Управление мандатными атрибутами выполняется в соответствующем разделе. Этот раздел доступен только на максимальном уровне защищённости (Смоленск).

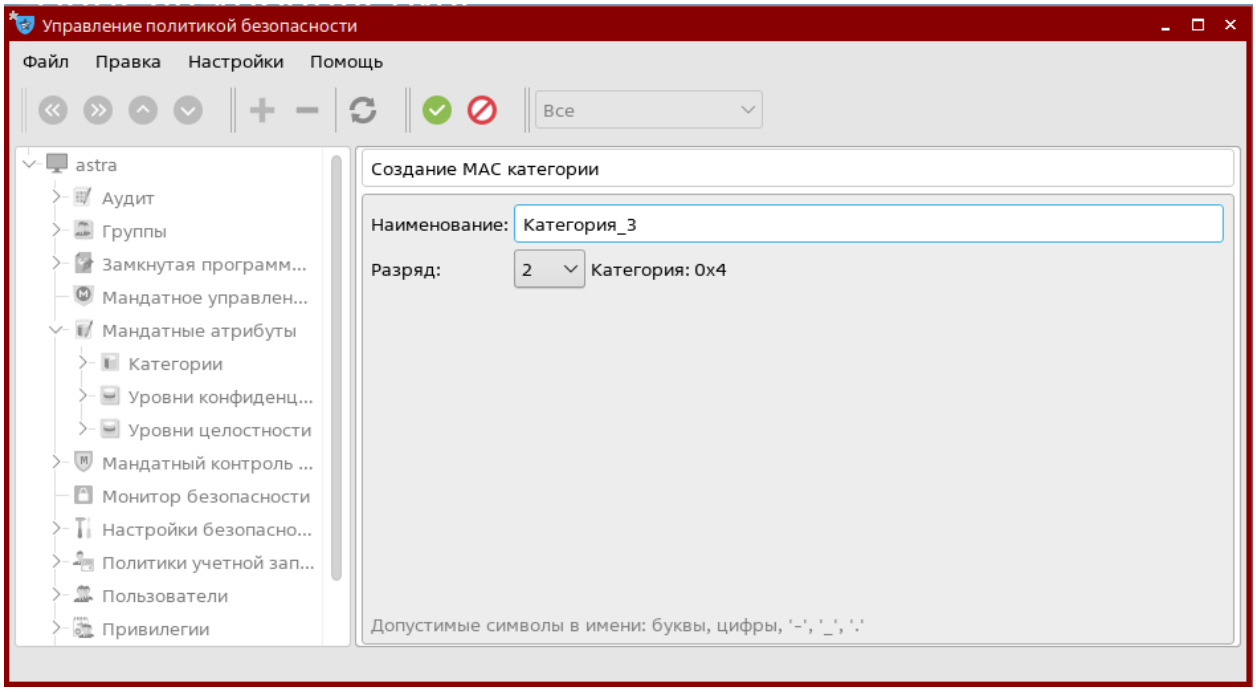


Мандатные атрибуты

Раздел содержит три вкладки, на которых можно редактировать соответствующие атрибуты:

- Категории;
- Уровни целостности;
- Уровни конфиденциальности.

Создать атрибут можно с помощью кнопки в виде плюса синего цвета. Для удаления атрибута предусмотрена кнопка в виде минуса красного цвета. Двойное нажатие на атрибут позволит перейти к его редактированию. Редактированию подвержены только лишь наименования категорий и уровней конфиденциальности. В именах уровней конфиденциальности и категорий допустимо использовать только буквы, цифры и символы: «.», «-», «_» . При создании атрибута доступен выбор уровня или разряда.



Создание атрибута

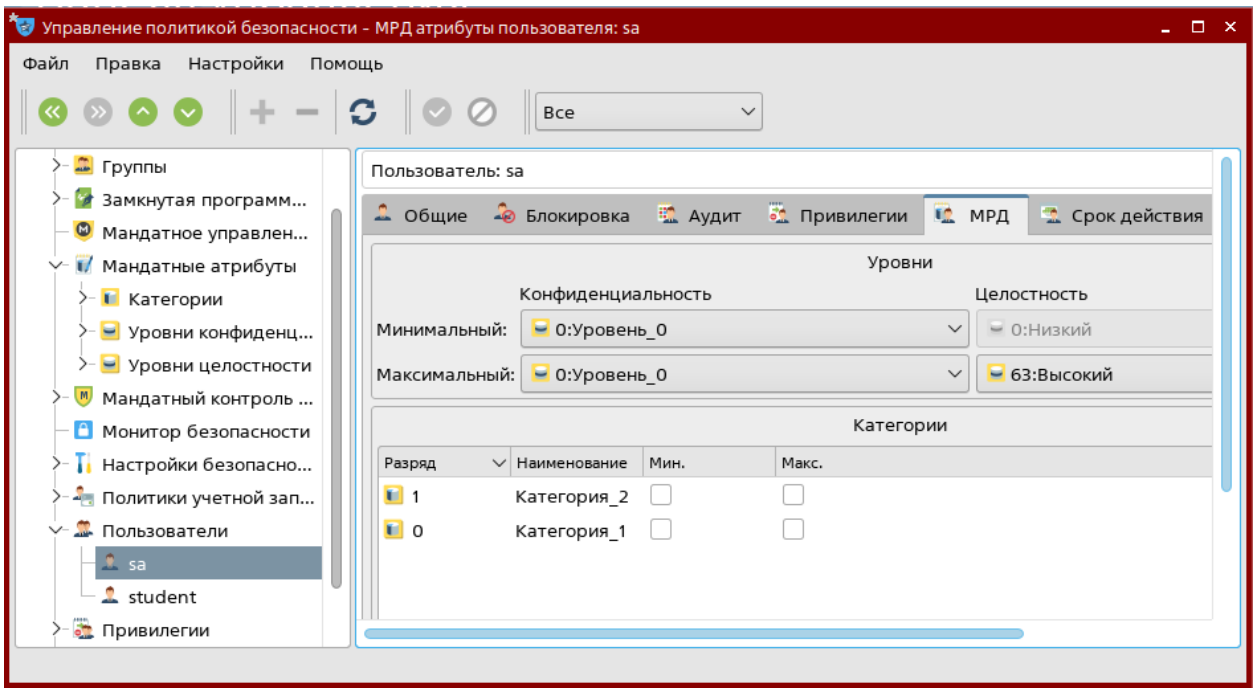
Если добавляется новый уровень конфиденциальности, то нужно:

- в скрипте `/usr/sbin/pdp-init-fs` установить значение переменной `sysmaxlev` равное новому максимальному значению уровня;
- выполнить скрипт `/usr/sbin/pdp-init-fs.`

Созданные атрибуты присваиваются в разделе Пользователи. Необходимо выбрать интересующего пользователя и перейти на вкладку МРД.

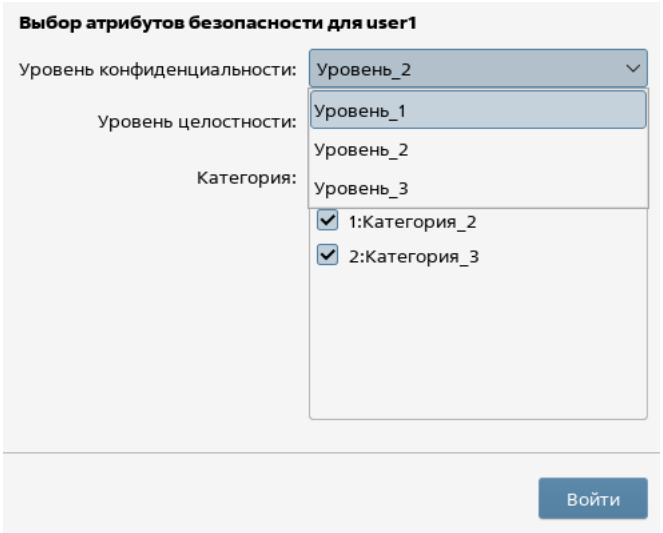
Для пользователя можно задать следующие мандатные атрибуты:

- в секции Конфиденциальность → минимальный и максимальный уровень конфиденциальности. Для этого следует в соответствующих выпадающих списках выбрать нужный уровень;
- в секции Целостность → максимальный уровень целостности. Для этого следует в выпадающем списке Максимальный выбрать нужный уровень. Минимальный уровень всегда равен 0;
- в секции Категории → допустимые категории. Для этого следует установить флаги в столбцах Мин. и Макс. соответствующих строк таблицы.



Настройка МРД пользователя

При авторизации пользователь выбирает уровни конфиденциальности и целостности, а также набор категорий. Категории, для которых установлен флаг Мин. будут выбраны всегда по умолчанию. Категории с флагом Макс. можно будет выбрать при авторизации.



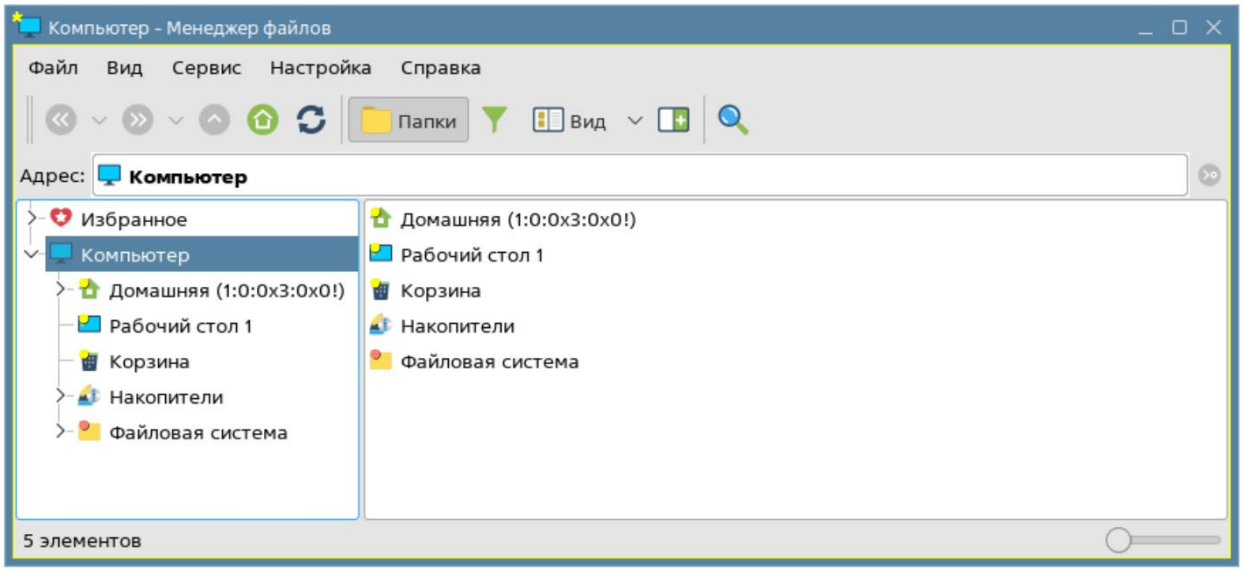
Выбор атрибутов безопасности

В интерфейсе системы предусмотрена цветовая индикация в зависимости от уровня конфиденциальности. Например, на первом уровне окна получат дополнительное жёлтое обрамление. Также файлы и каталоги, имеющие первый уровень конфиденциальности, будут иметь индикатор жёлтого цвета.

Цвета зарезервированы за каждым уровнем конфиденциальности. За нулевым уровнем закреплён голубой цвет. За вторым уровнем закреплён оранжевый цвет. За третьим — тёмно-розовый. За четвёртым — красный.

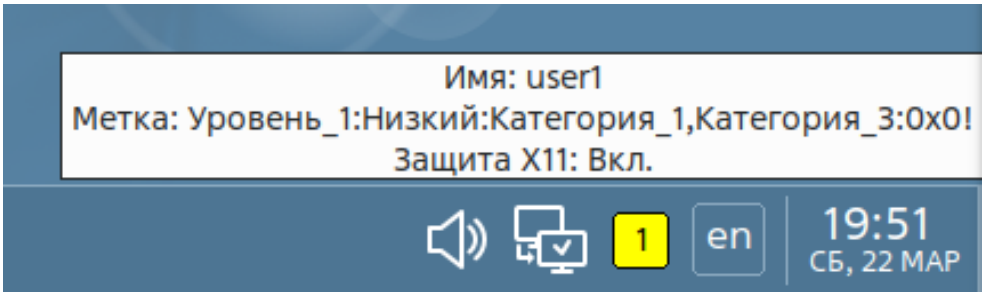
При работе на разных уровнях конфиденциальности и категориях пользователю следует учитывать, что ОС формально рассматривает одного и того же пользователя, но с

различными уровнями, как разных пользователей и создает для них отдельные домашние каталоги, одновременный прямой доступ пользователя к которым не допускается.



Обозначение уровня конфиденциальности

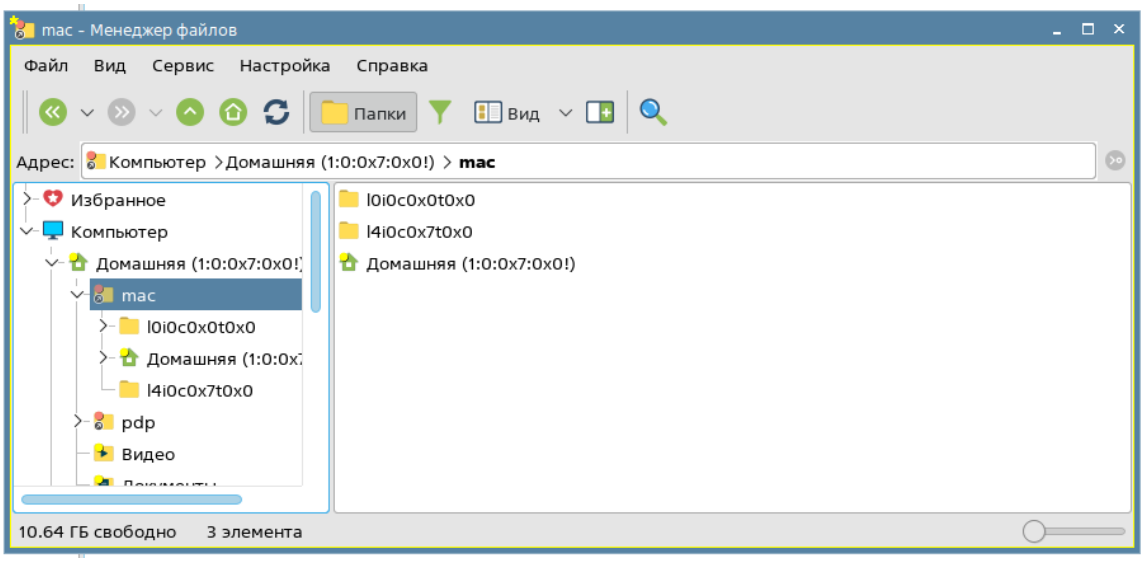
Текущий уровень конфиденциальности можно увидеть в виде значка на панели задач. Значок будет иметь цифру и цвет соответствующий уровню конфиденциальности. При наведении курсора отобразится дополнительная информация о текущем пользователе и его мандатной метке. Также можно нажать на него, и просмотреть эту информацию в окне.



Информация о текущем уровне конфиденциальности

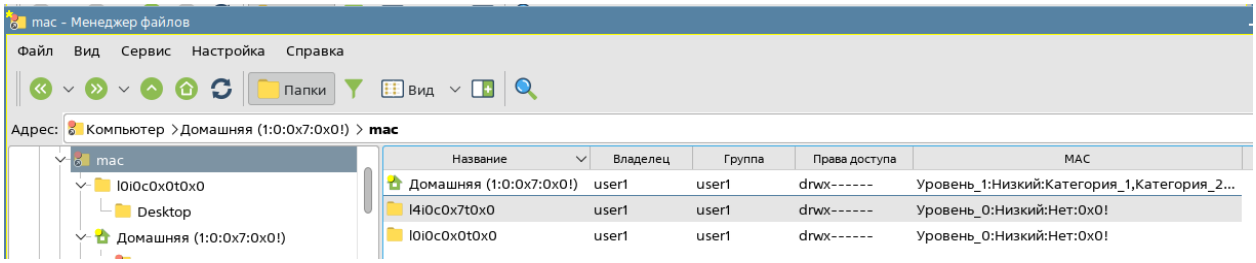
ОС формально рассматривает одного и того же пользователя, но с различными уровнями, как разных пользователей и создает для них отдельные домашние каталоги, одновременный прямой доступ пользователя к которым не допускается. Для каждой комбинации уровня целостности, конфиденциальности, категории и специальных атрибутов создаётся отдельный домашний каталог. Увидеть их (при наличии достаточных прав) можно в каталоге `mac`, расположенном в домашнем каталоге. В скобках закодирована комбинация атрибутов мандатной метки:

```
(Конфиденциальность: Целостность: Категории  Специальные атрибуты)
```



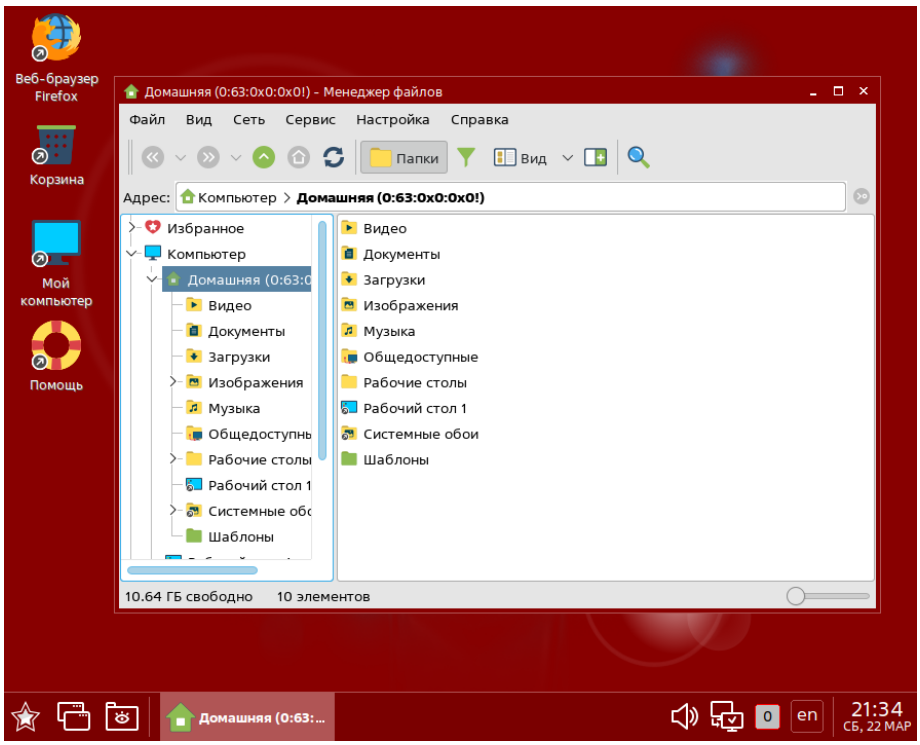
Комбинация атрибутов мандатной метки

Также, при просмотре каталогов в табличном виде, в столбце `MAC` эти атрибуты отображаются более подробно.



Подробные атрибуты

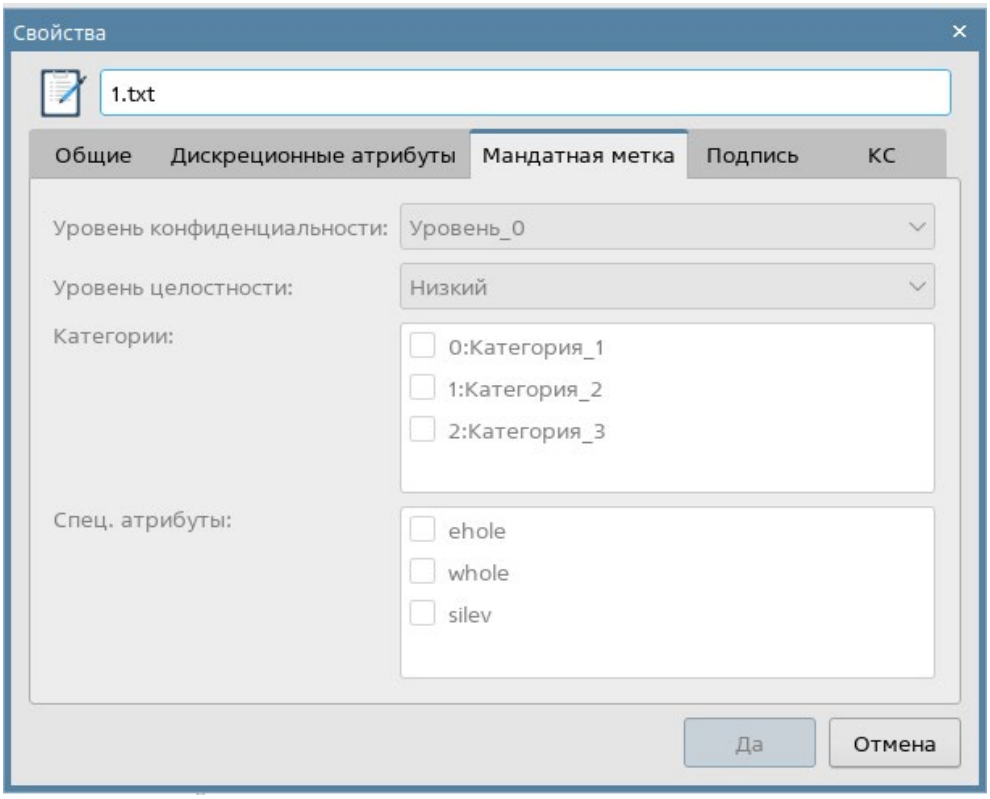
Интерфейс системы становится красным на высоком уровне целостности.



Высокий уровень целостности

Установка мандатной метки на файлы и каталоги

Для отображения мандатных атрибутов, установленных на файл или каталог, следует открыть его свойства, и перейти на вкладку Мандатная метка.



Просмотр мандатной метки

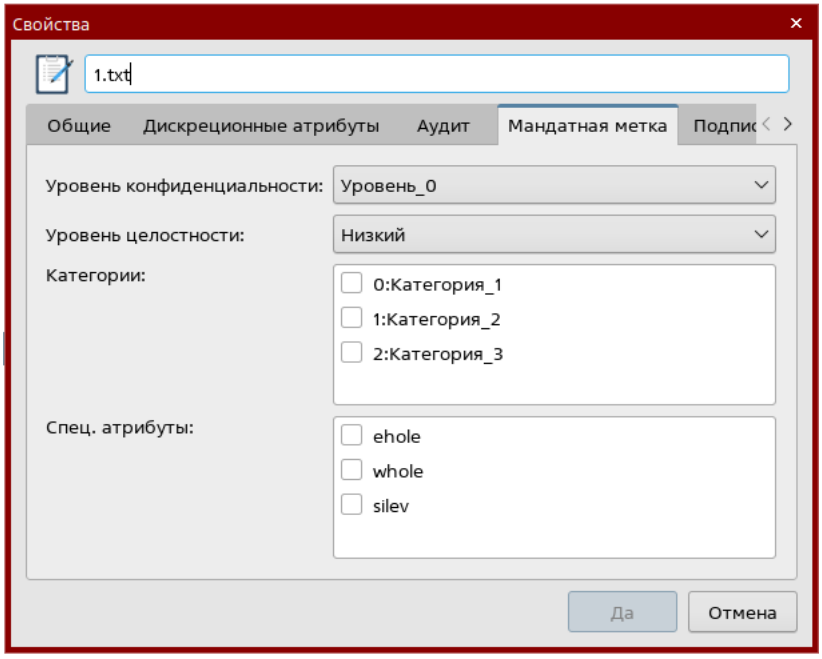
Мандатные атрибуты защищены от изменения.

При возникновении потребности, мандатные атрибуты всё же можно изменить. Для этого необходимо:

1. Авторизоваться под учётной записью `sa` с высоким уровнем целостности.
2. Запустить менеджер файлов от имени `root:`

```
sa@astra:~$ sudo -i
[sudo] пароль для sa:
root@astra:~# fly-fm
```

3.В этом случае поля на вкладке Мандатная метка файла `/home/user1/1.txt` станут доступны для изменения.



Доступные настройки мандатной метки

При создании файла или каталога ему присваиваются мандатные атрибуты, соответствующие текущей мандатной метке субъекта (пользователя или процесса).

Если субъект, имеющий, например, второй уровень конфиденциальности, скопирует себе объект, имеющий первый уровень, то скопированный объект автоматически получит второй уровень конфиденциальности. То есть, объект получит мандатные атрибуты субъекта.

Практические задания

Задание 1.

1. Войдите в ОС с учетной записью пользователя `sa` (`Уровень_0, Высокий`).

2. Запустите графическую утилиту редактирования учетных записей пользователей.

3. Создать 2 пользователя `user1, user2`. Для созданных учетных записей пользователей задайте максимальный уровень целостности.

4. Войдите в ОС с учетной записью пользователя `user2`, выбрав уровень доступа Уровень_0, Высокий.

5. Создайте в каталоге Документы файл `1.txt`, добавив в него любой текст.

6. Просмотрите уровень целостности, указанный в свойствах файла. Каким он оказался?

7 .Выйдите из ОС.

8. Войдите в ОС с учетной записью пользователя `sa` (Уровень_0, Высокий).

9. Проверьте, включен ли режим мандатного контроля целостности. В случае если режим мандатного контроля целостности не включен, включите. После включения режима для вступления изменений в силу требуется перезагрузка.

10. В графической утилите Политика безопасности выберите пункт `Мандатный контроль целостности → Режим эксперта → Редактирование конфига` добавьте строку, указав файл пользователя `user2` Файл `1.txt`, и установите для пользователя user2 уровень целостности максимальный. Перезагрузите ОС.

11. Войдите в ОС с учетной записью пользователя `user2`, выбрав уровень доступа `Уровень_0, Высокий`.

12. Попробуйте отредактировать файл `1.txt`, добавив в него любой текст. Получилось? Почему? Выйдите из ОС.

Задание 2.

1. Зайдите в систему под администратором. Запустите графическую утилиту Мандатное управление доступом с правами `root.`

2. Переименуйте уровни конфиденциальности:

• 0 - `for _all`;

• 1 - `secret`;

• 2 - `very_secret`;

• 3 - `very_important`.

3. Создайте учетную запись для пользователя `ivanov`:

• минимальный уровень конфиденциальности - `for_all`;

• максимальный уровень конфиденциальности - `very_secret`.

4. Создайте учетную запись для пользователя `petrov`:

• минимальный уровень конфиденциальности - `for_all`;

• максимальный уровень конфиденциальности – `secret`.

Задание 3.

1.Создайте каталог `/home/project`. Установите на каталог уровень конфиденциальности `very_important` и дополнительный атрибут `ccnr.`

2. Создайте каталог `/home/project/secret`. Установите на каталог уровень конфиденциальности secret.

3. Создайте каталог `/home/project/very_secret`. Установите на каталог уровень конфиденциальности `very _secret`.

4. Установите файловые списки управления доступом (ACL) и файловые списки управления доступом по умолчанию (default ACL) на каталоги `/home/project`, `/home/project/secret` и `/home/project/very_secret`, позволяющие пользователям `ivanov` и `petrov` создавать и удалять файлы в этих каталогах и изменять содержимое созданных файлов.

5.Зайдите в систему под учетной записью `ivanov` с уровнем конфиденциальности secret.

6. Создайте файл `file1.txt` в каталоге `/home/project/secret`. В этот файл добавьте строку ivanov. Сохраните файл. Удалось ли создать, изменить и сохранить файл `file1.txt`?

7.Виден ли каталог `/home/project/very _secret`?

8. Зайдите под учетной записью `ivanov` в систему с уровнем конфиденциальности `very_secret.`

9.Создайте файл `file2.txt` в каталоге `/home/project/very_secret`. В этот файл добавьте строку `ivanov`. Сохраните файл. Удалось ли создать, изменить и сохранить файл `file2.txt`?

10. Виден ли каталог `/home/project/secret`?

11. Виден ли файл `/home/project/secret/file1.txt`?

12. Добавьте в файл `/home/project/secret/file1.txt` строку `ivanov2`. Удалось ли изменить содержимое этого файла?

13. Зайдите в систему под учетной записью пользователем `petrov` с уровнем конфиденциальности `secret`.

14. Добавьте в файл `/home/project/secret/file1.txt` строку `petrov`. Удалось ли изменить содержимое этого файла?

15. Можете ли вы прочитать содержимое файла `/home/project/very _secret/fi le2.txt`?

Задание 4.

1.Создайте пользователей `user5, user6 и user7`.

2.Настройте графический киоск для пользователя `user5,` для этого:

• добавьте запуск следующих приложений: Веб-браузер Firefox, Офис Libreoffice, Почта Thunderblrd;

• поставьте галочки: Разрешить изменение внешнего вида и Разрешить создание и удаление файлов на рабочем столе;

• сохраните настройки;

3. Войдите в ОС под пользователем `user5` и протестируйте, какой функционал доступен:

• открываются ли приложения на Рабочем столе?

• можете ли вы создать файл или каталог на Рабочем столе?

4.Войдите в ОС под пользователем `sa` на высоком уровне целостности.

5. Добавьте еще один ярлык на рабочий стол пользователя user5, для этого:

• выберите меню `Пуск → Интернет→Веб-браузер Chromium→ПКМ→Отправить→ Рабочий стол;`

• скопируйте данный ярлык в профиль пользователя киоска user5 таким образом, чтобы у пользователя `user5` ярлык появился на рабочем столе. Путь для копирования: `/etc/fly-kiosk/user5/desktop`.

6. Войдите в ОС под пользователем `user5` и убедитесь, что пользователь теперь может запускать веб-браузер Chromium (ярлык появился на рабочем столе).

7. Войдите в ОС под пользователем `sa` на высоком уровне целостности и по аналогии с предыдущими пунктами задайте для пользователя user6 режим графического киоска с запуском одного приложения. В качестве приложения выберите веб-браузер Chromium.

8. После этого войдите в ОС под пользователем user6 и убедитесь, что запускается только одно приложение - веб-браузер Chromium. Закрыв браузер, выйдите из ОС.

9. Войдите в ОС под пользователем `sa` на высоком уровне целостности.

10 Настройте работу в системном киоске, для этого:

• откройте приложение `Пуск → Параметры → Панель управления →Безопасность → Системный киоск`;

• на верхней панели инструментов нажмите + и добавьте профиль для нового пользователя `user7`;

• выделив пользователя `user7` справа в окне Профили, выберите в качестве профиля пользователя everything;

• после этого включите режим киоска, выбрав в верхнем меню `Файл → Включить режим киоска`;

• во всплывающем сообщении Несохраненные изменения нажмите `Да`.

• в окне с требованием аутентификации введите пароль пользователя `sa` и нажмите `Да`.

11. Войдите в ОС под пользователем `user7` и убедитесь, что пользователю доступен стандартный функционал системы (откройте браузер, создайте файлы на рабочем столе и в домашнем каталоге, откройте любое доступное приложение из меню Пуск).

Вопросы

1. Что реализуют политики мандатного контроля целостности?
2. Какой уровень целостности является минимальным?
3. Какой уровень целостности присваивается привилегированному пользователю?
4. Для чего предназначен режим графического киоска в Astra Linux?
5. В какой программе настраивается графический киоск?
6. Для чего предназначен системный киоск?
7. От чего зависит цветовая индикация интерфейса?
8. На что влияет установка минимальной категории конфиденциальности пользователя?
9. На каком уровне защищённости доступно редактирование мандатных атрибутов?
10. Как изменить мандатные атрибуты объекта?
11. Что может сделать субъект имеющий первый уровень конфиденциальности с объектом, имеющим второй уровень?