**Дисциплина «Защита в операционных системах»**
**Лабораторная работа № 10**

**Тема:** Настройка параметров мандатного управления доступом и мандатного контроля целостности.

**Цель:** Освоить администрирование основных параметров мандатного управления доступом и мандатного контроля целостности в ОССН с применением графических утилит и консольных команд.

**Порядок выполнения лабораторной работы:** работа выполняется самостоятельно под руководством преподавателя.

**Время выполнения лабораторной работы (аудиторные часы) -** 4 часа.

**Оборудование и программное обеспечение:** работа выполняется на ПЭВМ типа IBM PC с использованием стандартных функций ОССН Astra Linux.

## 1. Теоретические сведения

В ОССН наряду с традиционной для ОС семейства Linux системой дискреционного управления доступом реализована система мандатного управления доступом и мандатного контроля целостности на основе МРОСЛ ДП-модели. С этим связано наличие у сущностей ОССН (файлов, каталогов) мандатных меток конфиденциальности и целостности.

Параметрами мандатного управления доступом (мандатной меткой) являются следующие элементы:

- уровень доступа или конфиденциальности (соответствует уровню конфиденциальности сущности или доступа субъект-сессии);
- набор неиерархических категорий сущности и субъект-сессии;
- уровень целостности сущности и субъект-сессии;
- специальные атрибуты сущности (CCNR, CCNRI, E.Hole, W-Hole)

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

- 2 непосредственно используемых уровня целостности («Низкий» значение 0, «Высокий» - 63);
- 4 уровня доступа/конфиденциальности («Уровень_0» значение 0, «Уровень_1» - 1, «Уровень_2» - 2, «Уровень_3» - 3);
- неиерархические категории - «Категория_1», «Категория_2».

Мандатное управление доступом процессов (субъект-сессий) к ресурсам (сущностям) основано на реализации соответствующего механизма в ядре ОССН. При этом принятие решения о запрете или разрешении доступа субъект-сессии к сущности осуществляется в соответствии с правилами, описанными в рамках МРОСЛ ДП- модели, и зависит от запрашиваемого вида доступа (чтение, запись, применение права доступа на выполнение) и мандатного контекста (используемых в запросе уровней конфиденциальности, доступа и целостности).

Для администрирования параметров мандатных управления доступом и контроля целостности применяются следующие команды и графические утилиты:

• `pdpl-user` – команда просмотра и изменения допустимых мандатных уровней и неиерархические категорий учётных записей пользователей;

• `pdpl-file` – команда установки параметров мандатного управления доступом на сущность файловой системы;

• `pdp-id` – команда вывода параметров мандатных управления доступом и контроля целостности для текущей сессии;

• `userlev` – команда просмотра и редактирования уровней доступа, заданных в ОССН;

• `usercat` – команда просмотра и редактирования неиерархических категорий учётных записей пользователей в ОССН;

• `usercaps` – команда просмотра и редактирования привилегий учётных: записей пользователей;

• `fly-admin-smc` – графическая утилита, позволяющая решать весь комплекс задач по администрированию учётных записей пользователей и групп, в том числе администрировать параметры мандатных управления доступом и контроля целостности.

## 2. Задание

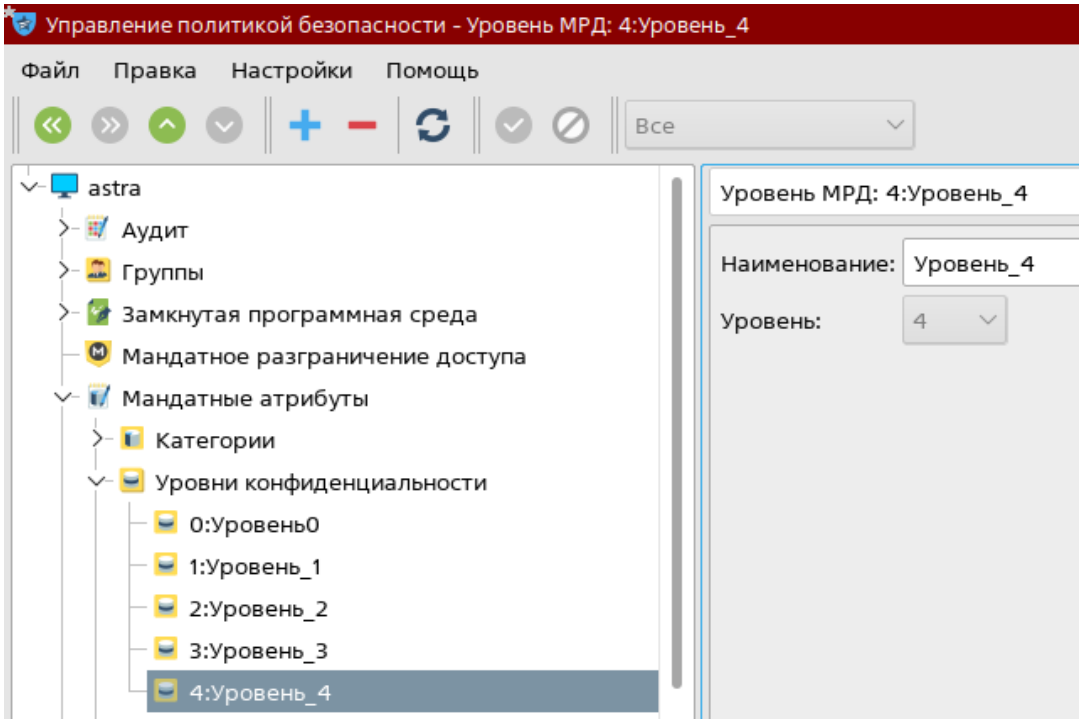
**1.** Начать работу со входа в ОССН в графическом режиме с учётной записью привилегированного пользователя (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).

**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».

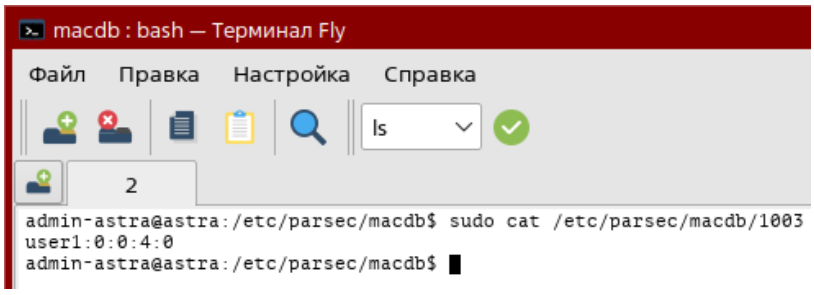
**4.** Создать учётную запись пользователя `user1`, установив максимальный уровень доступа: «Уровень_4».

**5.** Попытаться удалить уровень доступа 4 из раздела «Уровни конфиденциальности» путём выбора в контекстном меню пункта «Удалить». Объяснить результат.

**6.** 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 cat /etc/parsec/macdb/XXXX` (`XXXX – UID` пользователя `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».

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

• в разделе «Категории» (Панель управления → Безопасность → Мандатные атрибуты → Категории) удалить исходные неиерархические категории;

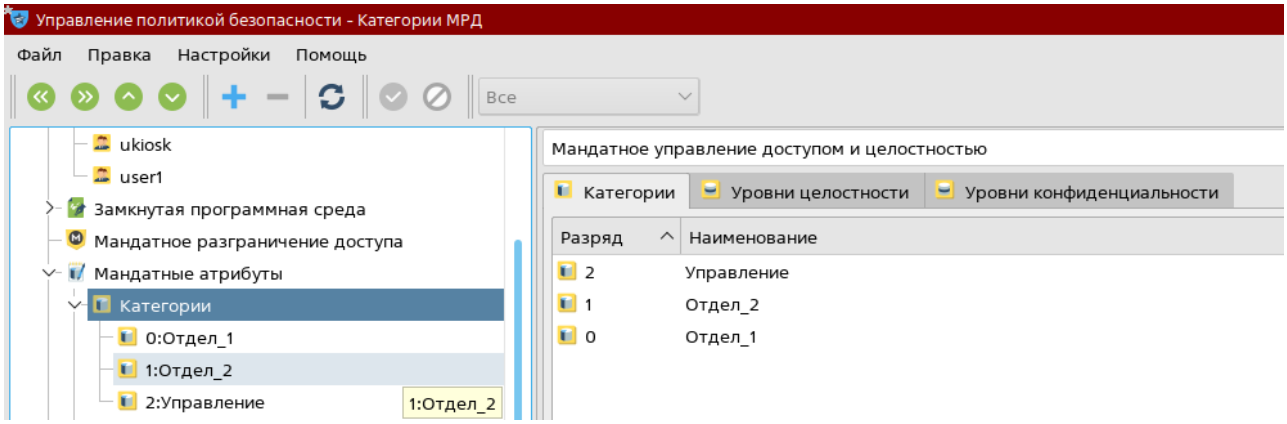
• затем создать новую неиерархическую категорию с именем «Otdel1», «Разряд» - 0;

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

**7.** 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.

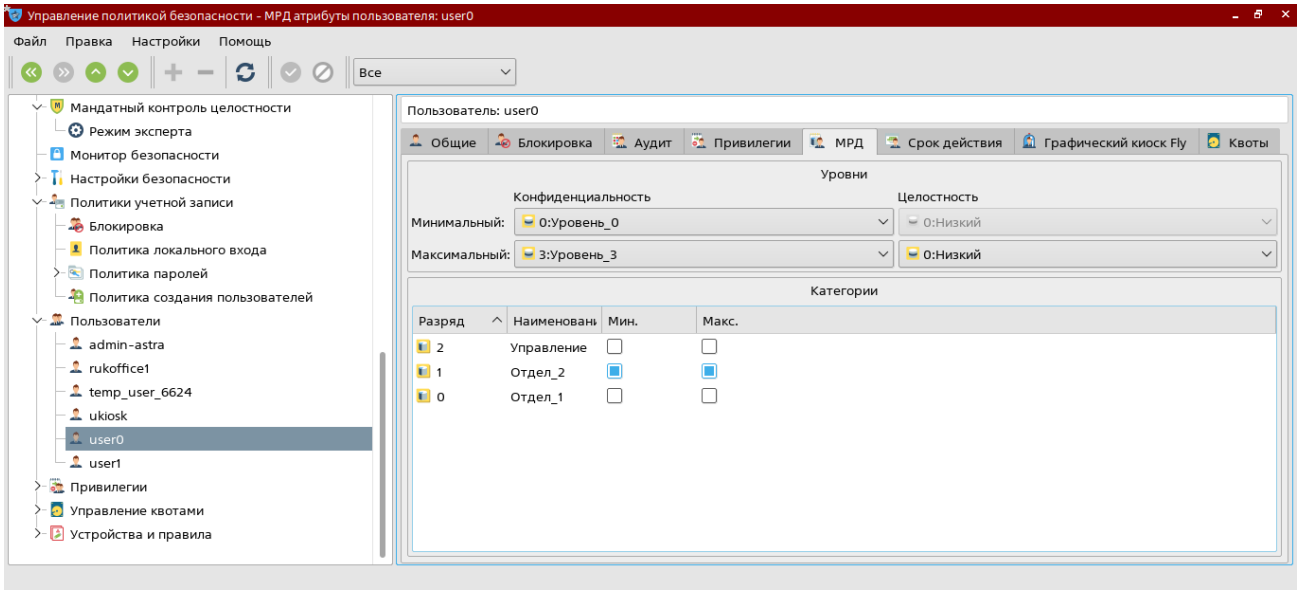



**8.** Изменить мандатный уровень доступа с использованием графической утилиты «Политика безопасности», для этого выполнить следующие действия:

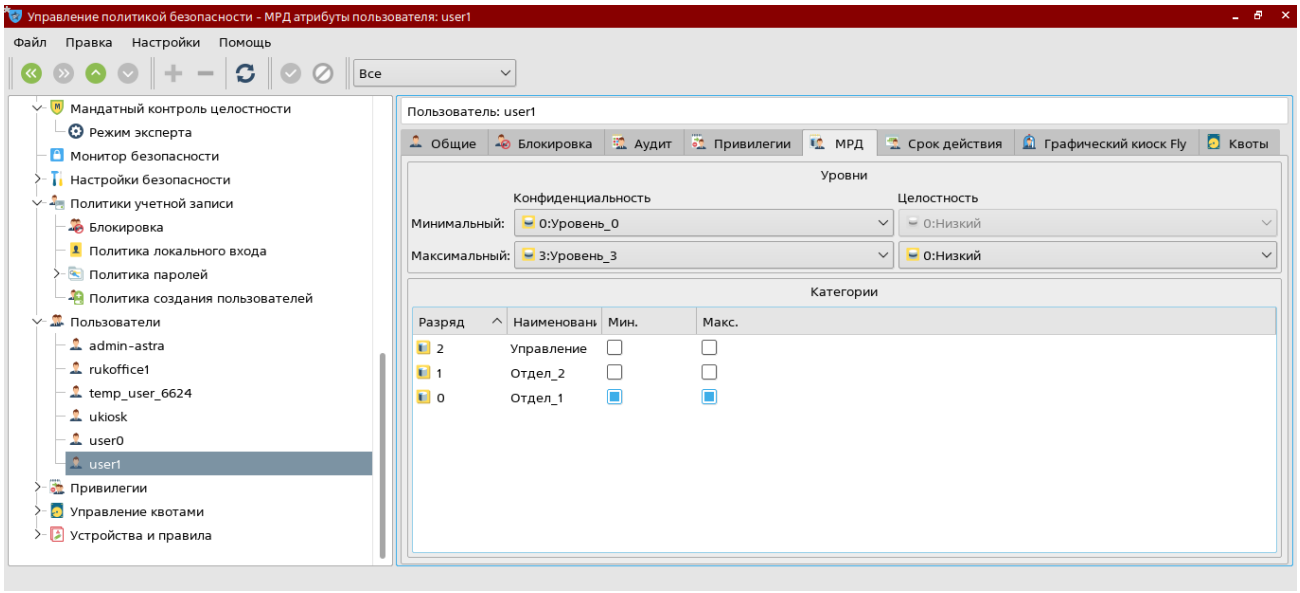
• создать новую группу с именем «office1» и задать первичную группу учётной записи пользователя user1 - «office1»;

• создать новую учётную запись пользователя user0 и установить её первичную группу – «office1»;

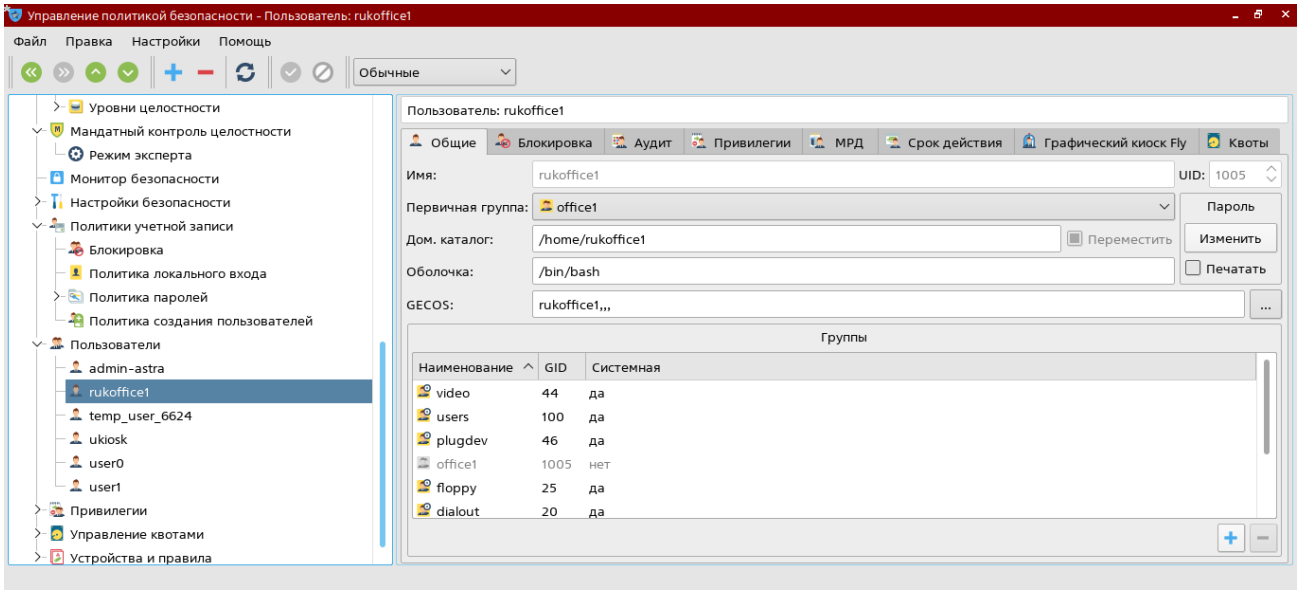
• для учётной записи пользователя user2 в вкладке «МРД» выбрать максимальный уровень доступа — «Уровень_3», максимальный набор неиерархических категорий — «Отдел_2», после чего задать минимальный набор неиерархических категорий — «Отдел_2»;



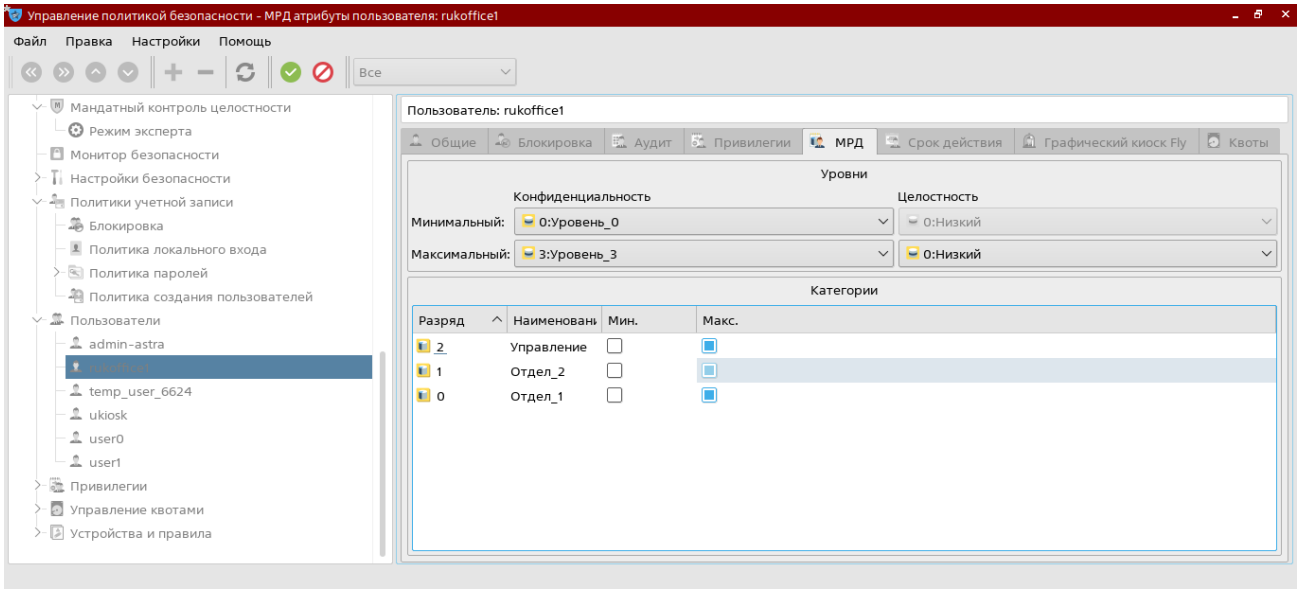

• открыть параметры учётной записи пользователя `user1` и выбрать максимальный уровень доступа — «`Уровень_3`», максимальный набор неиерархических категорий — «`Отдел_1`», минимальный набор неиерархических категорий — «`Отдел_1`»;




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




• в вкладке «МРД» пользователя `rukoffice1` выбрать максимальный уровень: «`Уровень_3`», максимальный набор категорий: «`Отдел_1`», «`Отдел_2`», «`Управление`».




**9.** 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 user1.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 Y1, Y2, Y3 в каталогах otdel1, otdel2, upr командами:

```
mkdir -p otdel1/{Y1,Y2,Y3}
mkdir -p otdel2/{Y1,Y2,Y3}
mkdir -p upr/{Y1,Y2,Y3}
```

и установить соответствующие владельца и группу владельца файлов:

```
chown user1:office1 otdel1/Y{1,2,3}
chown user2:office1 otdel2/Y{1,2,3}
chown rukoffice1:office1 upr/Y{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/Y1
pdpl-file 2:0:Управление:0 /home/work/upr/Y2
pdpl-file 3:0:Управление:0 /home/work/upr/Y3
chown rukoffice1.office1 upr/Y{1,2,3}
chmod 770 upr/Y{1,2,3}
```

**10.** 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/YX 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).

**11.** 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/YX 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 (fly-fm).

**12.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа - 3, неиерархическая категория — «Отдел_2») 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.

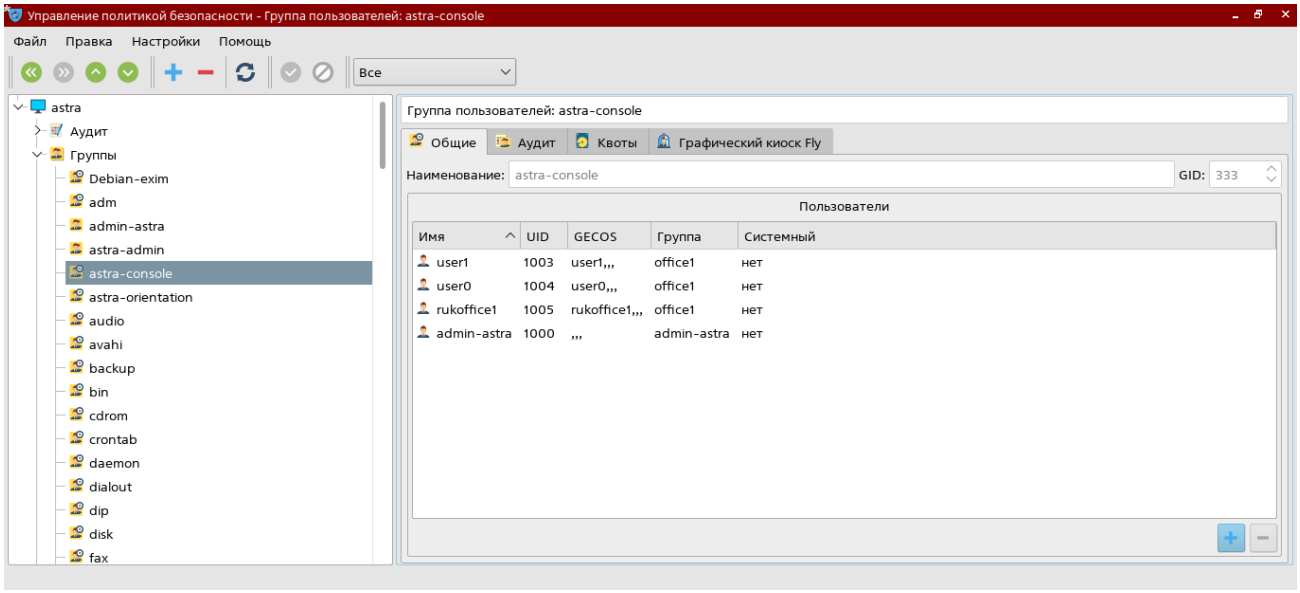
**13.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 2, неиерархическая категория — «Отдел_1») и проверить возможность получения следующих доступов к файлам: **доступ на чтение** к файлам 11.txt, 12.txt, **доступ на запись** к файлу 12.txt.

**14.** 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.

**15.** Войти в ОССН с учётной записью пользователя rukoffice1 (уровень доступа — 3, неиерархическая категория — «Управление»). Создать файл u3.txt в каталоге /home/work/upr/Y3.

**16.** 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. Объяснить результат.

**17.** 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.




**18.** 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;

```
rukoffice1@astra:~$ pdp-id -a
Уровень конф.=2(Уровень_2), Уровень целостности:0(Низкий), Категории=0x5(Отдел_1,Управление)
Роли=()
rukoffice1@astra:~$
```

• 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`.

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

• войти в ОССН с учётной записью привилегированного пользователя (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`;

```
root@astra:/home/admin-astra# pdpl-user -l 0:2 rukoffice1
минимальная метка: Уровень_0:Низкий:Нет:0x0
   0:0:0x0:0x0
максимальная метка: Уровень_2:Низкий:Отдел_1,Отдел_2,Управление:0x0
   2:0:0x7:0x0
```

```
root@astra:/home/admin-astra# pdpl-user -c 0:2 rukoffice1
минимальная метка: Уровень_0:Низкий:Нет:0x0
   0:0:0x0:0x0
максимальная метка: Уровень_2:Низкий:Отдел_2:0x0
   2:0:0x2:0x0
```

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

```
root@astra:/home/admin-astra# pdpl-user -z rukoffice1
минимальная метка: Уровень_0:Низкий:Нет:0x0
   0:0:0x0:0x0
максимальная метка: Уровень_0:Низкий:Нет:0x0
   0:0:0x0:0x0
```

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

```
root@astra:/home/admin-astra# pdpl-user -l 1:3 -c 0:7 rukoffice1
минимальная метка: Уровень_1:Низкий:Нет:0x0
   1:0:0x0:0x0
максимальная метка: Уровень_3:Низкий:Отдел_1,Отдел_2,Управление:0x0
   3:0:0x7:0x0
```

**20.** 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.

**21.** 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_5`» (значение 5) командой `userlev Уровень_5 --add 5` и вывести в терминал уровни доступа командой `userlev`;

• выполнить переименование уровня доступа «Уровень_5» в «НовыйУровень» командой userlev Уровень_5 — rename НовыйУровень;

• удалить уровень доступа с именем «НовыйУровень» командой userlev НовыйУровень --delete 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 -i 1:4 rukoffice1;

```
root@astra:/etc/parsec/macdb# pdpl-user -i 1:4 rukoffice1
минимальная метка: Уровень_1:Низкий:Нет:0x0
   1:0:0x0:0x0
максимальная метка: Уровень_3:Сетевые_сервисы:Отдел_1,Отдел_2,Управление:0x0
   3:1:0x7:0x0
```

• 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 -i 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 -i 1:3 -c 0:7 rukoffice1.

**22.** Создать и модифицировать неиерархические категории:

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

• добавить новую неиерархическую категорию командой usercat 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;

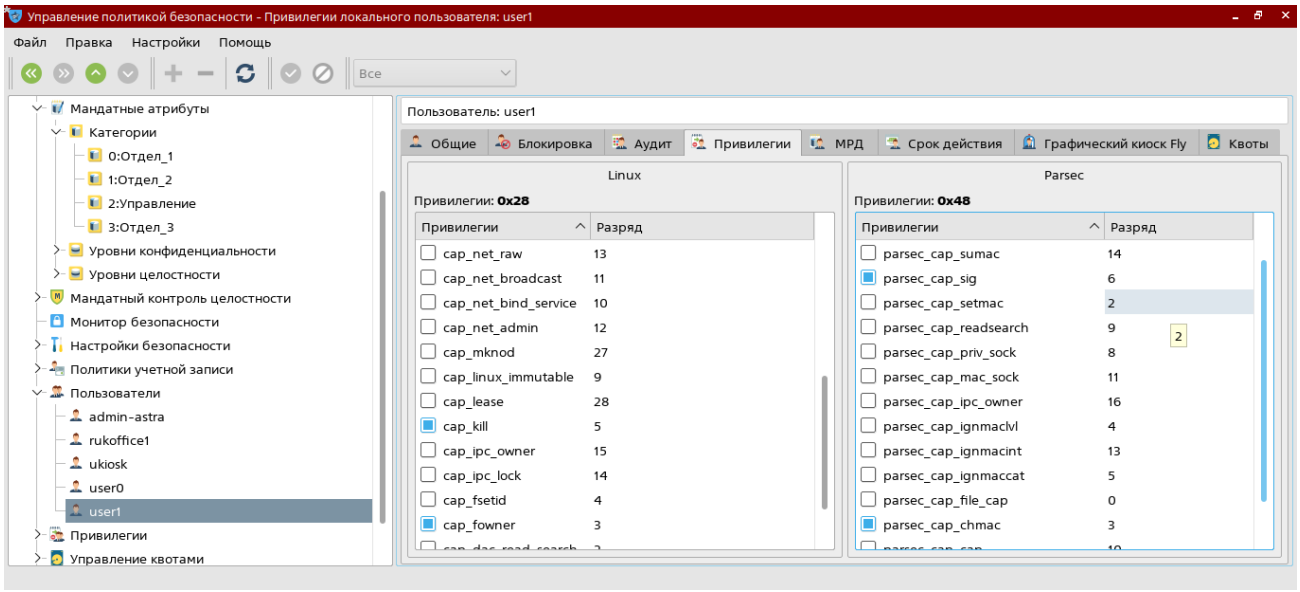
• изменить значение неиерархической категории «Управление» на 0x10 командой usercat Управление --modify 10, проанализировать результат по данным, выводимым командой pdpl-user rukoffice1;

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

**22.** 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`;

```
root@astra:/etc/parsec/macdb# usercaps user1
------------------
linux-привилегии:
 3 cap_fowner
 5 cap_kill
------------------
PARSEC-привилегии:
 3 parsec_cap_chmac
 6 parsec_cap_sig
```

• в графической утилите «Политика безопасности» открыть параметры учётной записи пользователя `user2`, 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:
```

```
root@astra:/etc/parsec/macdb# usercaps -l 9 user1
------------------
linux-привилегии:
 0 cap_chown
 3 cap_fowner
root@astra:/etc/parsec/macdb# usercaps -m 2 user1
------------------
PARSEC-привилегии:
 1 parsec_cap_audit
root@astra:/etc/parsec/macdb# usercaps -m 11 user1
------------------
PARSEC-привилегии:
 0 parsec_cap_file_cap
 4 parsec_cap_ignmaclvl
```

• 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.

## 3. Контрольные вопросы

1. Какие уровни доступа и неиерархические категории создаются при установке ОССН?
2. Как настроить минимальный и максимальный уровни доступа учётной записи пользователя с использованием графической утилиты fly-admin-smc?
3. Как добавить новые уровни доступа и неиерархические категории в ОССН?
4. Какие имеются особенности удаления и модификации уровней доступа и неиерархических категорий в ОССН?
5. Какие команды используются для создания, модификации и удаления уровней доступа и неиерархических категорий в ОССН?
6. Какие команды используются для настройки привилегий учётных записей пользователей?
7. Как принудительно удалить все привилегии для заданной учётной записи пользователя?
8. Какие существуют особенности настройки привилегий учётных записей пользователей в «непривилегированном» режиме?

## 4. Требования к отчёту

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4. На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, группа, проверил: преподаватель ФИО (образец титульного листа представлен в приложении 1).

Отчет должен содержать:

— титульный лист;
— цель работы;
— краткие теоретические сведения, ответы на контрольные вопросы;
— описание хода выполнения работы со скриншотами:

- полный перечень использованных команд с кратким описанием их назначения;
- примеры выполнения команд, которые были использованы в ходе работы с описанием результатов их выполнения;
- описание порядка работы с графической утилитой «Политика безопасности» при выполнении следующих действий:
  - создание, изменение и удаление уровней доступа и неиерархических категорий;

- настройка уровней доступа и неиерархических категорий учётных записей пользователей;
- создание общих каталогов для совместного использования несколькими учётными записями пользователей.

- описание порядка работы и команд, использованных при осуществлении следующих действий:
  - настройка уровней доступа и неиерархических категорий в ОССН;
  - настройка уровней доступа и неиерархических категорий учётных записей пользователей.
- описание особенностей функционирования команд при работе в «привилегированном» и «непривилегированном» режимах;
- список и назначение системных файлов, связанных с хранением параметров мандатных управления доступом и контроля целостности;
- описание команд при настройке привилегий учётных записей пользователей.

— выводы

**Приложение 1**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(ДГТУ)**

Факультет Информатика и вычислительная техника
Кафедра Кибербезопасность информационных систем

**Лабораторная работа № ____**
на тему «_____»

Выполнил обучающийся гр._____

_____
(Фамилия, Имя, Отчество)

Проверил:

_____
(должность, Фамилия, Имя, Отчество)

Ростов-на-Дону
20____