1. 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.

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.

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.

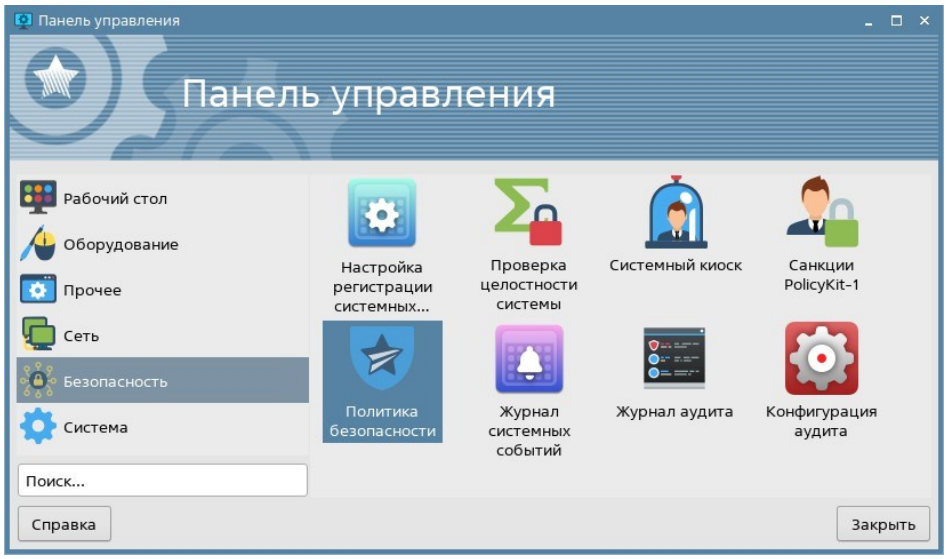
Начиная с оперативного обновления 1.7.2 добавлены дополнительные атрибуты:

- 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,

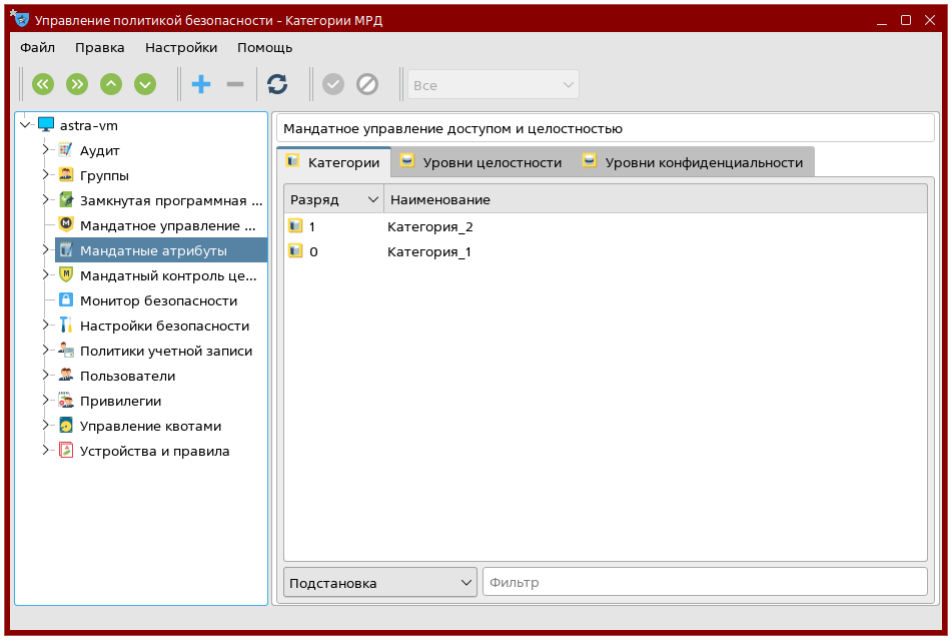
для корректного запуска файла/usr/bin/passwd, имеющего высокий уровень целостности, пользователем с низким уровнем целостности.

2. Определение мандатных уровней для учётных записей

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



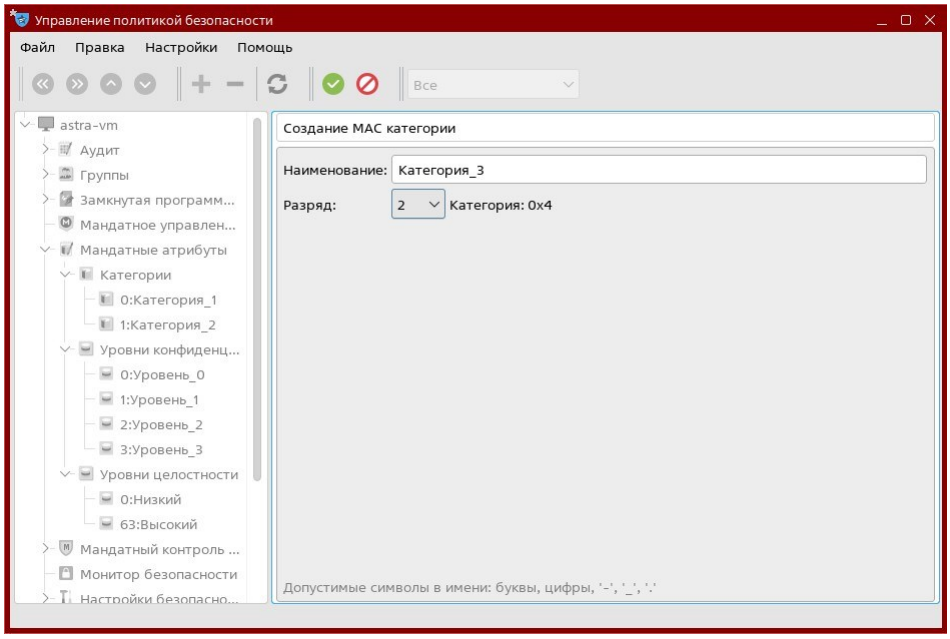
Управление мандатными атрибутами выполняется в соответствующем разделе. Этот раздел доступен только на максимальном уровне защищённости (Смоленск).



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.



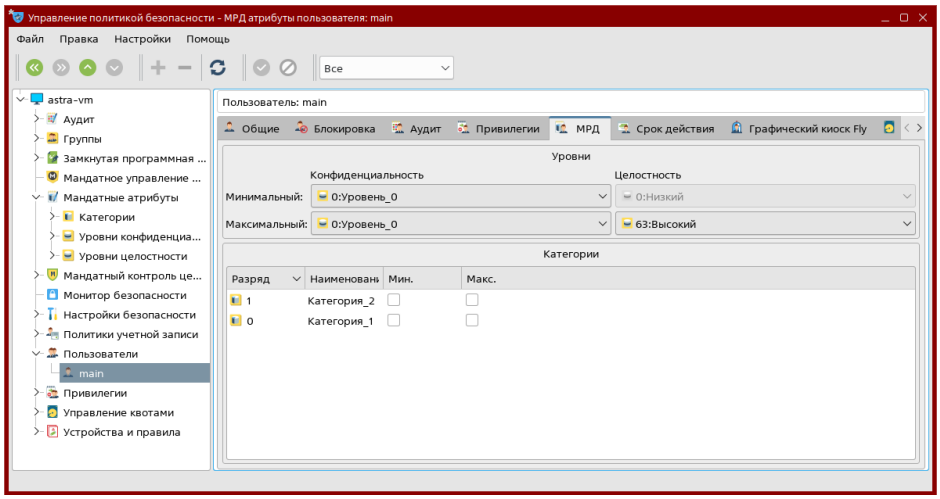
Если добавляется новый уровень конфиденциальности, то нужно:

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

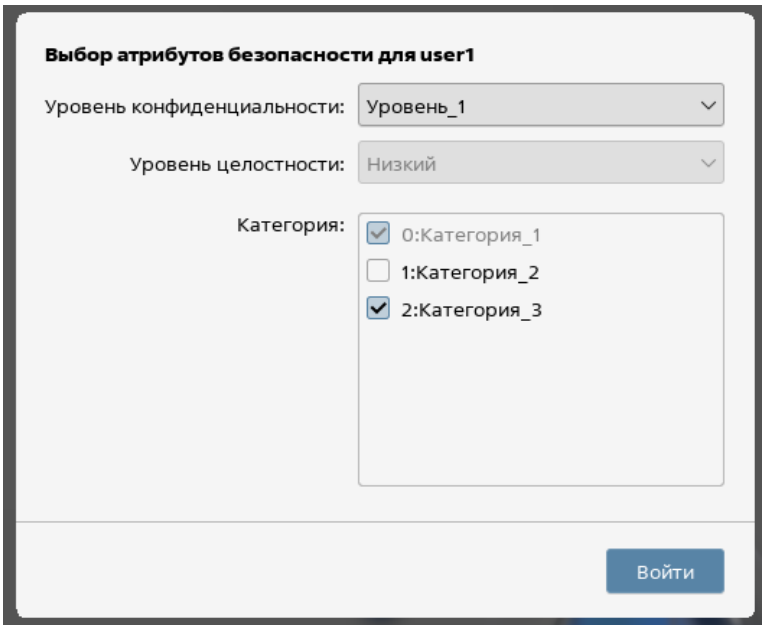
Созданные атрибуты присваиваются в разделе **Пользователи**. Необходимо выбрать интересующего пользователя и перейти на вкладку МРД.

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.



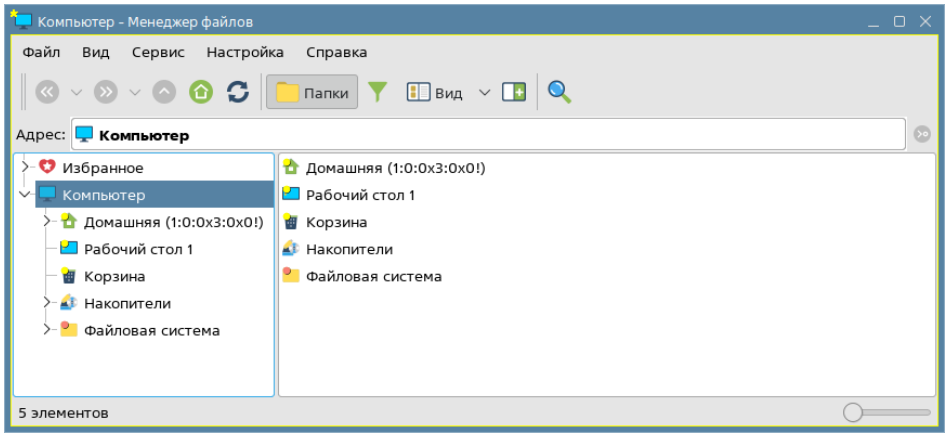
При авторизации пользователь выбирает уровни конфиденциальности и целостности, а также набор категорий. Категории, для которых установлен флаг Мин. будут выбраны всегда по умолчанию. Категории с флагом Макс. можно будет выбрать при авторизации.



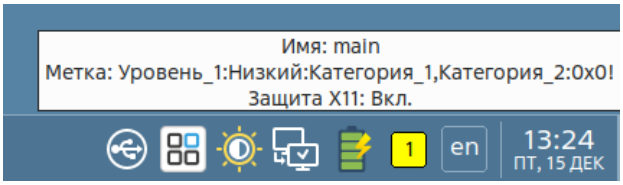
В интерфейсе системы предусмотрена цветовая индикация в зависимости от уровня конфиденциальности. Например, на первом уровне окна получат дополнительное жёлтое обрамление. Также файлы и каталоги, имеющие первый уровень конфиденциальности, будут иметь индикатор жёлтого цвета.

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.

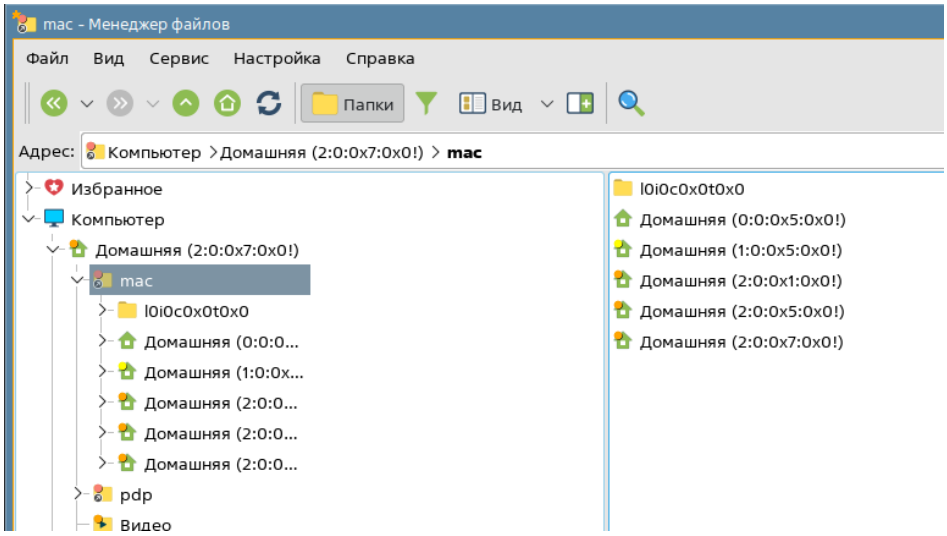


Текущий уровень конфиденциальности можно увидеть в виде значка на панели задач. Значок будет иметь цифру и цвет соответствующий уровню конфиденциальности. При наведении курсора отобразится дополнительная информация о текущем пользователе и его мандатной метке. Также можно нажать на него, и просмотреть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



Для каждой комбинации уровня целостности, конфиденциальности, категории и специальных атрибутов создаётся отдельный домашний каталог. Увидеть их (при наличии достаточных прав) можно каталоге mac, расположенный в домашнем каталоге. В скобках закодирована комбинация атрибутов мандатной метки:

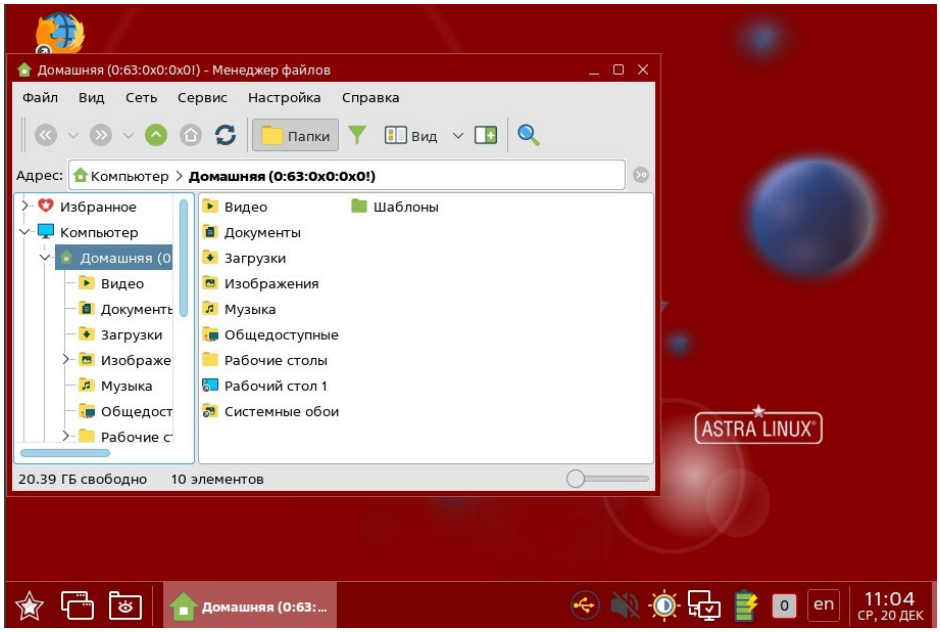
(Конфиденциальность : Целостность : Категории : Специальные атрибуты)



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

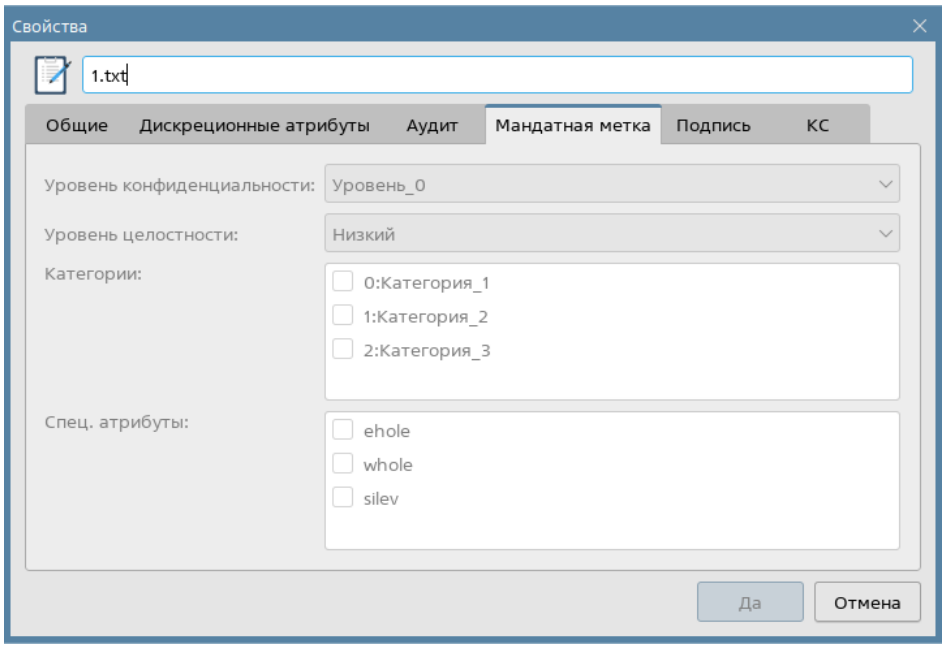
Название	Владелец	Права доступа	МАС
l0i0c0x0t0x0	user1	drwx------	Уровень_0:Низкий:Нет:0x0!
Домашняя (0:0:0x5:0x0!)	user1	drwx------	Уровень_0:Низкий:Категория_1,Категория_3:0x0!
Домашняя (1:0:0x5:0x0!)	user1	drwx------	Уровень_1:Низкий:Категория_1,Категория_3:0x0!
Домашняя (2:0:0x1:0x0!)	user1	drwx------	Уровень_2:Низкий:Категория_1:0x0!
Домашняя (2:0:0x5:0x0!)	user1	drwx------	Уровень_2:Низкий:Категория_1,Категория_3:0x0!
Домашняя (2:0:0x7:0x0!)	user1	drwx------	Уровень_2:Низкий:Категория_1,Категория_2,Категория_3:0x0!

Интерфейс системы становится красным на высоком уровне целостности.



3. 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.

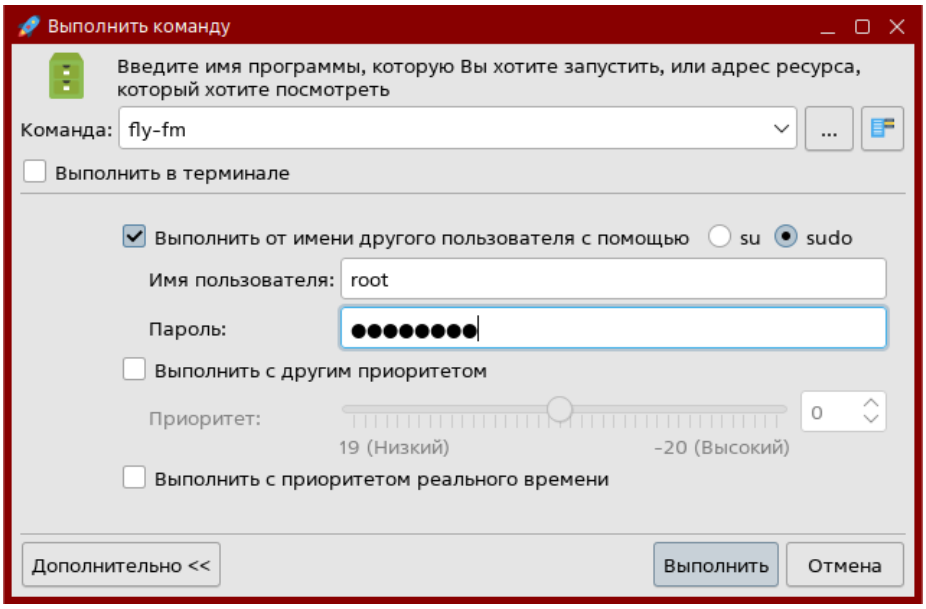


Мандатные атрибуты защищены от изменения.

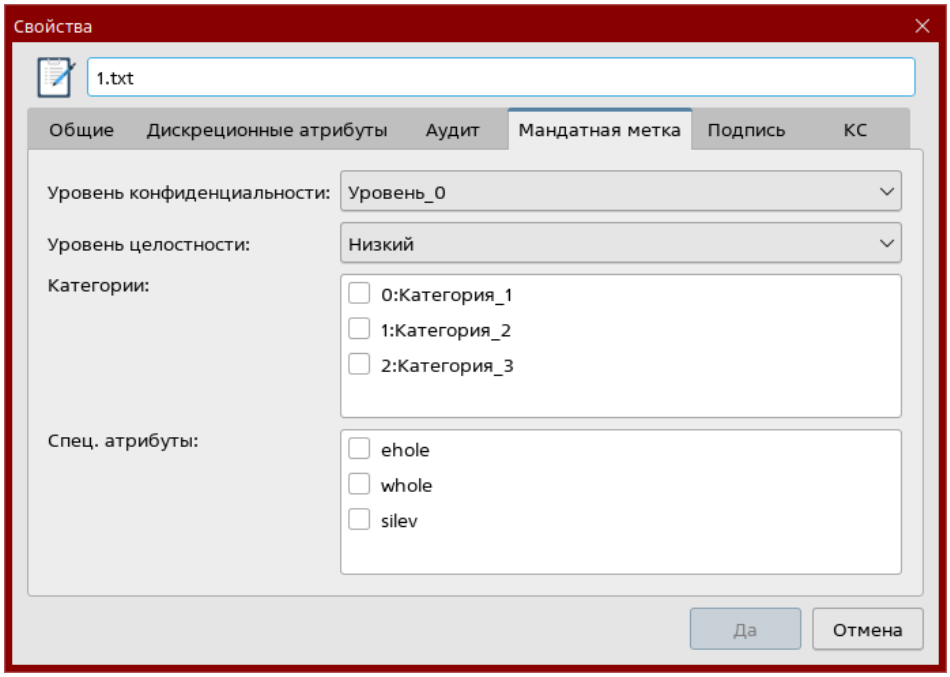
При возникновении потребности, мандатные атрибуты всё же можно изменить. Для этого необходимо:

☐. Авторизоваться под учётной записью администратора (пользователь, состоящий в группе astra-admin) с **высоким** уровнем целостности.

☐. Запустить менеджер файлов от имени root.



В этом случае поля на вкладке Мандатная метка станут доступны для изменения.



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.