ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник С. Войцеховский

(воинское звание, подпись, инициал имени, фамилия)

«___» _____ 2022 г.

Автор: доцент 24 кафедры к.т.н. подполковник С. Краснов

(должность, ученая степень, ученое и воинское звание, инициал имени, фамилия)

Задание на практическое занятие №13

Тема: Мандатное управление доступом в операционной системе специального назначения «Astra Linux Special Edition»

(наименование темы семинара, лабораторной работы, практического занятия и других видов учебных занятий по тематическому плану изучения дисциплины)

Обсуждено и одобрено на заседании кафедры

(предметно-методической комиссии)

«____» _____ 20__ г.

протокол № _____

Санкт-Петербург

2022

Перечень заданий:

Обучающийся должен на практическом занятии выполнить индивидуальное задание определенное преподавателем из списка индивидуальных заданий. 1.

Мандатное управление доступом в операционной системе специального назначения «Astra Linux Special Edition»

Цель работы: освоить администрирование основных параметров мандатного управления доступом в ОССН, в том числе к объектам файловых систем с применением графических утилит и консольных команд.

Материально-техническое обеспечение: ОС Astra Linux Special Edition 1.6 (Версия Смоленск, пользователь leti пароль 11111111) с установленным оперативным обновлением 20211126SE16.iso (оперативное обновление №10).

При установке ОССН (по умолчанию) задаются следующие параметры мандатного управления доступом и мандатного контроля целостности:

непосредственно используемых уровня целостности («Низкий» значение 0, «Высокий» – 63);

Для выполнения работы необходима установленная ОССН версии 1.6, в которой создана учётная запись пользователя user (учетная запись создается индивидуально по фамилии обучающегося латиницей), с параметрами: максимальный и минимальный уровни доступа – 0, неиерархические категории – нет, уровень целостности – «Высокий», входит в группу администраторов – astra-admin (вторичная группа), разрешено выполнение привилегированных команд (sudo).

Начать работу со входа в ОССН в графическом режиме с учётной записью пользователя user (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Высокий»).

Краткие теоретические сведения

Для доступа и настроек систем разграничения доступа в ОС существует специальная библиотека как с консольным, так и графическим управлением.

В данном практическом занятии мы будем использовать графическую утилиту fly-admin-smc (рис. 1).

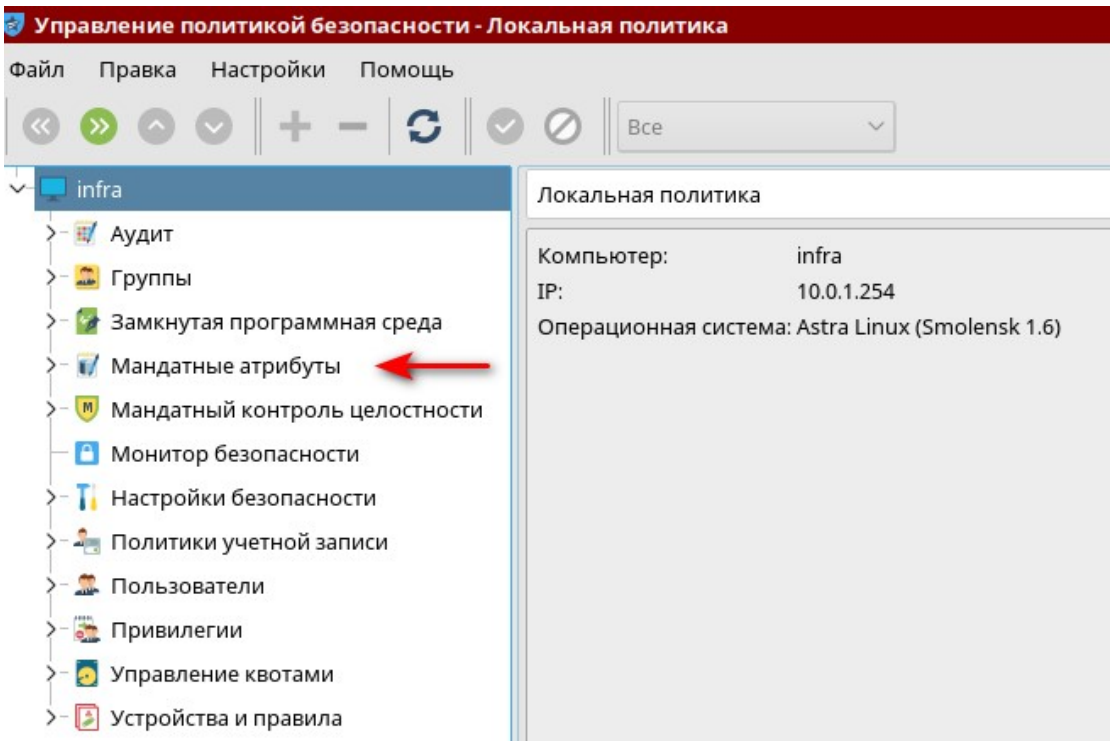

Рис. 1. Панель управления политикой безопасности

Перед началом работы с мандатным управлением доступом необходимо задать мандатные атрибуты. Найдите вкладку «Мандатные атрибуты» и активируйте ее (рис. 2). Для настройки будет использовать только вкладки «Категории» и «Уровни конфиденциальности» в правом окне. Вкладка «Уровни целостности» не будет применяться.

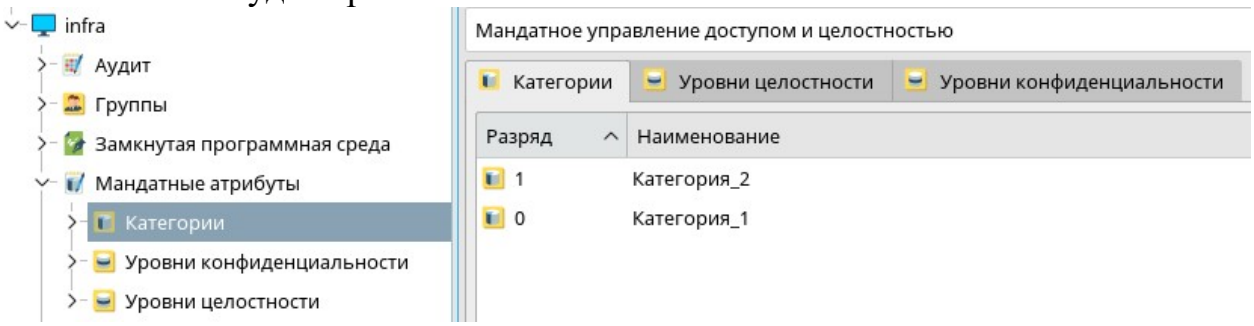

Рис. 2. Мандатные атрибуты

При помощи командной строки мы можем просмотреть файлы, хранящие информацию о настройках мандатного управления доступом.

Файл /etc/parsec/max_levels хранит информацию об уровнях конфиденциальности (рис. 3). В приведенном примере видны уровни конфиденциальности, заданные по умолчанию, до настройки системы.

```
root@infra:~# cat /etc/parsec/mac_levels
#levels
Уровень_0:0
Уровень_1:1
Уровень_2:2
Уровень_3:3
```

Рис. 3. Содержимое файла /etc/parsec/max_levels

Файл /etc/parsec/mac_categories хранит информацию о категориях конфеденциальности (рис. 4). В приведенном примере видны категории конфиденциальности, заданные по умолчанию, до настройки системы.

```
root@infra:~# cat /etc/parsec/mac_categories
#categories
Нет:0
Категория_1:1
Категория_2:2root@infra:~#
```

Рис. 4. Содержимое файла /etc/parsec/max_ categories

До настроек системы уровень конфиденциальности, отображаемый в трее ОС равен 0 (рис. 5).

Рис. 5. Содержимое трея ОС

Каждому уровню конфиденциальности в рабочем столе fly соответствует определенный цвет, являющийся индикатором мандатного уровня (рис. 6).

Рис. 6. Индикаторы мандатного уровня

Например, обратите внимание на абрис активного акта панели управления политикой безопасности. Она имеет синий индикатор, что визуализирует то, что мы работаем на уровне конфиденциальности равном 0 (рис. 7).

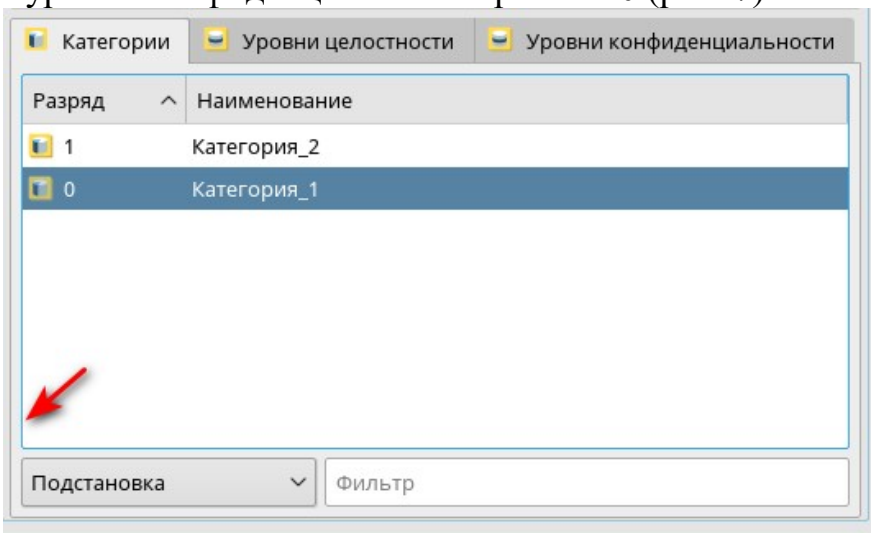

Рис. 7. Абрис активного акта панели управления политикой безопасности на уровне конфиденциальности 0

Все объекты в ОС располагаются иерархично в контейнерах. Иерархия строится по уровню доступа. Т.е. каталог является контейнером для файлов, база данных является контейнером для записей и уровень конфиденциальности контейнера не может быть меньше уровня конфиденциальности объектов, которые в нем содержаться (рис. 4).

Создадим трех пользователей ОС, например, student1, student2, student3.

Для в этого в окне панели управления политикой безопасности выберем вкладку «Пользователи» и нажмем знак «+» (рис. 8)

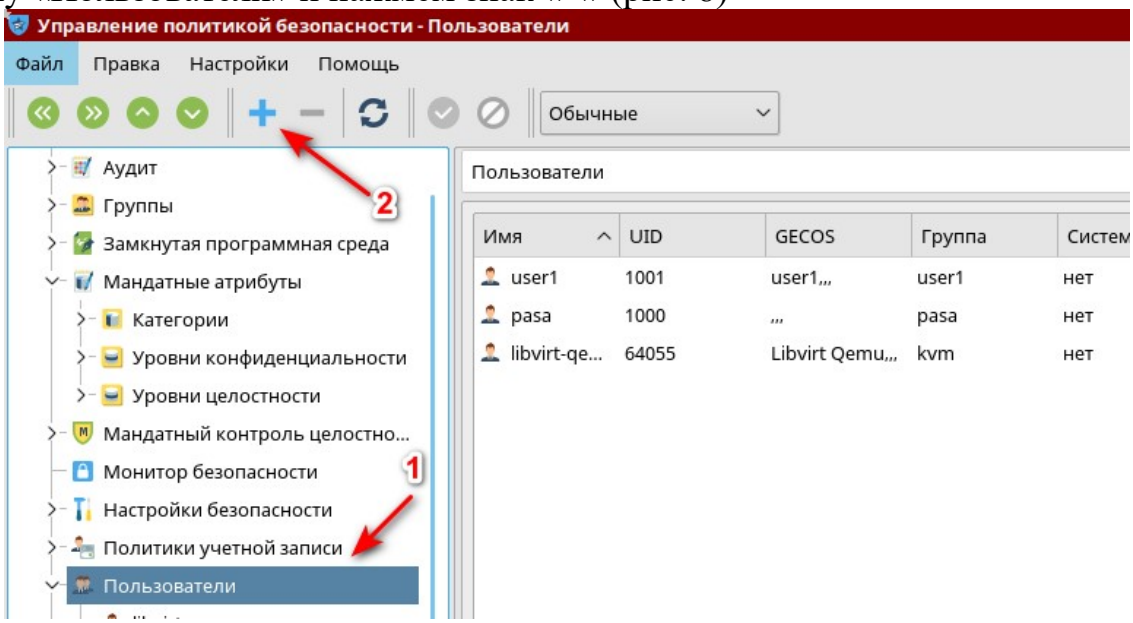

Рис. 7. Создание нового пользователя в ОС

Первого пользователя student1 создадим и назначим ему привилегии администратора системы и с высоким уровнем целостности (подобное решение не применяется на практике из-за явных предпосылок к нарушению информационной безопасности и сделано только для наглядного примера в данном практическом задании для удобства просмотра настроек). Для этого необходимо добавить его в две группы: astra-admin и astra-console.

Сначала добавим пользователя в группу astra-admin (рис. 8).

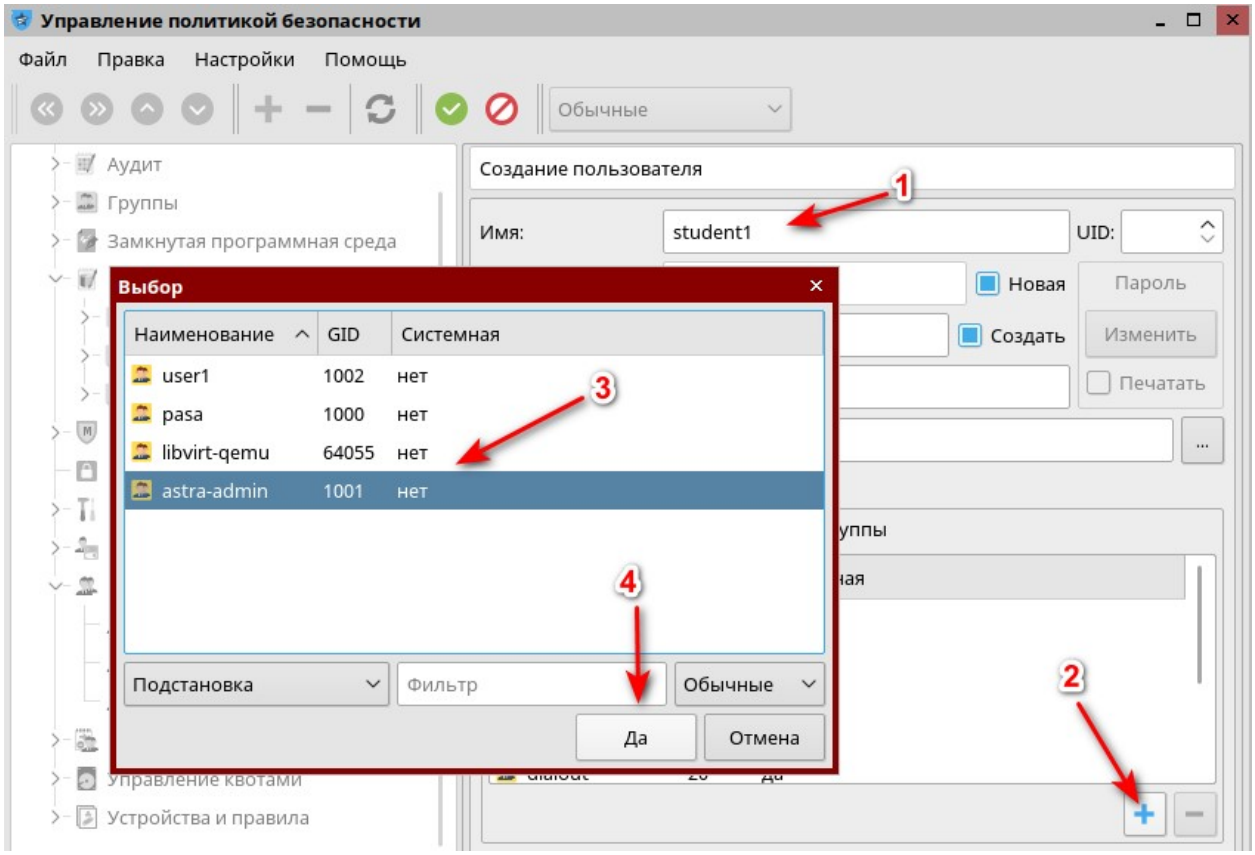

Рис. 8. Добавление пользователя student1 в группу astra-admin

Затем добавим пользователя в группу astra-console (рис. 8). Группа astra-console является системной, поэтому необходимо выбрать ее среди системных групп (рис. 9). Остальные настройки оставляем без изменений и нажимаем «ОК» (зеленая галочка). Далее задайте пароль для пользователя (не забудьте записать его в блокнот!!!). Установите пользователю высокий уровень целостности.

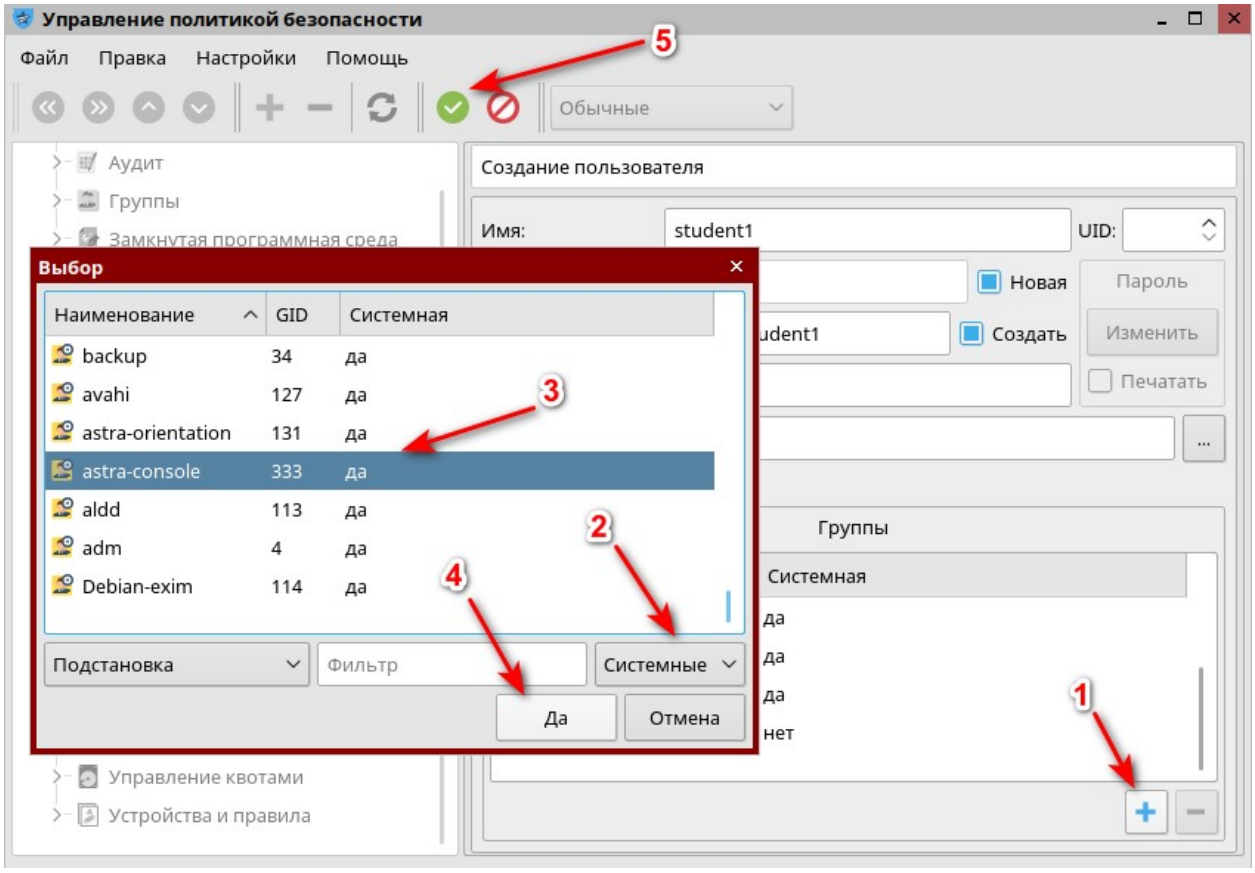

Рис. 9. Добавление пользователя student1 в группу astra-console

Пользователей student2 и student3 создаем без добавления их в какие-либо группы. Задаем пароли для пользователей.

Настроим уровни конфиденциальности. Начнем с уровня 0 (рис. 10).

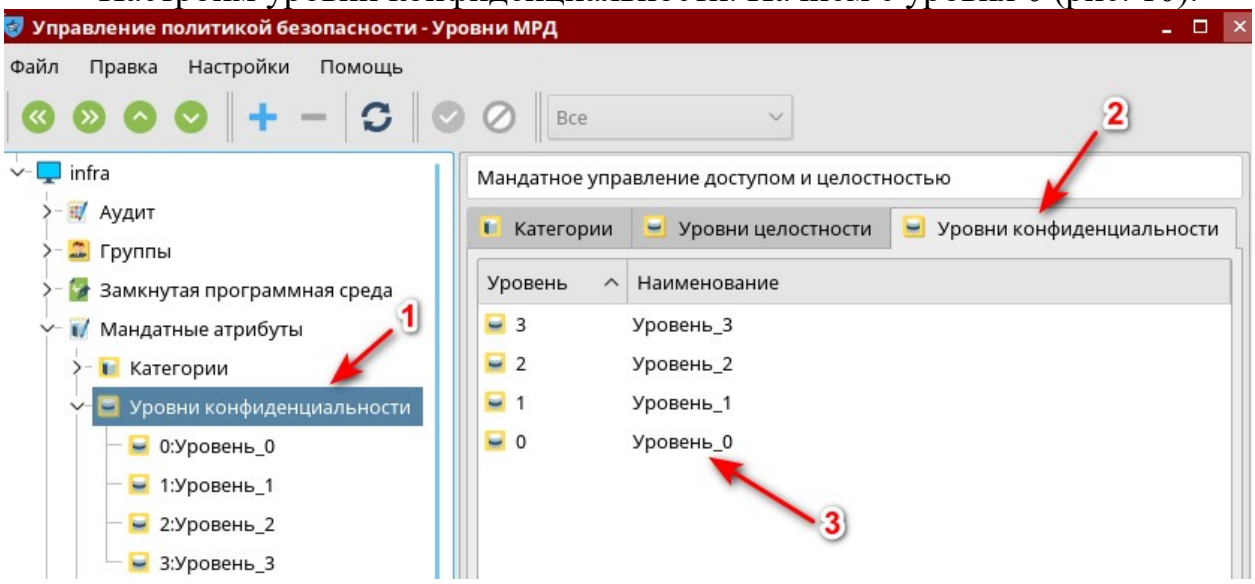

Рис. 10. Настройка уровней конфиденциальности

Уровню 0 присвоим буквенное значение «Несекретно» (рис.11).

ВАЖНО! При переименовании уровней нельзя использовать пробелы в названии. Используйте, при необходимости, символ нижнего подчеркивания.

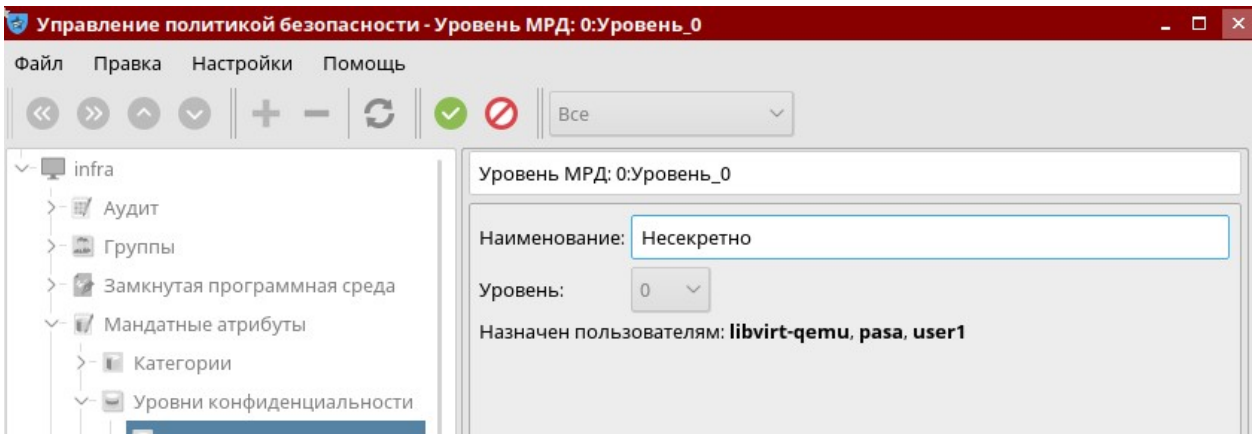

Рис. 11. Настройка уровня конфиденциальности «Несекретно

Переименуем оставшиеся уровни в ДСП, Секретно, Сов_секретно. Результат должен получиться как на рис. 12. После завершения настройки уровни конфиденциальности могут назначаться пользователям. В случае необходимости, можно расширить список уровней до 255. Однако, для создания уровня выше 4 необходимо провести дополнительные настройки в системе. Также, уровни можно удалять или переименовывать.

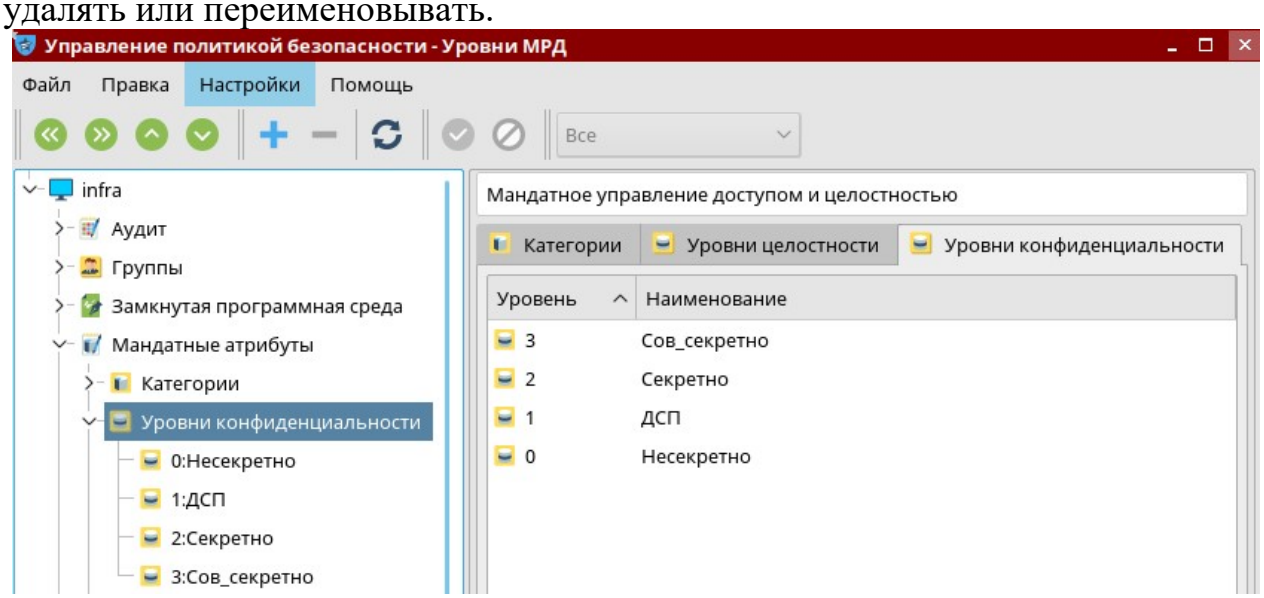

Рис. 12. Переименованные уровни конфиденциальности

Если уровень конфиденциальности процесса выше, чем уровень конфиденциальности файла, то доступ разрешается только на чтение и исполнение (для каталогов – получение содержимого и вход в каталог) (рис. 13). Если уровень конфиденциальности процесса ниже, чем уровень конфиденциальности файла, то доступ разрешается только на запись. Если уровни конфиденциальности процесса и файла несравнимы, то доступ запрещается полностью.

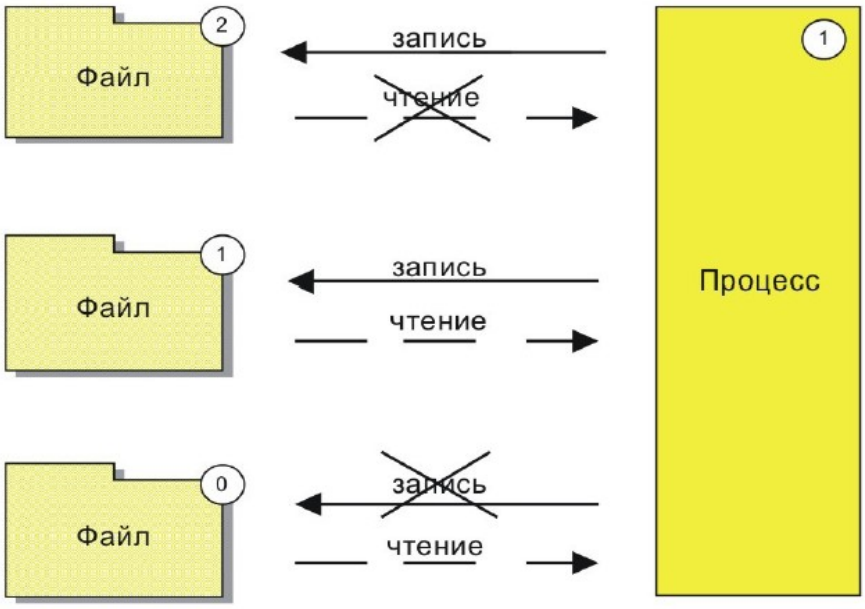

Рис. 13. Правила доступа процессов к файлам (иерархические уровни)

Перейдем к настройке категорий. Как уже рассматривалось в курсе лекций, категории нужны для того, чтобы разделить обрабатываемую информацию по организационным единицам. При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить. В ВС РФ это могут быть, например, различные рода войск, такие как ВКС, ВМФ, СВ. В гражданских организациях это могут быть, например, различные отделы на предприятии (рис. 14). Если мандатные метки процесса и файла равны, то доступ разрешается полностью – по чтению, записи и исполнению. Категориям приписываются пользователи и права доступа; можно считать, что они (категории) именуют отношения «многие ко многим» между пользователями и правами. Категории могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким категориям. Во время сеанса работы пользователя активизируется подмножество категорий, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным к атегориям. Одновременно пользователь может открыть несколько сеансов.

Категорию можно выбирать при входе в систему.

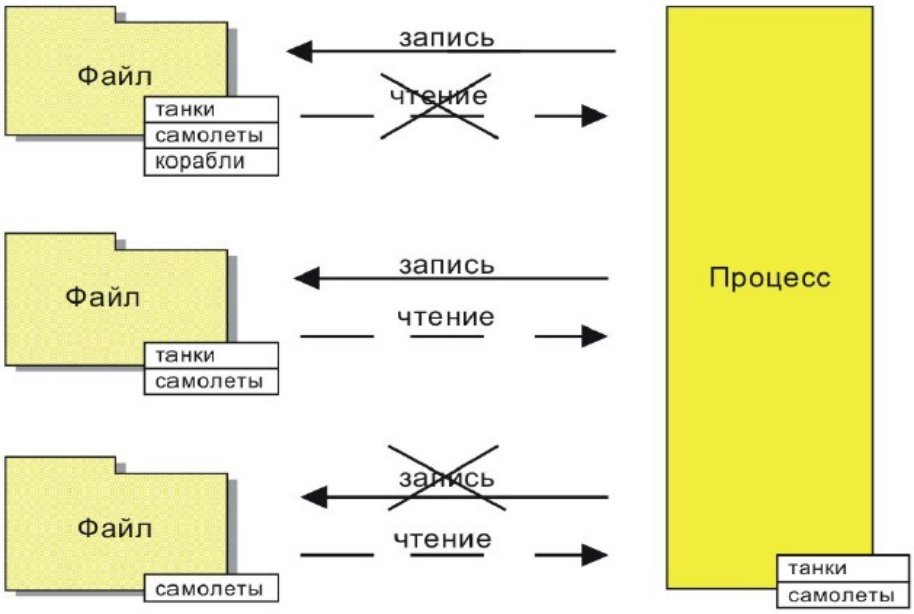

Рис. 14. Правила доступа процессов к файлам (неиерархические категории)

Создайте три категории «Танки», «Корабли», «Самолеты» как на рис. 15, переименовав для этого две имеющиеся в системе категории и создав одну новую.

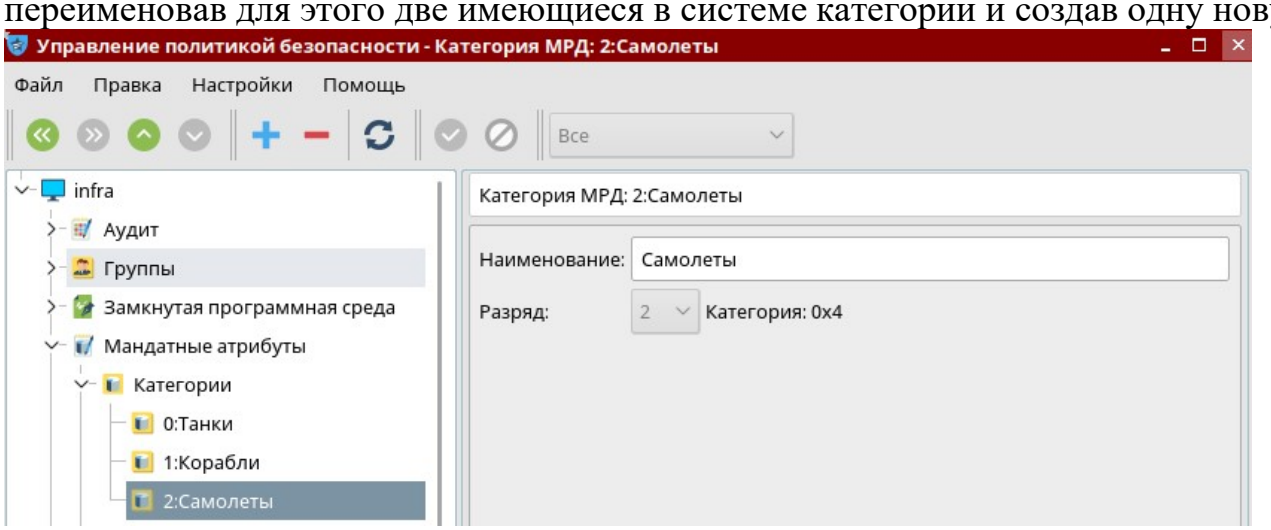

Рис. 15. Создание категорий «Танки», «Корабли» и «Самолеты»

Теперь можно назначить категории пользователям. Для назначения категории необходимо выбрать нужного пользователя на вкладке «Пользователи» и далее выбрать вкладку «МРД». Один пользователь, как уже было сказано выше, может быть приписан нескольким категориям (рис. 16).

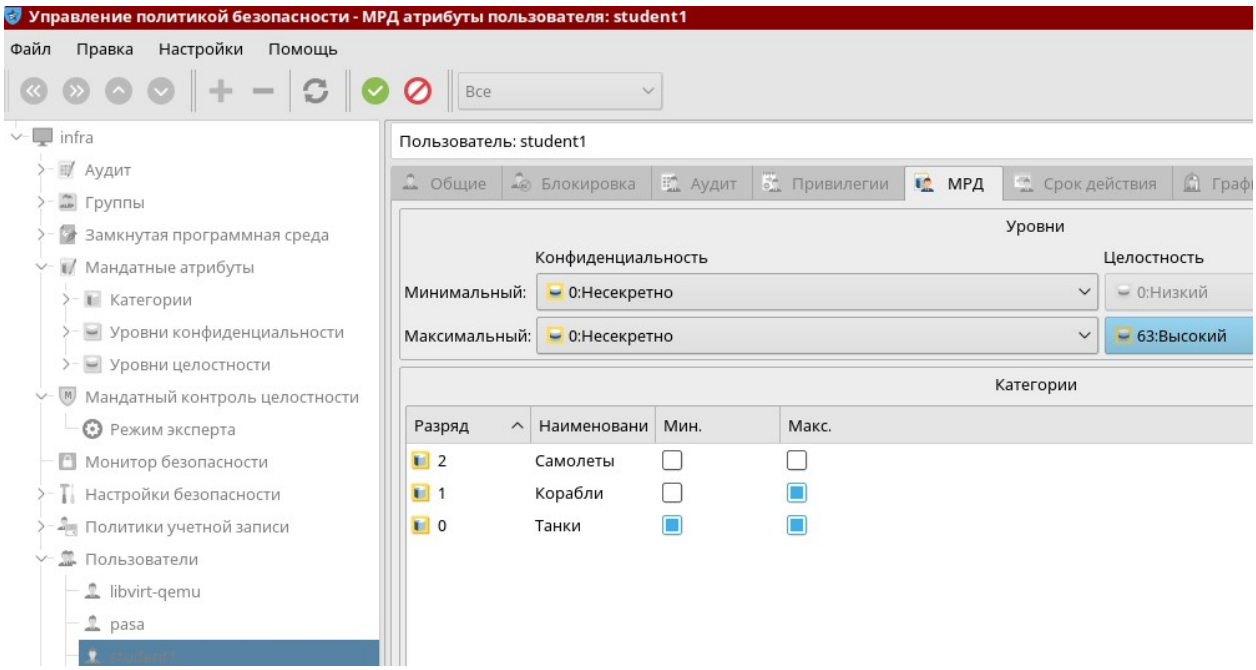

Рис. 16. Назначение категорий пользователю student1

При назначении категории есть выбор между минимальным и максимальным уровнем. При назначении только максимального уровня пользователю, он при входе в систему будет иметь возможность выбора категории (будет ли он работать с документами этой категории). При назначении минимального уровня, такой выбор пользователю предоставлен не будет. Так, например, при назначении категорий как на рис. 16 пользователь student1 при входе в систему может выбрать или не выбрать категорию «Корабли», но однозначно войдет с назначенной категорией «Танки» (рис. 17).

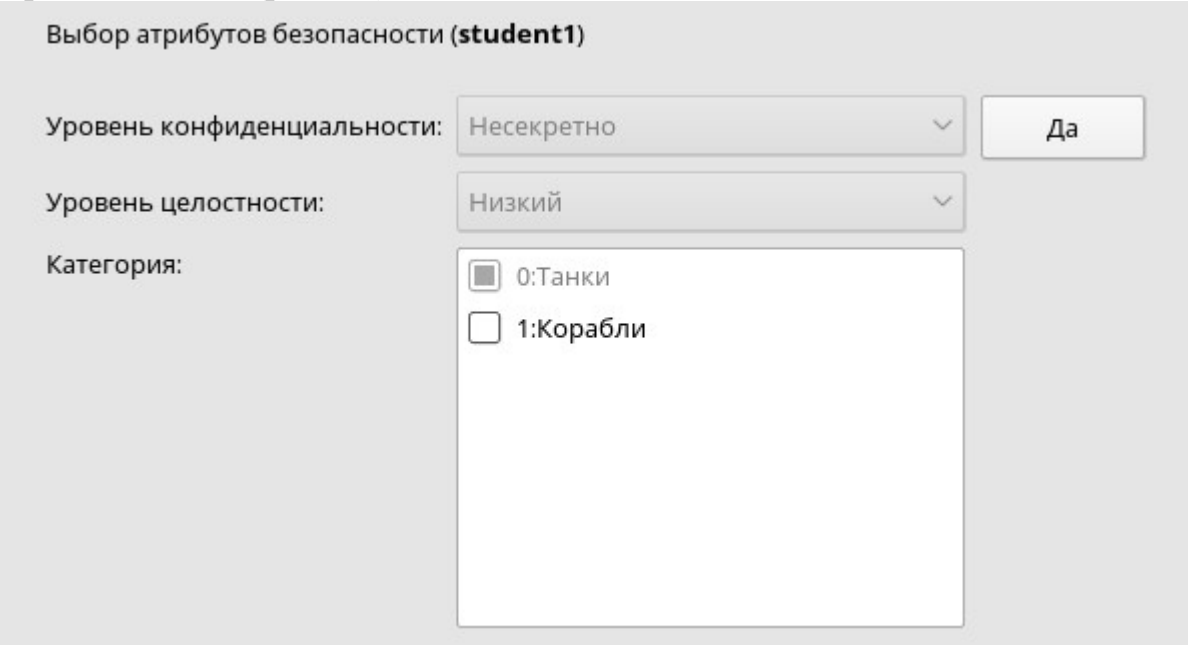

Рис. 17. Назначение категорий пользователю student1 при входе

Настроим МРД для трех учетных записей. Для учетной записи student1 установим максимальный уровень конфиденциальности «Сов_секретно»,

категории «Самолеты» уровень Макс., категория «Танки» уровень Мин. Не забудьте установить высокий уровень целостности для пользователя (рис.18).

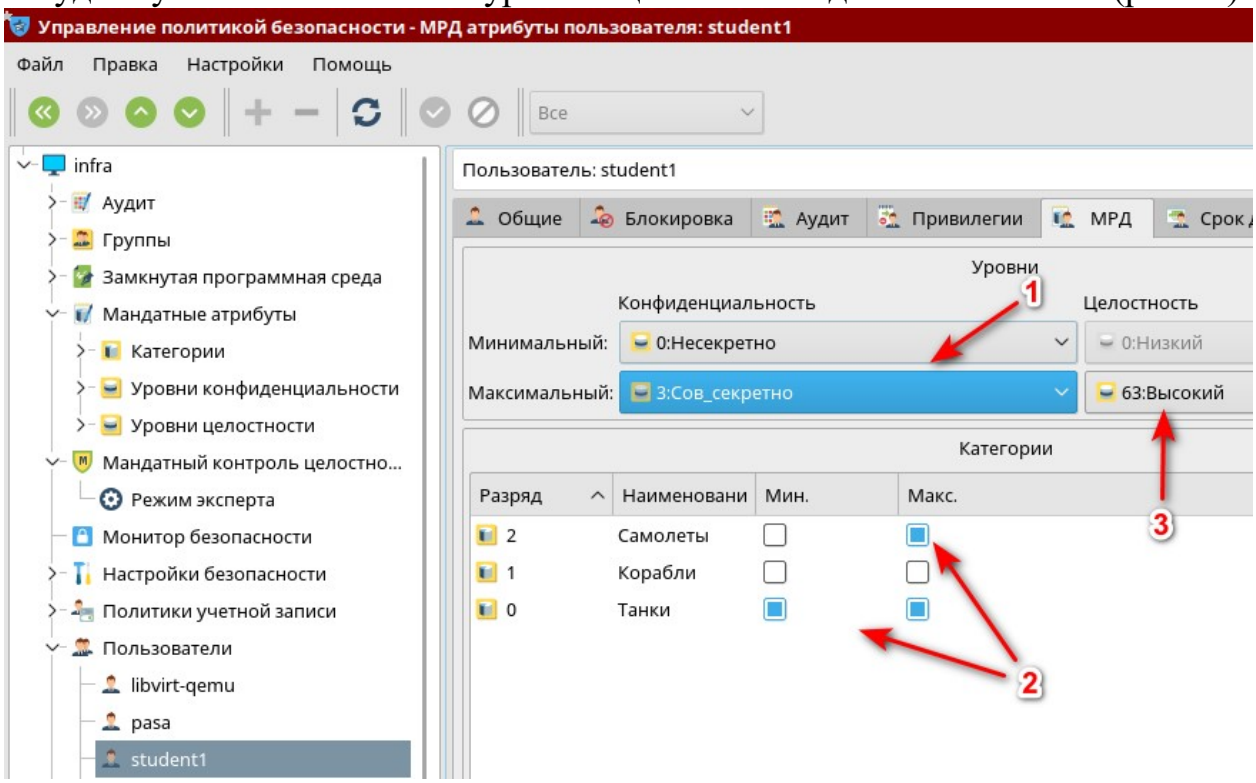

Рис. 18. Настройки мандатных атрибутов для пользователя student1

Далее пробуем зайти под данной учетной записью на всех уровнях конфиденциальности, МКЦ и категориях по очереди (**кроме УК Секретно**). Это важно, так как при входе пользователя на каждом уровне секретности будут созданы его домашние каталоги с соответствующими уровню мандатного доступа. И это будут разные каталоги соответственно. Уровень конфиденциальности Секретно оставим нетронутым для дальнейшей практики. Будьте предельно внимательны и аккуратны.

Необходимые комбинации для входа в систему:
УК несекретно, МКЦ низкий, категория только Танки;
УК несекретно, МКЦ высокий, категория только Танки;
УК несекретно, МКЦ низкий, категория только Танки и Самолеты;
УК несекретно, МКЦ высокий, категория только Танки и Самолеты;

УК ДСП, МКЦ низкий, категория только Танки;
УК ДСП, МКЦ высокий, категория только Танки;
УК ДСП, МКЦ низкий, категория только Танки и Самолеты;
УК ДСП, МКЦ высокий, категория только Танки и Самолеты;

УК Сов_секретно, МКЦ низкий, категория только Танки;
УК Сов_секретно, МКЦ высокий, категория только Танки;
УК Сов_секретно, МКЦ низкий, категория только Танки и Самолеты;
УК Сов_секретно, МКЦ высокий, категория только Танки и Самолеты;

Итого мы поочерёдно совершили 12 входов в систему. Обратите внимание, как выглядит интерфейс ОС при УК Сов_секретно, МКЦ низкий.

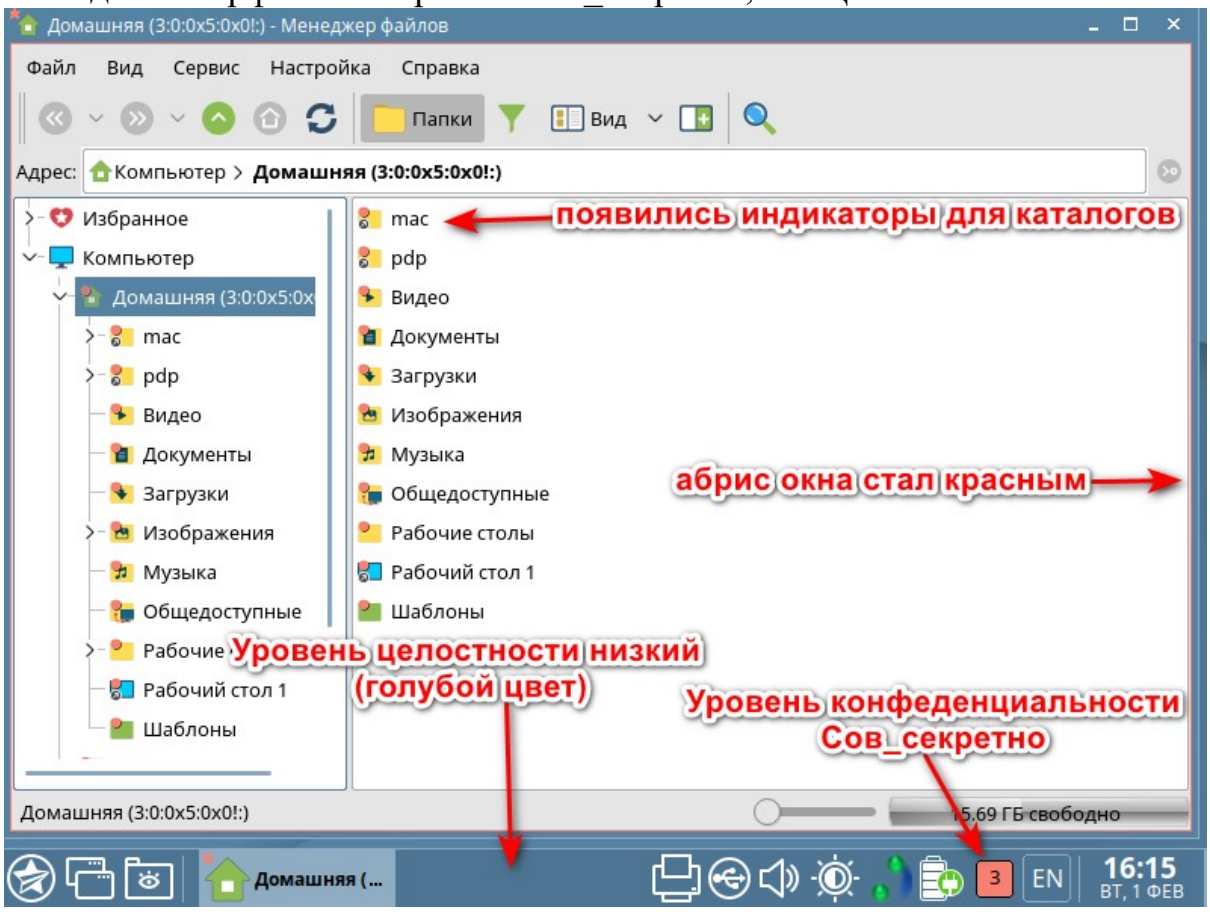

Рис. 19. Интерфейс ОС при УК Сов_секретно, МКЦ низкий

Далее, заходим в систему под пользователем student1 УК Секретно, МКЦ высокий, категория только Танки. Рассмотрим интерфейс системы. Запустим менеджер файлов. Обратите внимание на изменения, приведенные на рис. 20.

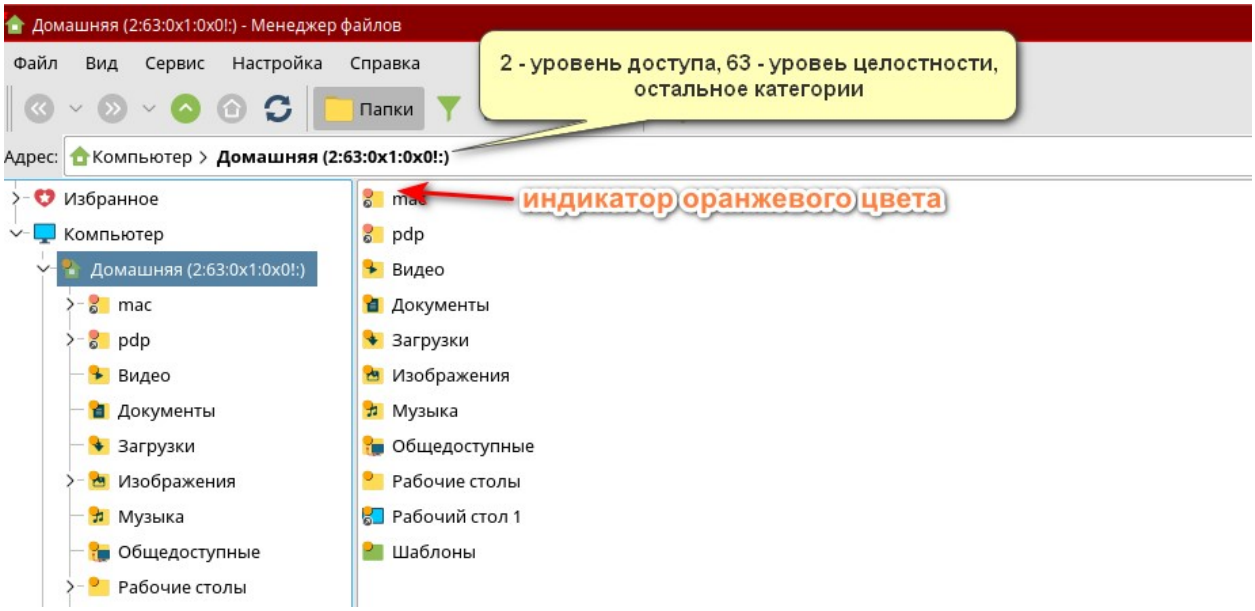

Рис. 20. Интерфейс менеждера файла при УК Секретно, МКЦ высокий, категория Танки

В каталогах mac и pdp (фактически одно и тоже) находятся домашние каталоги пользователя student1 соответствующие разным уровням конфиденциальности, целостности, категориям. Откройте содержимое каталога mac (рис. 21). Просмотрите его содержимое. Обратите внимание, что домашнего каталога третьего уровня, соответствующего уровню конфиденциальности «Сов_секретно» среди домашних каталогов пользователя student1 мы не видим, так как совершили вход в систему с уровнем конфиденциальности «Секретно» и выше нашего уровня мы не можем ни просматривать каталоги ни изменять их.

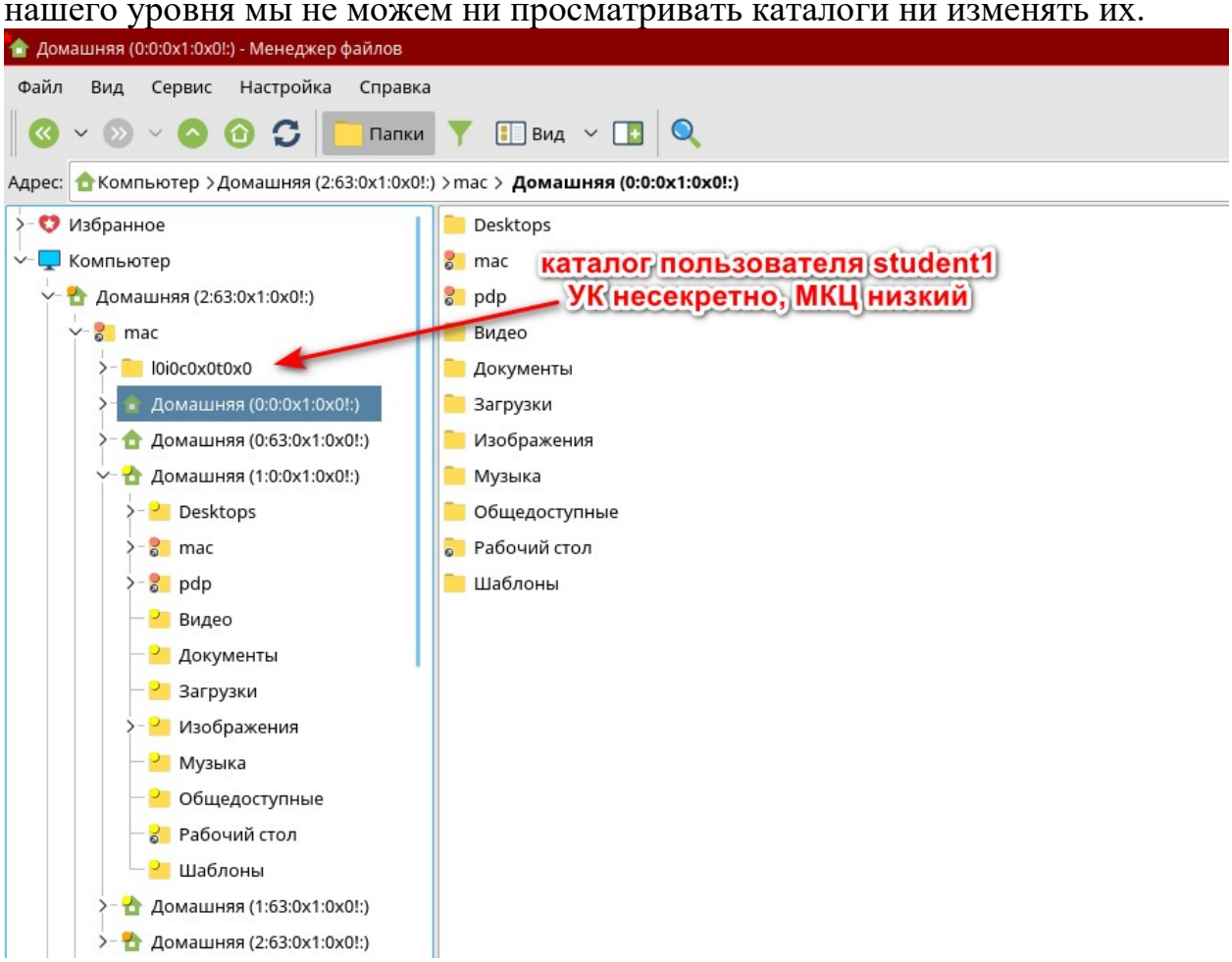

Рис. 20. Содержимое каталога mac

Если в имени каталогов нет слова «Домашняя», то можно выполнить действия, приведенные на рис. 21 (пункт 2 повторить два или несколько раз с «Применить»).

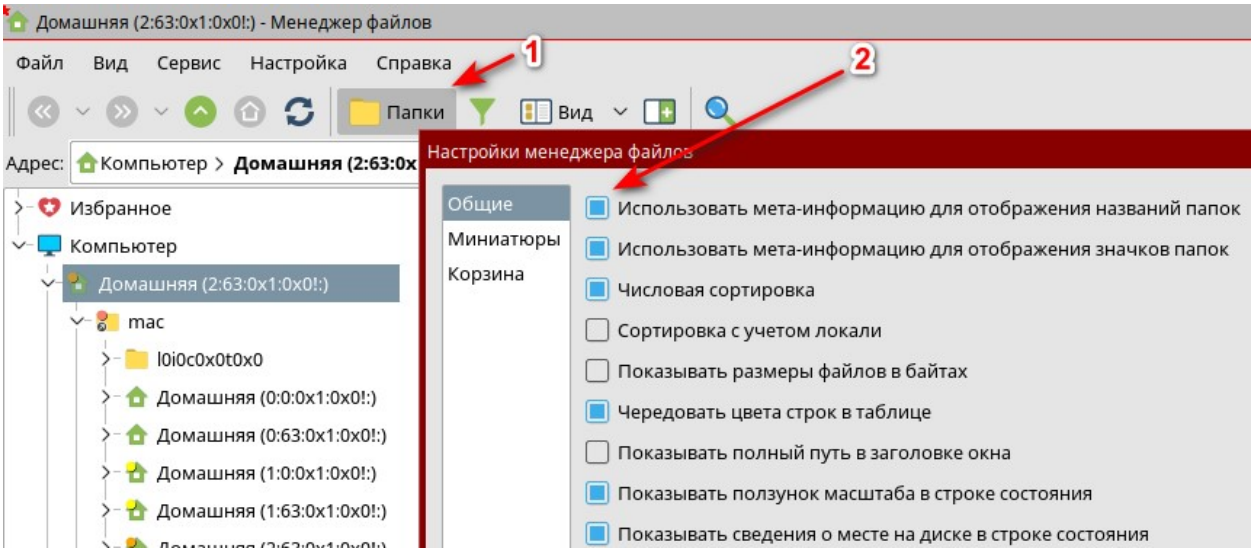

Рис. 21. Настройка отображения каталога mac

Создадим пустой текстовый файл в текущем домашнем каталоге пользователя, например файл proba.txt (рис. 22). Просмотрите свойства файла. Обратите внимание, что файл создан с УК «Секретно», что соответствует УК нашей текущей сессии. Об этом также сигнализирует индикатор уровня конфиденциальности (оранжевый кружок на иконке файла) А вот уровень целостности автоматически выставляется как низкий.

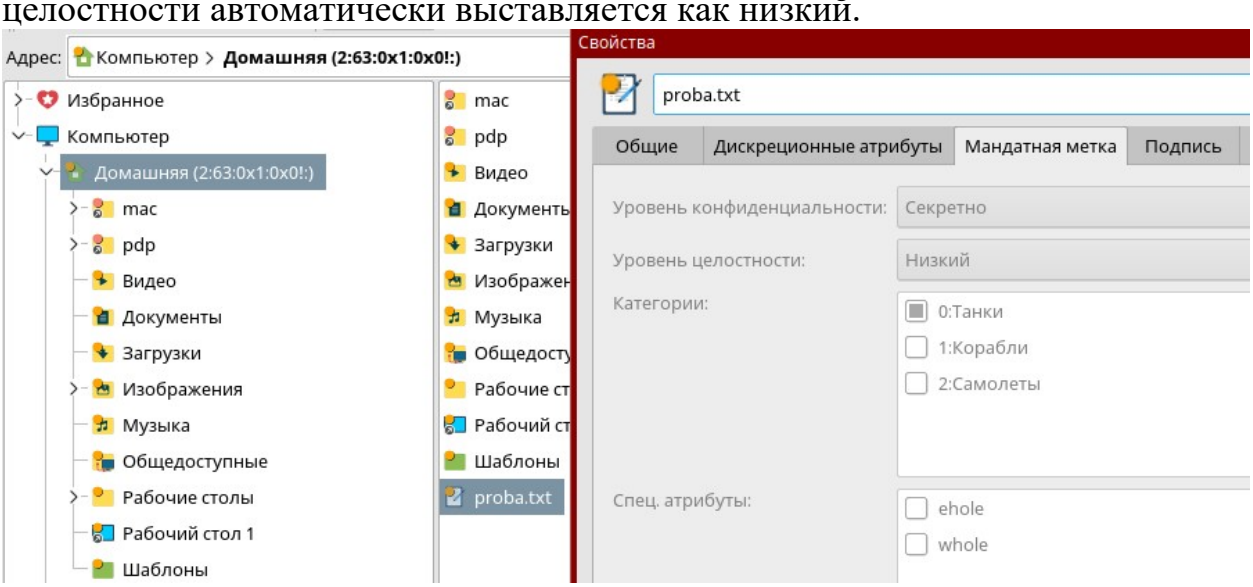

Рис. 23. Создание текстового файла и просмотр его атрибутов

Самостоятельно создайте любой каталог внутри домашнего каталога пользователя. Просмотрите и опишите свойства вновь созданного каталога.

Внесите любые изменения в тестовый файл proba.txt, открыв его, например, в любом текстовом редакторе. Сохраните и закройте файл. После этого попытайтесь с копировать его в домашний каталог пользователя с УК равным 1 «УК ДСП». Результат будет отрицательный, так как система блокирует копирование файлов с более высоким УК в каталог с более низким УК (рис. 24).

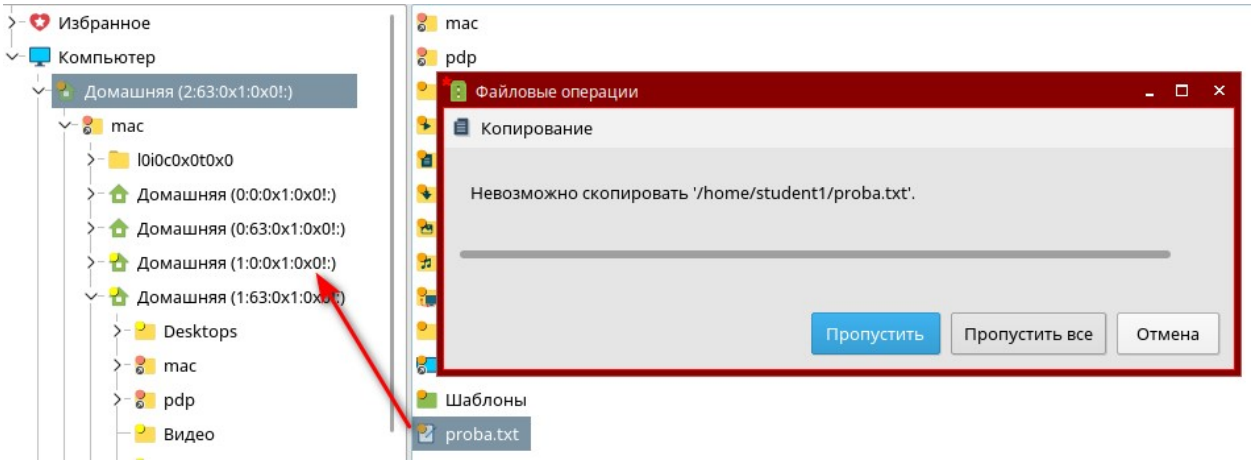

Рис. 24. Копирование текстового файла proba.txt в домашний каталог пользователя с более низким УК

Теперь рассмотрим обратную ситуацию, когда мы хотим скопировать в наш домашний каталог с УК «Секретно» любой файл с более низким УК, например «ДСП». Перейдите в каталог Домашняя (1:0:0x1:0x0!), далее в каталог, например, Desctop1. В каталоге находится файл, например, «Помощь». Просмотрите его мандатные метки. Как видите файл имеет мандатную метку «ДСП» (рис. 25).

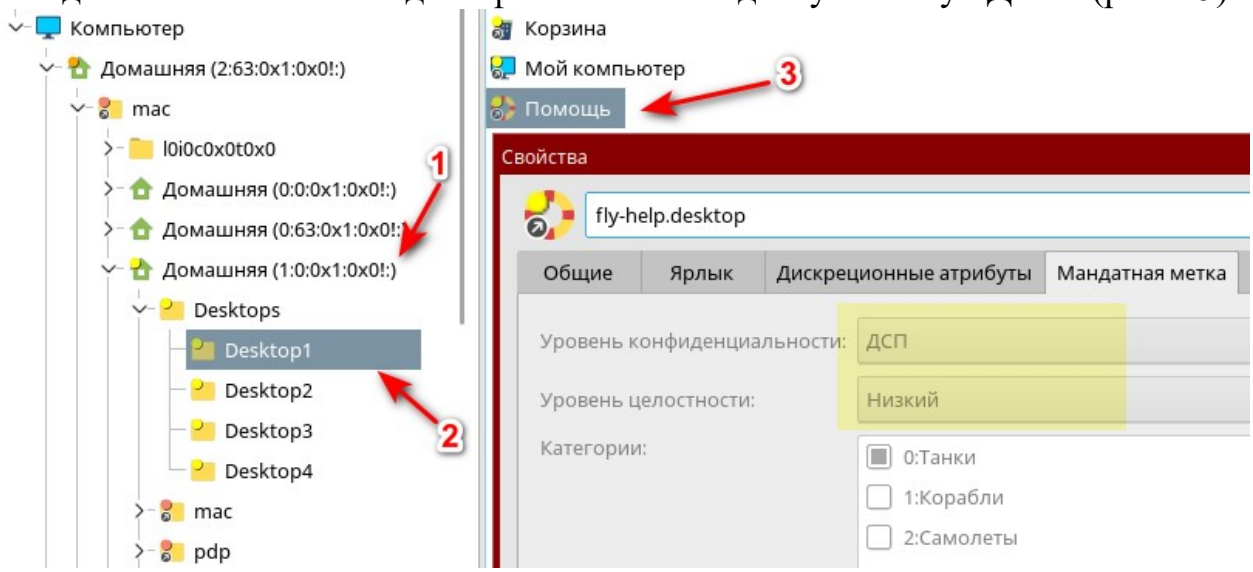

Рис. 25. Мандатные метки файла «Помощь» в домашнем каталоге пользователя с УК «ДСП»

Скопируйте файл «Помощь» в текущий домашний каталог (Домашняя 2:63:0x1:0x0!) с УК равным 2 (Секретно). Как видите, процедура копирования прошла без ошибок. Просмотрите свойства скопированного файла «Помощь» (рис. 26). У скопированного файла мандатные атрибуты поменялись. Файл теперь помечен мандатной меткой «Секретно». Таким образом, сотрудник с более низким УК имеет возможность отправить файл сотруднику с более высоким УК.

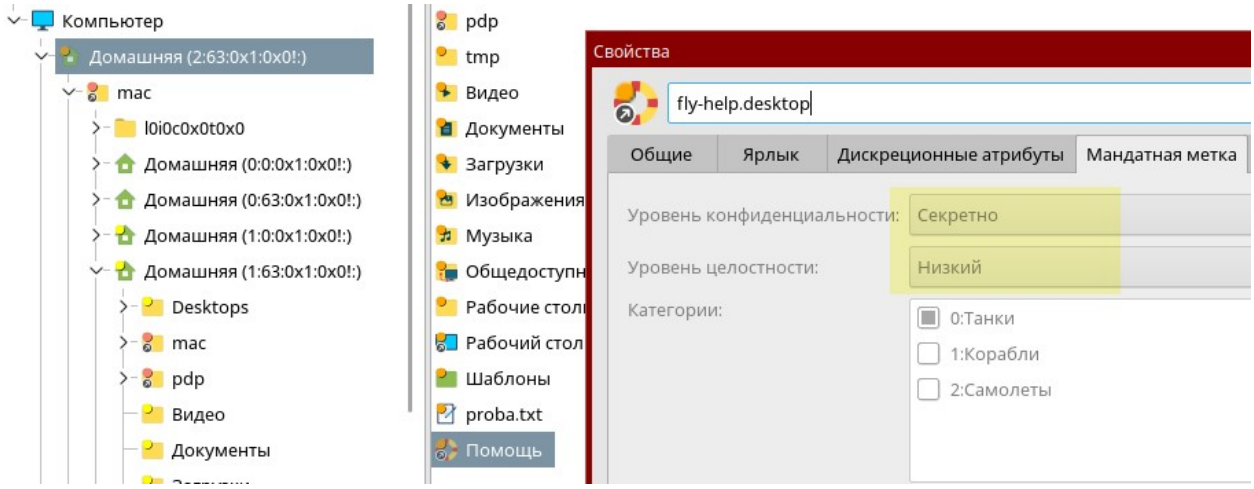

Рис. 26. Копирование файла «Помощь» в домашний каталог пользователя с более высоким УК

Самостоятельно проверьте возможности чтения и редактирования файлов с различными УК. Составьте отчет о возможностях копирования, чтения и редактирования файлов из каталогов с разными УК. Запишите цвета индикаторов мандатных меток для файлов с различными УК.

Работа с мандатными атрибутами при помощи консольных утилит

В ОС Astra Linux Special Edition, начиная с версии 1.5 имеется целый ряд новых команд и утилит для просмотра и редактирования мандатных атрибутов. Более подробное описание утилит см. в руководстве по КСЗ «Операционная система специального назначения «Astra Linux Special Edition»». Часть 1.

Для управления мандатными ПРД используются следующие утилиты:

Для управления мандатными ПРД в режиме командной строки используются следующие утилиты:

pdpl-file – управление мандатными атрибутами файлов (см. 4.8.1 руководства);

pdp-id – отображение мандатных атрибутов сессии пользователя ОС (см. 4.8.2 руководства);

pdp-init-fs – скрипт инициализации мандатных атрибутов ФС (см. 4.8.3 руководства);

pdp-ls – вывод аналогично стандартной команде ls информации о файлах с отображением мандатных атрибутов (см. 4.8.4 руководства);

pdpl-ps – управление мандатными атрибутами процессов (см. 4.8.5 руководства);

pdpl-user – управление допустимыми мандатными уровнями и категориями пользователей ОС (см. 4.8.6 руководства);

sumac – запуск процесса с заданными мандатными уровнем и категорией в отдельной графической сессии (см. 4.8.7 руководства);

userlev – изменение БД мандатных уровней (см. 4.8.8 руководства);

usercat –изменение БД мандатных категорий (см. 4.8.9 руководства).

Для совместимости с предыдущими версиями ОС сохранены следующие утилиты командной строки для управления мандатными ПРД:

chmac – управление мандатными атрибутами файлов (см. 4.8.10.1 руководства);

lsm – вывод аналогично стандартной команде ls информации о файлах с отображением мандатных атрибутов (см. 4.8.10.3 руководства);

macid – отображение мандатных атрибутов сессии пользователя ОС (см. 4.8.10.2 руководства);

psmac – управление мандатными атрибутами процессов (см. 4.8.10.4 руководства);

usermac – управление допустимыми мандатными уровнями и категориями пользователей ОС (см. 4.8.10.5 руководства);

getfmac – получение мандатных меток файловых объектов (см. 4.8.10.6 руководства);

setfmac – изменение мандатных меток файловых объектов (см. 4.8.10.7 руководства).

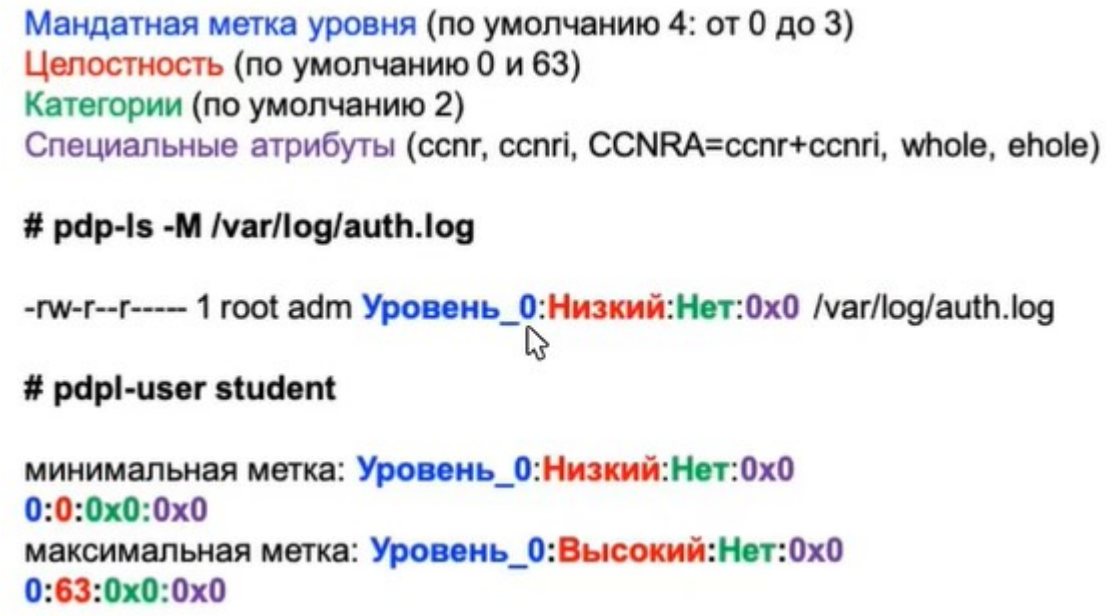

Рис. 27. Мандатный контекст безопасности

Просмотрим мандатные атрибуты файла **/var/log/auth.log** при помощи утилиты pdp-ls. Введите команду **pdp-ls -M /var/log/auth.log**. Опишите вывод команды (специальные атрибуты будут рассмотрены далее в занятии). Просмотрите мандатные атрибуты файлов текущего домашнего каталога пользователя student1 (рис. 28). Просмотрите мандатные уровни и категории командами **cat /etc/parsec/max_levels** и **cat /etc/parsec/mac_categories** соответственно.

```
student1@infra:~$ pwd
/home/student1
student1@infra:~$ pdp-ls -M
итого 44
drwx------m--  6 student1 student1 Секретно:Низкий:Танки:0x0 Desktops
-rw-r--r--m--  1 student1 student1 Секретно:Низкий:Танки:0x0 fly-help.desktop
lrwxrwxrwxm--  1 root     student1 Сов_секретно:Высокий:Танки,Корабли,Самолеты,0xffffffffffffff8:CCNRA mac -> /home/.pdp/student1
lrwxrwxrwxm--  1 root     student1 Сов_секретно:Высокий:Танки,Корабли,Самолеты,0xffffffffffffff8:CCNRA pdp -> /home/.pdp/student1
-rw-r--r--m--  1 student1 student1 Секретно:Низкий:Танки:0x0 proba.txt
drwxr-xr-xm--  2 student1 student1 Секретно:Низкий:Танки:0x0 tmp
drwxr-xr-xm--  2 student1 student1 Секретно:Низкий:Танки:0x0 Видео
drwxr-xr-xm--  2 student1 student1 Секретно:Низкий:Танки:0x0 Документы
drwxr-xr-xm--  2 student1 student1 Секретно:Низкий:Танки:0x0 Загрузки
drwxr-xr-xm--  3 student1 student1 Секретно:Низкий:Танки:0x0 Изображения
drwxr-xr-xm--  2 student1 student1 Секретно:Низкий:Танки:0x0 Музыка
drwxr-xr-xm--  2 student1 student1 Секретно:Низкий:Танки:0x0 Общедоступные
lrwxrwxrwxm--  1 student1 student1 Секретно:Низкий:Танки:0x0 Рабочий стол -> Desktops/Desktop1
drwxr-xr-xm--  2 student1 student1 Секретно:Низкий:Танки:0x0 Шаблоны
```

Рис. 28. мандатные атрибуты файлов
текущего домашнего каталога пользователя student1

Командой sudo pdpl-user можно просмотреть информацию о пользователе. Например, введите команду как на рис. 29. Самостоятельно просмотрите информацию о пользователях student2 и student3. Какие отличия от student1 в мандатных метках вы заметили?

```
student1@infra:~$ sudo pdpl-user student1
минимальная метка: Несекретно:Низкий:Танки:0x0
   0:0:0x1:0x0
максимальная метка: СоВ_секретно:Высокий:Танки,Самолеты:0x0
   3:63:0x5:0x0
```

Рис. 29. Мандатные атрибуты пользователя student1

В ОС порожденный процесс наследует мандатные метки процесса-родителя. Например, просмотрите максимальную и минимальную метку для пользователя root. Метки имеют одинаковое нулевое значение, что соответствует УК Несекретно. Однако, если вы при помощи команды **su –** повысите свои привилегии до roota и при помощи команды **macid** просмотрите текущий УК пользователя, вы увидите, что пользователь root работает на УК Секретно (текущий уровень пользователя student1). Это важно помнить при работе в системе (рис. 30).

```
student1@infra:~$ sudo pdpl-user root
минимальная метка: Несекретно:Низкий:Нет:0x0
   0:0:0x0:0x0
максимальная метка: Несекретно:Низкий:Нет:0x0
   0:0:0x0:0x0
student1@infra:~$ su -
Пароль:
root@infra:~# macid root
Уровень=2(Секретно) Категории=1(Танки)
```

Рис. 30. Мандатные атрибуты пользователя root

Командой userlev возможно изменение БД мандатных уровней. Просмотрите мандатные уровни введя команду **userlev**. Добавьте новый мандатный уровень с номером 4 и названием «Сверх_секретно», введя команду **userlev -a 4 Сверх_секретно**. Снова просмотрите БД мандатных уровней (рис. 31).

```
root@infra:~# userlev
0  Несекретно
1  ДСП
2  Секретно
3  СоВ_секретно
root@infra:~# userlev -a 4 СВерх_секретно
root@infra:~# userlev
0  Несекретно
1  ДСП
2  Секретно
3  СоВ_секретно
4  СВерх_секретно
```

Рис. 30. Изменение БД мандатных уровней

Командой usercat возможно изменение БД мандатных категорий. Просмотрите категории введя команду **usercat**. Самостоятельно добавьте новую категорию, например, Спутники.

Просмотрите содержимое каталога /etc/parsec/macdb. В этом каталоге перечисляются атрибуты, которые назначены учетным записям пользователей, точнее по их числовым идентификаторам user ID.

```
root@infra:~# ls /etc/parsec/macdb
1000  1001  1002  1003  1004
root@infra:~# cat /etc/parsec/macdb/1002
student1:0:1:3:5
root@infra:~# id student1
uid=1002(student1) gid=1003(student1) группы=20(dialout),24(cdrom)
-admin),333(astra-console),1003(student1)
root@infra:~# cat /etc/parsec/macdb/1003
student2:0:0:0:0
root@infra:~# id student2
uid=1003(student2) gid=1004(student2) группы=20(dialout),24(cdrom)
```

Рис. 31. Атрибуты, назначенные учетным записям пользователей

Запустите терминал с правами учетной записи student1 (введите в текущем окне терминала команду **exit**) и просмотрите мандатные атрибуты содержимого домашнего каталога пользователя командой **pdp-ls -M** (рис. 32). Также, можно использовать ключ -n для просмотра числовых значений категорий (**pdp-ls -M -n**)

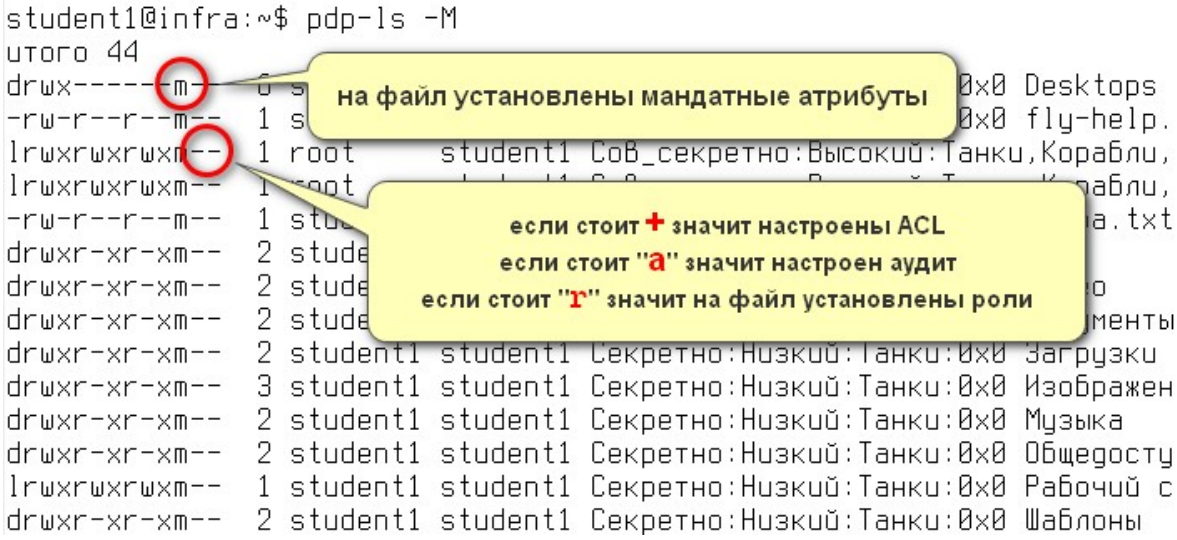

Рис. 32. Мандатные атрибуты содержимого домашнего каталога пользователя student1

Назначение ролей и привилегий пользователям при мандатном управлении доступом

Пользователям ОС возможно назначение ролей и привилегий для расширения их полномочий в системе. Различают Linux-привилегии и Parsec-привилегии. Linux-привилегии необходимы для назначения пользователям прав по администрированию каких-либо элементов ОС (стандартные для Linux систем). Parsec–привилегии необходимы для управления мандатным разграничением доступа. Также, они используются при управлении мандатным контролем сетевых соединений (передача мандатных меток по сети, по умолчанию используется

нулевая мандатная метка, если метка явно не назначена). При помощи Linux-привилегий можно, например, игнорировать права доступа к файлам (cap_dac_ovveride), игнорировать права на чтение или поиск файлов (cap_dac_read_search), игнорировать владельца файла (cap_fowner), игнорировать установку дополнительных битов доступа файлов (cap_fsetid), выдать права на сетевое администрирование (cap_net_admin) и т.п.

Как упоминалось выше, Parsec–привилегии необходимы для управления мандатным разграничением доступа. Например, можно дать пользователю права для изменения мандатной метки и установить другие привилегии (parsec_cap_setmac), менять мандатные метки файлов (parsec_cap_shmac), и т.п (рис. 33). Описание всех привилегий есть в страницах справочного руководства man.

cap_chown, cap_dac_ovveride	parsec_cap_file_cap, parsec_cap_audit
cap_dac_read_search, cap_fowner	parsec_cap_setmac, parsec_cap_chmac
cap_fsetid, cap_kill	parsec_cap_ignmaclvlparsec_cap_ignmaccat
cap_setgid, cap_setuid	parsec_cap_sig
cap_setpcap, cap_cap_linux_immutable	parsec_cap_update_atime
cap_net_bind_service	parsec_cap_priv_sock
cap_net_broadcast	parsec_cap_readsearch
cap_net_admin	parsec_cap_cap
cap_net_raw	parsec_cap_mac_soc
а)	*б)*

Рис. 33. Linux (а) и Parsec *(б) – привилегии*

Для управления привилегиями пользователей и процессов используется графическая утилита fly-admin-smc («Управление политикой безопасности»).

Также для управления привилегиями пользователей и процессов используются инструменты командной строки usercaps, execaps и pscaps, описанные, соответственно, в руководстве по КСЗ «Операционная система специального назначения «ASTRA LINUX SPECIAL EDITION»». Часть 1 пп. 4.9.1, 4.9.2 и 4.9.3.

Управление привилегиями пользователей выполняется только суперпользователем с максимальным уровнем целостности, установленным в ОС. Также, необходимо зайти в систему без уровней конфиденциальности (Несекретно).

Запустим графическую утилита fly-admin-smc («Управление политикой безопасности»). Для назначения привилегий пользователям выбираем вкладку «Пользователи», выбираем нужного пользователя и в правом окне активируем закладку «Привилегии» (рис. 34). Наведя курсор мыши на привилегию мы получаем подсказку по ней.

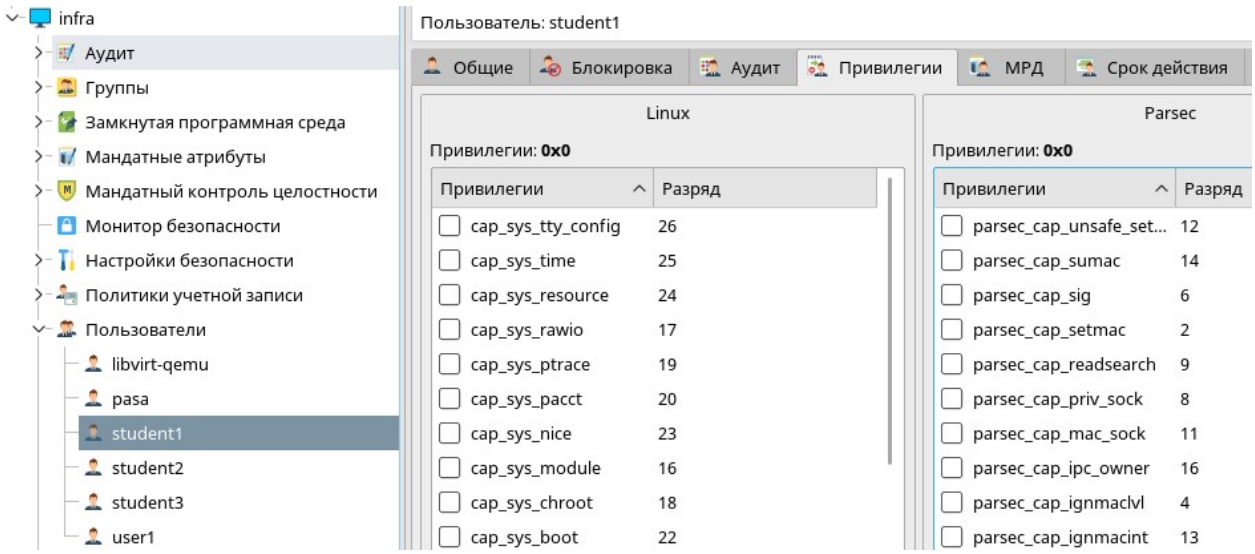

Рис. 34. Окно назначений привилегий пользователям

Например, можно дать право непривилегированному пользователю выполнять команды для общего системного администрирования системы, установив ему привилегию cap_sys_admin или права сетевого администратора (cap_net_admin). Для администраторов безопасности назначаются Parsec–привилегии. Самостоятельно сделайте пользователя student1 администратором безопасности, назначив ему одну или несколько Parsec–привилегий, а пользователю student2 назначьте привилегии общего системного администрирования системы.

Теперь во вкладке «Привилегии» появились пользователи с назначенными привилегиями (рис. 35).

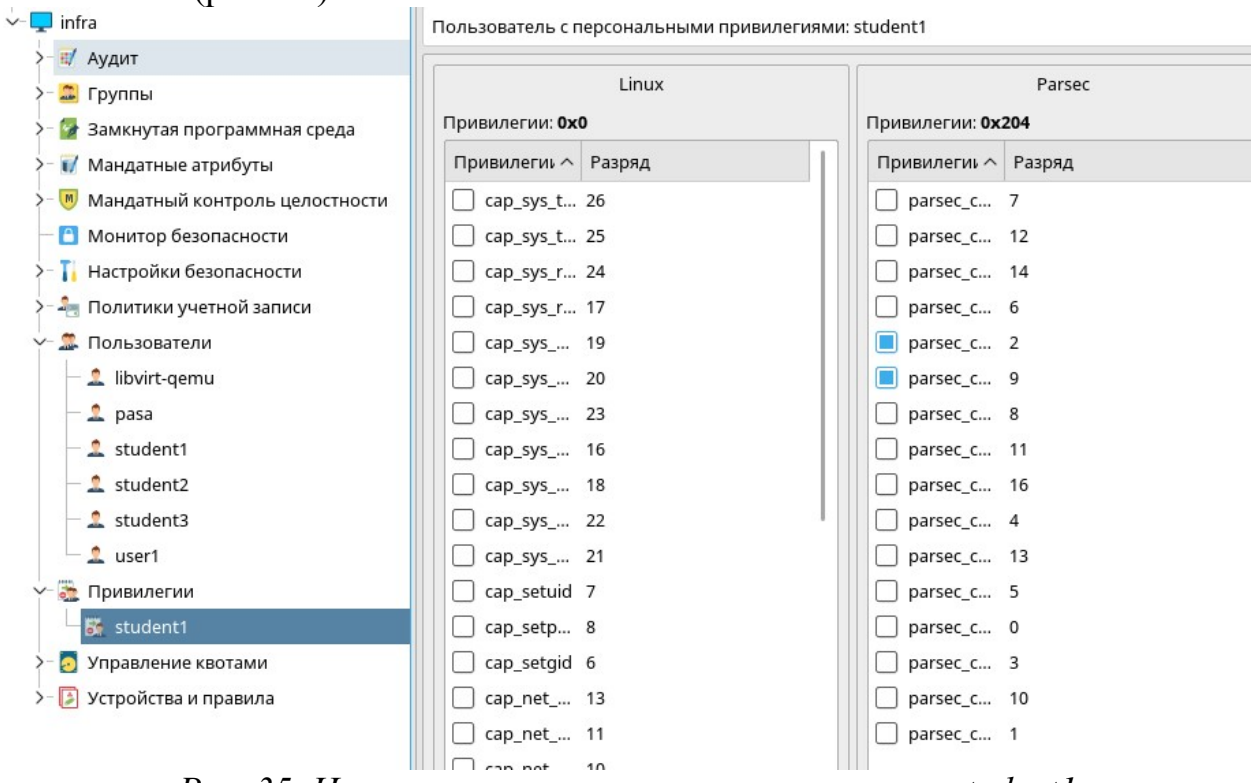

Рис. 35. Назначенные привилегии пользователю student1

Назначением привилегий можно заниматься и при помощи командной строки. Командной **usercaps -L** можно просмотреть все Linux-привилегии, а командой **usercaps -M** все Parsec-привилегии. Командой **usercaps student1** можно

просмотреть все привилегии, назначенные пользователю student1. Командой **usercaps -f student1** можно установить сразу все привилегии пользователю, а командой **usercaps -z student1** лишить его всех прав. Командой **usercaps -l +21: +12 student1** можно добавить какую-либо конкретную привилегию или несколько, как в данном примере. Если хотим убрать привилегию, то вместо + ставим **-**. Для назначения или отзыва Parsec-привилегий используем опцию **-m** (вместо **-l**). Самостоятельно отработайте вышеописанные команды.

Привилегии назначаются только пользователям, т.е. для групп назначение привилегий невозможно.

Дополнительные мандатные атрибуты управления доступом

Некоторым объектам в ОС может быть присвоены необязательные дополнительные мандатные атрибуты управления доступом, которые позволяют уточнить отдельные правила для управления этими объектами, и по умолчанию не входят в мандатную метку.

Рассмотрим Дополнительные мандатные атрибуты управления доступом, а именно:

мандатный атрибут CCNR может присваиваться сущностям, являющимся контейнерами, и могут содержать другие сущности (каталогам, которые могут содержать подкаталоги с разными мандатными метками, но не выше, чем его);

мандатный атрибут CCNRI может присваиваться контейнерам и определяет, что контейнер может содержать сущности с различными уровнями целостности (0, 63 и т.п.), но не большими, чем его собственный уровень целостности (тоже применяется только к контейнерам);

мандатный атрибут ehole может присваиваться сущностям (файлам), имеющим минимальную классификационную (мандатную) метку, и приводить к игнорированию мандатных правил управления доступом к ним (т.е. сущностям из которых субъект не может прочитать данные с меткой больше чем его собственная, например, устройство /dev/null);

мандатный атрибут whole присваивается сущностям (файлам) с ненулевой классификационной меткой и разрешает запись в них субъектам, имеющим более низкую классификационную (мандатную) метку (т.е. мы помним, что сверху вниз по УК писать запрещено, но при помощи такой метки можно сделать исключение).

Многие из этих атрибутов уже выставлены на каталоги, создаваемые при установке ОС.

/ – имеет наивысший мандатный уровень (по умолчанию 3), в битовой маске неиерархических категорий устанавливаются все биты, устанавливаются атрибуты CCNR и CCNRI. Это сделано для того, чтобы мы могли создавать свои сущности в корневом каталоге с разными классификационными метками и УК (например, каталог /home, в котором создаются домашние каталоги пользователей).

/bin, /boot, /etc, /lib, /lib32, /lib64, /lost+found, /media, /mnt, /opt, /proc, /root, /sbin, /selinux, /srv, /sys, /usr – системные каталоги с нулевой мандатным уровнем и пустой (нулевая) маской неиерархических категорий, атрибутов CCNR и CCNRI нет (чтобы пользователь не смог создать свои объекты с конфиденциальной информацией).

/media – большинство сменных носителей монтируется в каталог /home/%user%/media, несанкционированный доступ одного пользователя к сменным носителям другого пользователя становится невозможен. В ОС Astra Linux Special Edition хранение файлов с конфиденциальной информацией запрещено и все файлы имеют нулевые мандатные метки.

/dev, /run и /var – наивысший мандатный уровень и все неиерархические мандатные категории, устанавливается атрибут CCNR. Объекты, расположенные в каталогах /dev, /run и /var, имеют нулевые мандатные метки.

/parsecfs – каталог содержит внутренние системные объекты и имеет нулевой мандатный уровень, нулевая битовая маска неиерархических категорий и атрибут ehole.

/tmp – наивысший мандатный уровень и все неиерархические мандатные категории, устанавливаются атрибуты CCNR и ehole (являются единственными возможными настройками для обеспечения совместимости с программным обеспечением).

/home – наивысший мандатный уровень, ему присвоены все неиерархические мандатные категории и атрибут CCNR. Такие же мандатные атрибуты присваиваются служебному подкаталогу /home/.pdp. Мандатные атрибуты домашних каталогов пользователей соответствуют мандатным атрибутам учётных записей пользователей.

Перейдем к практическому изучению вопроса.

Убедимся в наличии у корневого каталога / наивысшего мандатного уровня (по умолчанию 3) и наличию всех битов в битовой маске неиерархических категорий (рис. 36).

```
pasa@infra:~$ pdp-ls -Md /
drwxr-xr-xm--  26 root root Сов_секретно:Высокий:Танки,Корабли,Самолеты,0xfffffffffffffff8:CCNRA /
```

Рис. 36. Мандатные атрибуты корневого каталога /

Как видно у корневого каталога установлены все максимальные мандатные метки и категории. Обратите внимание на мандатный атрибут CCNRA. Это композитный атрибут, который включает в себя два активных атрибута CCNR и CCNRI, т.е. в корневом каталоге мы можем создавать любые объекты с любым УК и УЦ.

Создадим каталог /primer и назначим ему дополнительные мандатные атрибуты. Каталог создается командой **mkdir /primer**. Созданный каталог будет иметь УК Несекретно, УЦ Низкий, без категорий. Поменяем метку командой **pdpl-file 1:0:0:0 /primer**. Просмотрите теперь мандатные атрибуты каталога. УК изменил свое значение на ДСП.

Создайте еще один каталог /primer1. Внутри каталога при помощи команды touch (или любой другой) создайте файл с именем file. Просмотрите мандатную метку каталога /primer1. Командой pdp-**ls -M /primer1** просмотрите мандатные метки файлов внутри каталога. Поменяйте рекурсивно мандатные метки для всех объектов внутри каталога, введя команду **pdpl-file -R 1:0:0:0 /primer1**. Как видите, попытка рекурсивного изменения мандатных меток закончилась неудачей. Это нормальное поведение ДП-модели контроля доступа. Для успешного выполнения операции нужно установить дополнительные мандатные атрибуты CCNR каталога

/primer1 командой **pdpl-file 1:0:0:ccnr /primer1**. Проверьте вновь установленные мандатные атрибуты каталога. Теперь можно изменять метки у файлов внутри каталога /primer1. Введите команду **pdpl-file 1:0:0:0 /primer1/file**. Операция прошла успешно. После изменения мандатных меток можно убрать атрибут CCNR у каталога /primer1 (рис. 37).

```
root@infra:~# mkdir /primer1
root@infra:~# touch /primer1/file
root@infra:~# pdp-ls -Md /primer1
drwxr-xr-x---  2 root root Несекретно:Низкий:Нет:0x0 /primer1
root@infra:~# pdp-ls -M /primer1
итого 0
-rw-r--r-----  1 root root Несекретно:Низкий:Нет:0x0 file
root@infra:~# pdpl-file -R 1:0:0:0 /primer1
pdpl-file: /primer1: Отказано в доступе
root@infra:~# pdpl-file 1:0:0:ccnr /primer1
root@infra:~# pdp-ls -Md /primer1
drwxr-xr-xm--  2 root root ДСП:Низкий:Нет:ccnr /primer1
root@infra:~# pdpl-file 1:0:0:0 /primer1/file
root@infra:~# pdp-ls -M /primer1
итого 0
-rw-r--r--m--  1 root root ДСП:Низкий:Нет:0x0 file
root@infra:~# pdpl-file 1:0:0:0 /primer1
```

Рис. 37. Изменение мандатных меток

Для автоматизации таких процедур существует сценарий bash (можно скачать с сайта производителя ОС). Сценарий необходим для облегчения труда администратора информационной безопасности в случае повседневной и масштабной смены мандатных атрибутов.

Запустите менеджер файлов (напомним, что управление привилегиями пользователей выполнялось суперпользователем (администратором) с максимальным уровнем целостности, установленным в ОС. Также, вход в систему был осуществлен без уровней конфиденциальности). Проверьте, видны ли созданные каталоги /primer1 и /primer с установленными мандатными атрибутами в окне менеджера? Если нет, то почему?

Войдите в систему под пользователем student1 с УК Секретно. Запустите менеджер файлов. Проверьте, видны ли созданные каталоги /primer1 и /primer с установленными мандатными атрибутами в окне менеджера? Откройте на редактирование файл /primer1/file, например, в LibreOffice. Внесите изменения в файл. Попробуйте сохранить его под тем же именем (или любым другим). Удалось ли сохранить файл? Если нет, то почему?

Создадим каталог общий для всех пользователей для возможности обмена файлов. Создадим каталог /test1. Проверьте мандатные атрибуты созданного каталога. Установим мандатные атрибуты на каталог с максимальным УК 2 и дополнительным мандатным атрибутом CCNR командой **pdpl-file -R 2:0:0:ccnr /test1**. Атрибут CCNR используем для возможности изменения УК сущностям внутри каталога /test1. Проверьте вновь установленные мандатные атрибуты каталога.

Создадим два каталога внутри каталога /test1 командой **mkdir /test1/dir1 /test1/dir2**. Проверим установленные мандатные атрибуты каталогов dir1 и dir2. Каталоги имеют мандатные атрибуты с УК Несекретно и низким УЦ. Предположим, что у нас есть два пользователя с разными УК, у одного УК

Секретно, у второго УК ДСП. Присвоим каталогу dir1 мандатный атрибут ДСП, а каталогу dir2 атрибут Секретно (рис. 38).

```
pasa@infra:~$ su -
Пароль:
root@infra:~# mkdir /test1
root@infra:~# pdp-ls -Md /test1
drwxr-xr-x---  2 root root Несекретно:Низкий:Нет:0x0 /test1
root@infra:~# pdpl-file -R 2:0:0:ccnr /test1
root@infra:~# pdp-ls -Md /test1
drwxr-xr-xm--  2 root root Секретно:Низкий:Нет:ccnr /test1
root@infra:~# mkdir /test1/dir1 /test1/dir2
root@infra:~# pdp-ls -M /test1
итого 8
drwxr-xr-x---  2 root root Несекретно:Низкий:Нет:0x0 dir1
drwxr-xr-x---  2 root root Несекретно:Низкий:Нет:0x0 dir2
root@infra:~# pdpl-file 1:0:0 /test1/dir1
root@infra:~# pdpl-file 2:0:0 /test1/dir2
root@infra:~# pdp-ls -M /test1
итого 8
drwxr-xr-xm--  2 root root ДСП:Низкий:Нет:0x0 dir1
drwxr-xr-xm--  2 root root Секретно:Низкий:Нет:0x0 dir2
```

Рис. 38. Создание каталогов и изменение их мандатных меток

Создадим два непустых файла file1.txt и file2.txt, по одному в каждом каталоге dir1 и dir2 соответственно.

echo Privet1>/test1/dir1/file1.txt

echo MiruMir>/test1/dir2/file2.txt

Обратите внимание на атрибуты вновь созданных файлов (рис. 39).

```
root@infra:/# pdp-ls -M /test1/dir1
итого 4
-rw-r--r--m--  1 root root ДСП:Низкий:Нет:0x0 file1.txt
root@infra:/# pdp-ls -M /test1/dir2
итого 4
-rw-r--r--m--  1 root root Секретно:Низкий:Нет:0x0 file2.txt
```

Рис. 39. Мандатные атрибуты файлов file1.txt и file2.txt

Мандатные атрибуты ДСП для file1.txt и Секретно для file2.txt были установлены такими же как и у каталогов в которых они находятся, так как у этих каталогов не установлен дополнительный мандатный атрибут CCNR.

Установим дискреционные права доступа на созданные файлы (rwx) командой **chmod -R 777 /test1/**. Убедимся в корректности установленных прав командой **ls -ld /test1/**.

Создаем двух пользователей test1 и test2 с разными УК (через «Панель управления»). Пользователю test1 назначаем максимальный МРД «ДСП», пользователю test2 назначаем максимальный МРД «Секретно». Сделайте это самостоятельно при помощи утилиты fly-admin-smc.

Зайдем в систему под пользователем test1 с УК ДСП. Запустим менеджер файлов. Перейдем в корень файловой системы. Перейдем в каталог /test1. В данном каталоге нам доступен только каталог dir1, потому что каталог dir2, который также находится в каталоге /test1 имеет более высокую мандатную метку (рис. 40).

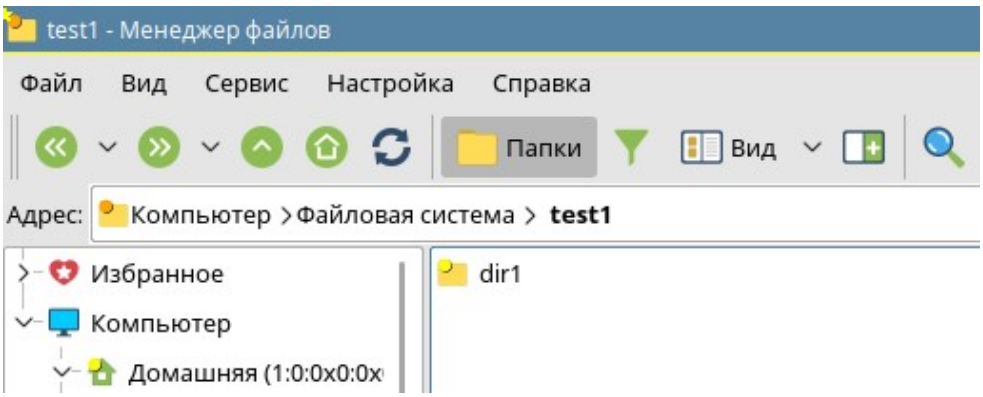

Рис. 40. Содержимое каталога /test1 *доступное пользователю test1*

Зайдите в каталог dir1, откройте на редактирование файл file1.txt, внесите в него изменения и сохраните. Как видите, операция прошла успешно. Создайте самостоятельно каталог и файл в каталоге dir1. Теперь попробуйте создать что-то в каталоге /test1. Как видите, это невозможно. Объясните, почему?

Зайдем в систему под пользователем test2 с УК «Секретно». Запустим менеджер файлов. Перейдем в корень файловой системы. Перейдем в каталог /test1. В данном каталоге нам доступен теперь и каталог dir1 и каталог dir2. Зайдите в каталог dir2, откройте на редактирование файл file2.txt, внесите в него изменения и сохраните. Как видите, операция прошла успешно. Создайте самостоятельно каталог и файл в каталоге dir2.

Зайдите в каталог dir1, откройте на редактирование файл file1.txt, внесите в него изменения и попробуйте сохранить. Как видите, операция завершилась ошибкой. Также мы не имеем возможности создавать какие-либо объекты в этом каталоге. Это также наглядно показывает работу ДП-модели, когда мы можем объекты с низлежащими уровнями только просматривать, а редактировать нет. Теперь попробуйте создать что-то в каталоге /test1. Как видите, теперь это возможно. Объясните, почему?

Предположим, что сотрудник с низлежащим УК подготовил для нас документ и разместил его в своем каталоге. В данном примере это пользователь test1 с УК «ДСП» подготовил для нас документ file1.txt (как мы убедились ранее этот файл, расположенный в каталоге dir1 доступен нам только на чтение). Скопируйте file1.txt в каталог dir2. Теперь попробуйте отредактировать и сохранить скопированный файл file1.txt. Как видите, операция прошла успешно и мандатная метка у файла изменилась на УК «Секретно» (рис. 41).

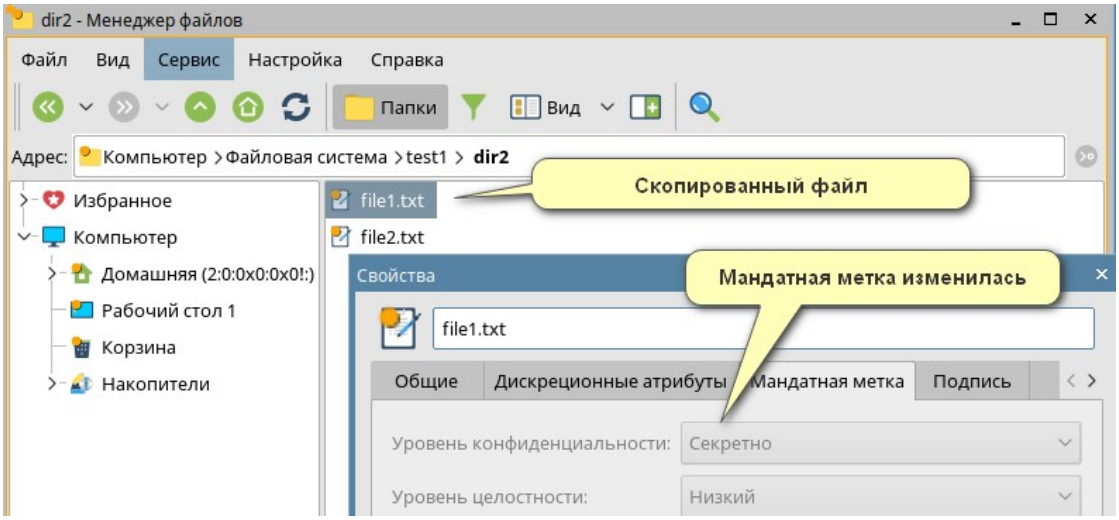

Рис. 41. Изменение мандатной метки скопированного файла file1.txt

Войдем в систему с системной учетной записью администратора. В меню «Пуск» перейдем на вкладку «Мультимедиа» и запустим медиаплеер VLC. Запустим терминал и перейдем в режим суперпользователя. При помощи команды **pgrep vlc** узнаем PID процесса VLC. Как мы знаем, все процессы в системе наследуют мандатные уровни пользователя, который их запустил на выполнение. Узнаем текущий УК процесса VLC при помощи утилиты psmac введя команду psmac и указав ей в качестве опции PID процесса VLC, например так psmac 10267.

```
root@infra:~# pgrep vlc
10267
root@infra:~# psmac 10267
10267 Несекретно:Нет
```

Рис. 42. Мандатный уровень процесса VLC

Если бы мы выбрали другой мандатный уровень и категорию при входе в систему вывод команды был бы другой. Если у пользователя включена привилегия parsec_cup_setmac то этот пользователь может модифицировать мандатные атрибуты процесса, например, при помощи утилиты psmac.

Задание для самостоятельного выполнения

1. Начать работу со входа в ОССН в графическом режиме с учётной записью пользователя user (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Высокий»).
2. Запустить графическую утилиту редактирования учётных записей пользователей «Политика безопасности» через меню «Панель управления» главного пользовательского меню.
3. Модифицировать параметры мандатного управления доступом, для этого осуществить следующие действия:

открыть раздел «Мандатные атрибуты», «Уровни конфиденциальности» и выбрать «0»:Уровень_0» и переименовать данный уровень доступа: «Уровень0»;

выполнить создание уровня доступа с именем «Уровень_4», задав значение равное 4, после чего проверить наличие записи «Уровень_4» в списке «Уровни конфиденциальности»;

выполнить обратное переименование: «Уровень0» в «Уровень_0».

4. Создать учётную запись пользователя user1, установив максимальный уровень доступа: «Уровень_4».

5. Выполнить удаление уровня доступа 4 из раздела «Уровни конфиденциальности» путём выбора в контекстном меню пункта «Удалить».

6. Открыть учётную запись пользователя user1 и в вкладке «МРД» в элементе «Максимальный уровень» проверить отсутствие записи имени уровня, при этом, в списке выбора уровня «Уровень_4» также будет отсутствовать.

7. Вывести в терминал Fly параметры мандатного управления доступом для учётной записи пользователя user1. Для этого выполнить следующие действия:

запустить терминал Fly и перейти в каталог /etc/parsec/macdb;

прочитать параметры учётной записи user1 командой **sudo grep "^user1:" ***;

определить максимальный уровень доступа учётной записи user1 командой **sudo grep "user1:" * | cut -d : -f 5**;

определить минимальный уровень доступа учётной записи user1 командой **sudo grep "user1" * | cut -d : -f 3** и проверить его соответствие данным, отображаемым в графической утилите «Политика безопасности».

8. Создать неиерархические категории с использованием графической утилиты «Политика безопасности». Для этого выполнить следующие действия:

в разделе «Категории» удалить исходные неиерархические категории;

затем создать новую неиерархическую категорию с именем «Otdel1», «Разряд» – 0;

в разделе «Категории» создать новые неиерархические категории: «Otdel2» («Разряд» – 1), «Upravlenie» («Разряд» – 2).

9. Изменить набор неиерархических категорий с использованием графической утилиты «Политика безопасности», для этого выполнить следующие действия в разделе «Категории»:

выбрать неиерархическую категорию «Otdel1» и ввести наименование «Отдел_1»;

аналогично переименовать неиерархические категории «Otdel2» и «Upravlenie» в «Отдел_2» и «Управление», соответственно;

проанализировать возможность одновременного изменения элемента «Разряд».

10. Изменить мандатный уровень доступа с использованием графической утилиты «Политика безопасности», для этого выполнить следующие действия:

создать новую группу с именем «office1» и задать первичную группу учётной записи пользователя user1 – «office1»;

создать новую учётную запись пользователя user2 и установить её первичную группу – «office1»;

в вкладке «Дополнительные» осуществить попытку выбора минимального набора неиерархических категорий – «Отдел_2», и проанализировать результат;

в вкладке «Дополнительные» выбрать максимальный уровень доступа – «Уровень_3», максимальный набор неиерархических категорий – «Отдел_2», после чего задать минимальный набор неиерархических категорий – «Отдел_2»;

открыть параметры учётной записи пользователя user1 и выбрать максимальный уровень доступа – «Уровень_3», максимальный набор неиерархических категорий – «Отдел_1», минимальный набор неиерархических категорий – «Отдел_1»;

создать учётную запись пользователя rukoffice1 и задать первичную группу: «office1»;

в вкладке «Дополнительные» выбрать максимальный уровень: «Уровень_3», максимальный набор категорий: «Отдел_1», «Отдел_2», «Управление».

11. Создать общий каталог для работы от имени учётных записей пользователей user1, user2, rukoffice1 в каталоге /home/work. При этом, для работы от имени учётных записей пользователей с наборами неиерархическими категорий равными «Отдел_1», «Отдел_2» и «Управление» выделить отдельные каталоги «otdel1», «otdel2» и «upr», соответственно. При этом обеспечить хранение файлов с различными уровнями конфиденциальности в каталогах с использованием специального атрибута CCNR, для чего осуществить следующие действия:

запустить терминал Fly в «привилегированном» режиме командой sudo fly-term;

создать каталог work и задать параметры мандатного и дискреционного управления доступом командами:

mkdir /home/work
chown user:office1 /home/work
chmod 750 /home/work
pdpl-file 3:0:Отдел_1,Отдел_2,Управление:ccnr /home/work

создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел_1» и задать параметры мандатного и дискреционного управления доступом командами:

cd /home/work
mkdir otdel1
chown user1:office1 otdel1
chmod 770 otdel1
pdpl-file 3:0:Отдел_1:ccnr otdel1

создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Отдел_2» и задать параметры мандатного и дискреционного управления доступом командами:

mkdir otdel2
chown user2:office1 otdel2
chmod 770 otdel2
pdpl-file 3:0:Отдел_2:ccnr otdel2

создать каталог upr для работы от имени учётных записей пользователей с набором неиерархических категорий равным «Управление» командами:

mkdir upr
chown rukoffice1:office1 upr
chmod 770 upr

pdpl-file 3:0:Управление:ccnr upr

создать вложенные каталоги У1, У2, У3 в каталогах otdel1, otdel2, upr командой:

mkdir {otdel{1,2},upr}/У{1,2,3}

установить для каталогов otdel1, otdel2, upr необходимые уровни (см. команды для каталога upr):

pdpl-file 1:0:Управление:0 /home/work/upr/У1
pdpl-file 2:0:Управление:0 /home/work/upr/У2
pdpl-file 3:0:Управление:0 /home/work/upr/У3
chown rukoffice1:office1 upr/У{1,2,3}
chmod 770 upr/У{1,2,3}

12. Выполнить последовательные входы в ОССН с учётной записью пользователя user1 (неиерархическая категория – «Отдел_1», уровни доступа 1, 2, 3). При работе на уровнях доступа 1, 2 и 3 создать в каталоге /home/work/otdel1/уровеньX файлы с именами 11.txt, 12.txt, 13.txt, соответственно, и установить дискреционные права доступа с разрешением на запись и чтение для группы office1 в графическом файловом менеджере Fly (fly-fm).

13. Выполнить последовательные входы в ОССН с учётной записью пользователя user2 (неиерархическая категория – «Отдел_2», уровни доступа 1, 2, 3). При работе на мандатных уровнях доступа 1, 2 и 3 создать в каталоге /home/work/otdel2/уровеньX файлы с именами 21.txt, 22.txt, 23.txt, соответственно, и установить дискреционные права доступа с разрешением на запись и чтение для группы office1 в файловом менеджере Fly.

14. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа – 3, неиерархическая категория – «Отдел2») и проверить возможность получения следующих доступов к файлам: доступ на чтение к файлам 21.txt, 22.txt, 23.txt, доступ на запись к файлу 23.txt.

15. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа – 2, неиерархическая категория – «Отдел_1») и проверить возможность получения следующих доступов к файлам: доступ на чтение к файлам 11.txt, 12.txt, доступ на запись к файлу 12.txt.

16. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа – 3, набор неиерархических категорий – «Отдел_1», «Отдел_2», «Управление») и проверить возможность получения доступа на чтение к файлам 11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt.

17. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа – 3, неиерархическая категория – «Управление»). Создать файл u3.txt в каталоге /home/work/upr/У3.

18. Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа – 3, набор неиерархических категорий: «Отдел_1», «Отдел_2», «Управление») и проверить возможность получения следующих доступов к файлам: доступ на запись к файлу u3.txt, доступ на чтение к файлам u3.txt, 11.txt, 12.txt, 13.txt, 21.txt, 22.txt, 23.txt.

19. Для доступа к терминалу Fly настроить включение учётных записей пользователей user1, user2, rukoffice1 во вторичную группу astra-console. Это

позволит данным учётным записям пользователей запускать терминал Fly с использованием комбинации Win+R.

20. Вывести в терминал Fly параметры мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей. Для этого выполнить следующие действия:

войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа – 2, набор неиерархических категорий: «Отдел_1», «Управление»);

в терминале Fly выполнить команду pdp-id -a, проанализировать результат;

выполнить избирательный вывод параметров мандатного управления доступом (с числовыми значениями) командами pdp-id -l и pdp-id -c;

выполнить избирательный вывод параметров мандатного управления доступом (с именами) командами pdp-id -ln и pdp-id -cn.

21. Изменить параметры мандатного управления доступом и мандатного контроля целостности учётной записи пользователя rukoffice1. Для этого выполнить следующие действия:

войти в ОССН с учётной записью пользователя user (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Высокий») и запустить терминал Fly в «привилегированном» режиме командой sudo fly-term;

изменить минимальный и максимальный уровни доступа учётной записи пользователя rukoffice1 командой **pdpl-user -l 0:2 rukoffice1**, а также минимальный и максимальный наборы неиерархических категорий пользователя rukoffice1 командой **pdpl-user -c 0:2 rukoffice1**;

обнулить значения уровней доступа и наборов неиерархических категорий в параметрах учётной записи пользователя rukoffice1 командой **pdpl-user -z rukoffice1**;

установить значения уровней доступа и наборов неиерархических категорий в параметрах учётной записи пользователя rukoffice1 командой **pdpl-user -l 1:3 -c 0:7 rukoffice1**.

22. Считать параметры мандатного управления доступом и мандатного контроля целостности учётной записи пользователя rukoffice1 из файлов настроек. Для этого выполнить следующие действия:

перейти в каталог /etc/parsec/macdb и считать минимальный и максимальный уровни доступа командами **grep “rukoffice1” * | cut -d : -f 3 и grep “rukoffice1” * | cut -d : -f 5**, соответственно;

считать минимальный и максимальный наборы неиерархических категорий командами **grep “rukoffice1” * | cut -d : -f 4 и grep “rukoffice1” * | cut -d : -f 6**, соответственно.

23. Создать и модифицировать мандатные уровни доступа, осуществив следующие действия:

вывести в терминал созданные уровни доступа командой userlev и сравнить

полученные данные с настройками в утилите «Политика безопасности»;

добавить новый уровень доступа с именем «Уровень_4» (значение 4) командой **userlev Уровень_4 --add 4** и вывести в терминал уровни доступа командой userlev;

выполнить переименование уровня доступа «Уровень_4» в «НовыйУровень» командой **userlev Уровень_4 --rename НовыйУровень**;

добавить возможность работы от имени учётной записи пользователя rukoffice1 на уровне доступа 4 командой **pdpl-user -l 1:4 rukoffice1**;

выполнить попытку изменения значения уровня доступа «НовыйУровень» на 3 командой **userlev НовыйУровень --modify 3**, проанализировать результат;

изменить значение уровня доступа «НовыйУровень» на 5 командой **userlev НовыйУровень --modify 5** и вывести в терминал максимальный уровень доступа учётной записи пользователя rukoffice1 командой **pdpl-user rukoffice1**, проанализировать результат;

установить максимальный уровень доступа учётной записи пользователя rukoffice1 равным 5 командой **pdpl-user -l 1:5 rukoffice1**;

удалить уровень доступа с именем «НовыйУровень» командой **userlev НовыйУровень -d** и определить максимальный уровень доступа учётной записи пользователя rukoffice1 командой **pdpl-user rukoffice1**, проанализировать результат;

восстановить набор неиерархических категорий и уровней доступа учётной записи пользователя rukoffice1 командой **pdpl-user -l 1:3 -c 0:7 rukoffice1**.

24. Создать и модифицировать неиерархические категории:

в терминале Fly, запущенном в «привилегированном» режиме, вывести неиерархические категории командой **usercat**;

добавить новую неиерархическую категорию командой u**sercat otdel3 --add 0x8**;

переименовать неиерархическую категорию «otdel3» в «Отдел_3» командой **usercat otdel3 --rename Отдел_3**;

осуществить попытку модификации наборов неиерархических категорий учётной записи пользователя rukoffice1 командой **pdpl-user -c 0:15 rukoffice1**,

проанализировать результат;

добавить неиерархическую категорию «Отдел_3» в наборы неиерархических категорий учётной записи пользователя rukoffice1 командой **pdpl-user -c 3:F rukoffice1**, обратить внимание на то, что неиерархическая категория задаётся в шестнадцатеричном формате;

осуществить попытку изменения значения неиерархической категории «Отдел_3» на значение 2 командой **usercat Отдел_3 --modify 2**, проанализировать результат;

изменить значение неиерархической категории «Отдел_3» на 0x10 командой **usercat Отдел_3 --modify 10**;

изменить значение неиерархической категории «Отдел_3» на 0x20 командой **usercat Отдел_3 --modify 0x20**, обратить внимание на то, что независимо от указания типа числа по префиксу «0x» (десятичное или шестнадцатеричное) значение неиерархической категории задаётся в шестнадцатеричном формате;

удалить неиерархическую категорию «Отдел_3» командой **usercat Отдел_3 --delete**;

изменить значение неиерархической категории «Управление» на 0x10 командой **usercat Управление --modify 10**, проанализировать результат по данным, выводимым командой **pdpl-user rukoffice1**;

изменить значение неиерархической категории «Управление» на 4 командой **usercat Управление --modify 4**.

25. Для настройки привилегий учётных записей пользователей осуществить следующие действия:

вывести в терминал заданные в ОССН привилегии учётных записей пользователей командой usercaps, при работе в терминале Fly в «привилегированном» режиме;

запустить графическую утилиту «Политика безопасности» и открыть настройки учётной записи пользователя user1, в вкладке «Привилегии» установить Linux-привилегии cap_kill, cap_fowner и PARSEC-привилегии parsec_cap_chmac, parsec_cap_sig, после чего закончить работу с утилитой;

вывести привилегии учётной записи пользователя user1 командой usercaps user1;

в графической утилите «Политика безопасности» открыть параметры учётной записи пользователя user, в вкладке «Привилегии» выбрать Linux-привилегии cap_kill, cap_fowner и PARSEC-привилегии parsec_cap_chmac, parsec_cap_sig;

запустить терминал Fly в «непривилегированном» режиме командой fly-term и осуществить попытку запуска команды usercaps;

определить расположение файла usercaps командой which usercaps, выполненной из «привилегированного» режима, а затем выполнить в «непривилегированном» режиме команду /usr/sbin/usercaps, проанализировать результат;

запустить терминал Fly в «привилегированном» режиме командой sudo fly-term и выполнить модификацию Linux-привилегий и PARSEC-привилегий командами:

usercaps -l 9 user1

usercaps -m 2 user1

usercaps -m 11 user1

с использованием графической утилиты «Политика безопасности» определить установленные привилегии и формат параметра модификации привилегий учётных записей пользователей (десятичная, восьмеричная или шестнадцатеричная система счисления при этом используется?);

установить для учётной записи пользователя user1 полный список привилегий командой **usercaps -f user1**, затем удалить все привилегии учётной записи пользователя user1 командой **usercaps -z user1**;

вывести списки Linux-привилегий и PARSEC-привилегий командами usercaps -L и usercaps -M, соответственно.

Литература

1. «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1»,

2. «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

3. «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя».

Критерии выставления оценок обучающимся:

Знания, умения и навыки обучающихся определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Общими критериями, определяющими оценку знаний и умений обучающихся на текущем практическом занятии, являются:

«отлично» – наличие глубоких и исчерпывающих знаний в объеме материала практического занятия, правильные, уверенные действия по применению полученных знаний на практике, грамотное, логичное изложение материала при ответе.

«хорошо» – наличие твердых и достаточно полных знаний в объеме материала практического занятия, незначительные ошибки при освещении вопросов, правильные действия по применению знаний на практике, четкое изложение материала при ответе.

«удовлетворительно» – наличие твердых знаний в объеме материала практического занятия, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость в наводящих вопросах экзаменуемому, правильные действия по применению знаний на практике.

«неудовлетворительно» – наличие грубых ошибок в ответах, непонимание сущности излагаемых вопросов, неумении применять знания на практике, неуверенности и неточности в ответах на дополнительные и наводящие вопросы.

Порядок оценки выполнения задания

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

- название практического занятия;
- текст индивидуального задания;
- ход выполнения работы

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

подполковник С. Краснов

(воинское звание, подпись, инициал имени, фамилия автора)

«___»_____202_г.