

# ЛАБОРАТОРНАЯ РАБОТА №1.

## РАБОТА С УЧЕТНЫМИ ЗАПИСЯМИ

### ПОЛЬЗОВАТЕЛЕЙ И ГРУППАМИ. НА- СТРОЙКА КВОТ

**Цель работы:** Изучить особенности администрирования локальных учётных записей пользователей и групп в ОССН с использованием командной строки и графического интерфейса.

**Время выполнения работы:** 1 академический час.

#### Краткие теоретические сведения

ОССН — многопользовательская ОС, потому учётная запись пользователя — ключевой элемент всей системы управления доступом. Для идентификации учётных записей пользователей и групп в ОССН как во всех ОС семейства *Linux* используются *uid* и *gid*, соответственно. Каждая учётная запись пользователя должна принадлежать как минимум одной группе — первичной группе. При создании учётной записи пользователя командой *adduser* или с использованием графической утилиты *fly-admin-smc* создаётся группа, имя которой совпадает с системным именем учётной записи пользователя. Данная группа применяется как первичная группа и будет задана идентификатором в учётной записи пользователя, расположенной в файле */etc/passwd*. учётная запись пользователя может входить более чем в одну группу, тогда имена таких групп (в ОССН данные группы называются вторичными) будут находиться в файле */etc/group*.

Данные об учётных записях пользователей и группах хранятся в файлах */etc/passwd* и */etc/group*, соответственно. Если в файле */etc/passwd* для некоторой учётной записи пользователя вместо пароля указан символ «х», то свёртка пароля находится в файле */etc/shadow*. Его структура представляет собой список, каждая строка которого состоит из элементов, разделённых символом «:», среди которых: число дней с 1 января 1970 г. до дня последнего изменения пароля, минимальное число дней действия пароля со дня его последнего изменения, максимальное число дней действия пароля, за сколько дней до устаревания пароля ОССН начнёт выдавать предупреждения, число дней со времени обязательной смены пароля до блокировки учётной записи пользователя, день блокировки учётной записи пользователя.

Для администрирования параметров учётных записей пользователей используются следующие команды и утилиты:

- *useradd* и *adduser* — команды добавления учётной записи пользователя;
- *passwd* — команда смены пароля учётной записи пользователя;
- *usermod* — команда модификации параметров уже существующей учётной записи;
- *userdel* — команда удаления учётной записи пользователя;
- *gpasswd* — команда управления группами;
- *addgroup* — команда создания группы;
- *delgroup* — команда удаления группы;
- *fly-admin-smc* — графическая утилита, позволяющая решать весь комплекс задач по администрированию учётных записей пользователей и групп, в том числе администрировать параметры мандатного управления доступом и мандатного контроля целостности.

### **Используемое методическое и лабораторное обеспечение**

1. ОССН версии 1.6, в которой создана учётная запись пользователя *user*, 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*).
2. Документация: «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя».
3. Для выполнения работы в течение двух занятий необходимо обеспечить возможность сохранения состояния ОССН за счёт применения технологий виртуализации (создания виртуальных машин с ОССН).

### **Порядок выполнения работы**

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 терминал *Fly* из меню «Системные».
3. Определить текущую учётную запись пользователя с использованием команды *whoami*.

4. Проверить наличие права доступа на чтение к файлу `/etc/passwd` и получить следующие данные, выполнив команды `cat /etc/passwd` или `less /etc/passwd`:

- количество параметров учётных записей пользователей (для этого дополнительно можно использовать команды `wc` и `sort`);
- текущее число учётных записей пользователей;
- количество различных используемых командных интерпретаторов.

5. Вывести строку, соответствующую текущей учётной записи пользователя, из файла `/etc/passwd` с использованием команды `cat /etc/passwd | grep "^$(whoami):"`, при этом получить следующие данные:

- наличие пароля или свёртки пароля (вывести эти данные командой `cat /etc/passwd | grep "^$(whoami):" | cut -d : -f 2`);

```
root@astra:/home/user# cat /etc/passwd | grep "^$(whoami):"
root:x:0:0:root:/root:/bin/bash
root@astra:/home/user# exit
exit
user@astra:~$ cat /etc/passwd | grep "^$(whoami):"
user:x:1000:1000:,,,:/home/user:/bin/bash
```

- группа и идентификатор текущей учётной записи пользователя;
- командный интерпретатор по умолчанию для текущей учётной записи пользователя.

6. Найти отличия исполняемых файлов `adduser` и `useradd`, для чего:

- определить расположение файлов `adduser` и `useradd` с использованием команд `sudo which adduser` и `sudo which useradd`;
- вывести в терминал `Fly` тип обоих файлов командой `file`, определить их принципиальное отличие.

7. Добавить две учётные записи пользователей `user1` и `user2` (с соответствующими домашними каталогами) с использованием команд `sudo adduser user1` и `sudo adduser user2`.

8. Проанализировать изменения в ОСН, связанные с добавлением новых учётных записей пользователей, для чего определить:

- домашние каталоги учётных записей пользователей по данным файла `/etc/passwd`;
- номер алгоритма свёртки паролей учётных записей пользователей по файлу `/etc/shadow` с использованием привилегированного режима или команды `sudo`;

```
root@astra:/home/user# cat /etc/shadow | grep "^user:" | cut -d$ -f2
6
```

- скрипты, которые были перемещены в домашние каталоги учётных записей пользователей из каталога `/etc/skel`, при этом сравнить файлы в каталоге `/etc/skel` с файлами домашних каталогов учётных записей пользователей с использованием команды `sudo diff -s /etc/skel /home/имя_пользователя | grep "идентичны"`;

- новые группы в файле */etc/group*;
- идентификаторы новых учётных записей пользователей и групп в файлах */etc/group* и */etc/passwd*.

9. Осуществить попытку создания учётных записей пользователей *user3*, *user4* командами *useradd user3* и *useradd user4* без использования команды *sudo*, проанализировать результат. Выполнить те же действия с применением команды *sudo*, после чего определить:

- домашние каталоги учётных записей пользователей по файлу */etc/passwd*;
- были ли созданы домашние каталоги учётных записей пользователей;
- наличие свёрток паролей учётных записей пользователей по файлам */etc/passwd* и */etc/shadow*;
- новые группы в файле */etc/group*;
- идентификаторы новых учётных записей пользователей в файле */etc/passwd*;

```
root@astra:/home/user# tail -1 /etc/passwd | cut -d: -f7  
/bin/bash
```

- командный интерпретатор по умолчанию для созданных учётных записей пользователей.

10. Реализовать попытки задать пароль для учётных записей пользователей *user3* и *user4* с использованием команд *passwd user3* и *passwd user4* без использования и с использованием команды *sudo*, сравнить результаты. Определить алгоритм свёртки пароля этих учётных записей пользователей по файлу */etc/shadow*.

11. Выполнить дополнительную настройку ОССН для обеспечения возможности входа с учётной записью пользователя *user3*, для чего осуществить следующие действия:

- выполнить вход в ОССН с учётной записью пользователя *user3*, введя его имя и пароль, проанализировать предупреждения, выдаваемые ОССН;
- войти в ОССН с учётной записью пользователя *user*;
- создать домашний каталог учётной записи пользователя *user3* командами *sudo mkdir /home/user3*, и назначить ему необходимые права доступа: *sudo chown user3:user3 /home/user3*, *sudo chmod 750 /home/user3*;
- проверить возможность входа в ОССН с учётной записью пользователя *user3*;
- войти в ОССН с учётной записью пользователя *user*.

12. Запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*.

- 13. Модифицировать параметры учётных записей пользователей:
- установить домашний каталог учётной записи пользователя *user1* командой *usermod -d /home/userone user1*;
- установить домашний каталог учётной записи пользователя *user2* командой *usermod -m -d /home/usertwo user2*;

- проверить содержимое каталога */home* командой *ls -la* и определить отличия в результатах выполнения команды *usermod* на предыдущих этапах.
14. Осуществить последовательные попытки входа в ОССН с учётными записями созданных пользователей *user1* и *user2*, при этом выполнить следующие действия:
- проанализировать причины появления предупреждений при входе в ОССН с учётной записью пользователя *user1*, сравнив отличия в командах, использованных при модификации параметров учётных записей пользователей *user1* и *user2*;
  - вернуть домашний каталог учётной записи пользователя *user1* командой *usermod -d /home/user1 user1*, рассмотреть результат её выполнения, проверить запись о домашнем каталоге в файле */etc/passwd*;
  - повторно установить домашний каталог пользователя *user1* командой *usermod -m -d /home/userone user1*, проверить результат;
  - проверить возможность входа в ОССН с учётной записью пользователя *user1*, выйти из ОССН.
15. Задать квоты пользователю *user1* и проверить их действие. Для этого:
- открыть **Пуск → Панель управления → Безопасность → Управление политикой безопасности**
  - в разделе Управление квотами (вкладка Общие настройки) включить поддержку квот для пользователей.
16. Задать квоты для группы *group1* (если группа не создана, создайте ее, используя команду *groupadd*). При выполнении данного пункта ориентируйтесь на п.15.

# ЛАБОРАТОРНАЯ РАБОТА №2.

## РАБОТА С УЧЕТНЫМИ ЗАПИСЯМИ

### ПОЛЬЗОВАТЕЛЕЙ И ГРУППАМИ. ОСНОВА

### МАНДАТНОГО УПРАВЛЕНИЯ ДОСТУПОМ

**Цель работы:** Изучить особенности администрирования локальных учётных записей пользователей и групп в ОССН и основы мандатного управления доступом.

**Время выполнения работы:** 2 академических часа.

#### Краткие теоретические сведения

Как правило, файлы, владельцами которых являются учётные записи пользователей, хранятся в соответствующих им домашних каталогах, находящихся в каталоге */home*. При этом, во время первого входа в ОССН с заданными уровнем доступа (*Num1*), уровнем целостности (*Num2*) и набором неиерархических категорий (*Num3*) (например, 0x2 — вторая категория) создаётся уникальный каталог с именем вида:

*/home/.pdp/имя\_пользователя/Num1iNum2cNum3t0x0,*

что позволяет распределить по каталогам файлы (в том числе, документы) в зависимости от их уровней конфиденциальности и целостности. Доступ субъект-сессий (процессов), функционирующих от имени других учётных записей пользователей, к домашнему каталогу в ОССН версии 1.6 может быть ограничен с использованием как параметров (меток конфиденциальности) мандатного управления доступом, так и дискреционных прав доступа.

При работе от имени учётной записи администратора в ОССН версии 1.6 желательно использовать только высокий уровень целостности (по умолчанию он равен 63) и минимальный уровень конфиденциальности в связи с особенностями монтирования его домашнего каталога.

При администрировании ОССН необходимо руководствоваться следующими рекомендациями. Если в ней включён мандатный контроль целостности на файловой системе, то для администрирования ОССН требуется его временно отключить, для чего:

1. снять мандатный контроль целостности с файловой системы ОССН с помощью графической утилиты *fly-admin-smc* или командой *unset-fs-ilev*;
2. выполнить необходимые действия по администрированию ОССН (настроить ОССН, установить пакеты, и т. д.);

3. включить мандатный контроль целостности на файловой системе ОССН с помощью графической утилиты *fly-admin-smc* или командой *set-fs-ilev*;
4. настроить метки целостности установленных системных объектов.

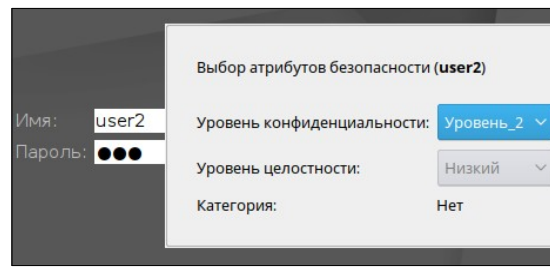
Для полного выключения режима мандатного контроля целостности:

5. при использовании графического интерфейса с помощью графической утилиты *fly-admin-smc* выбрать «Мандатный контроль целостности» и снять отметку «подсистема МКЦ»;
6. при использовании терминала *Fly* выполнить команду *astra-mic-control disable*.

Независимо от способа выключения, чтобы изменения вступили в силу необходимо перезагрузить ОССН. Полностью выключать мандатный контроль целостности крайне не рекомендуется, т.к. многие механизмы защиты связаны с его включённым режимом, а именно: блокировка интерпретаторов, режим блокировки установки бита исполнения – *nochmodx*, блокировка доступа к конфиденциальной информации и т.д.

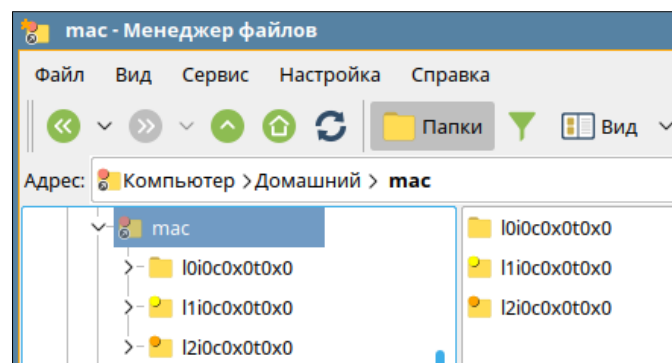
### Порядок выполнения работы

1. Войти в ОССН с учётной записью пользователя *user* (Уровень\_0, «Высокий»). Запустить графическую утилиту редактирования учётных записей пользователей «Политика безопасности» через меню «Панель управления» главного пользовательского меню.
2. Открыть раздел настройки локальных пользователей, и для созданных учётных записей пользователей *user1*, *user2*, *user3*, *user4* произвольно задать их параметры:
  - максимальный и минимальный уровни доступа;
  - минимальные и максимальные наборы неиерархических категорий;
  - максимальный уровень целостности.
  1. Настроить параметры учётной записи пользователя *user2*:
    - установить минимальное количество дней между сменой пароля – 180 дней, число дней до выдачи предупреждения о смене пароля — 5 дней;
    - выбрать максимальный уровень — «Уровень\_3»;
    - проверить возможность задать минимальный или максимальный набор неиерархических категорий.
  1. Войти в ОССН с учётной записью пользователя *user2*, выбрав уровень доступа «Уровень\_1». Проверить возможность выбора набора неиерархических категорий и уровня целостности. Создать в каталоге «Документы» файл *1.txt*. Выйти из ОССН.
  2. Войти в ОССН с учётной записью пользователя *user2*, выбрав уровень доступа «Уровень\_2». Создать в каталоге «Документы» файл *2.txt*.



3. Проверить возможность чтения объектов файловой системы ОССН, владельцем которых является учётная запись пользователя *user2* (на текущем уровне доступа «Уровень\_2»):

- открыть каталог «Документы» уровня доступа «Уровень\_1» (Компьютер/Домашний/*mac*/*I0i0c0x0t0x0*/Документы);



- открыть файл *1.txt*, проверив возможность его чтения или записи;
- выйти из ОССН.
  1. Проверить наличие и возможность чтения объектов файловой системы ОССН, владельцем которых является учётная запись пользователя *user2* на текущем уровне доступа («Уровень\_1»):
- войти в ОССН с учётной записью пользователя *user2*, выбрав уровень доступа «Уровень\_1»;
- проверить возможность открытия каталога «Документы» для уровня доступа «Уровень\_2» (Компьютер/Домашний/*mac*/*I2i0c0x0t0x0*/Документы);
- выйти из ОССН.
  1. Войти в ОССН с учётной записью пользователя *user*. Запустить графическую утилиту «Политика безопасности». Сравнить списки вторичных групп для учётных записей пользователей *user*, *user1*, *user2*, *user3*, *user4*, при этом определив:
    - учётные записи пользователей, являющиеся администраторами (входящими в группу *astra-admin*);
    - учётные записи пользователей, входящие в группу *users*.
      1. Создать новую учётную запись пользователя *user10*, при этом:



- установить минимальное количество дней между сменой пароля — 180 дней и число дней выдачи предупреждения до смены пароля — 5 дней;
- выбрать максимальный уровень доступа — «Уровень\_3», минимальный уровень доступа — «Уровень\_0», уровень целостности — «Высокий»;
- добавить в список вторичных групп группы *astra-admin* и *lpadmin*;
- проверить возможность входа в ОССН с учётной записью пользователя *user10* с уровнями доступа «Уровень\_2» или «Уровень\_3» (уровень целостности «Низкий»).
- 1. Войти в ОССН с учётной записью пользователя *user10* (уровень доступа — «Уровень\_0», уровень целостности «Высокий»). Проверить возможность создания новой учётной записи пользователя *user11* с использованием графической утилиты *fly-admin-smc* без использования и с использованием команды *sudo*. Выйти из ОССН.
- 2. Войти в ОССН с учётной записью пользователя *user1* с уровнем доступа — «Уровень\_0». Осуществить попытки запуска графической утилиты «Политика безопасности» через главное пользовательское меню и запуска её с использованием терминала *Fly* командой *fly-admin-smc*. Проанализировать результаты и предупреждения ОССН.
- 3. Осуществить переключение между сеансами различных учётных записей пользователей без выхода из ОССН:
- через меню «Завершение работы» главного пользовательского меню перейти в подменю «Сессия» и далее «Отдельная» и войти в ОССН с учётной записью пользователя *user* (уровень целостности «Высокий»);
- аналогично вернуться и далее закрыть сеанс от имени учётной записи пользователя *user1*.
- 1. С использованием графической утилиты «Политика безопасности» заблокировать пароль учётной записи пользователя *user1*. Проверить изменения файлов */etc/passwd* и */etc/shadow*, осуществив следующие действия:
- в терминале *Fly* выполнить команды *sudo cat /etc/passwd* и *sudo cat /etc/shadow*;
- проверить наличие блокировки учётной записи пользователя по файлу */etc/shadow* (должен быть установлен знак «!» в начале свёртки пароля);
- проверить функционирование блокировки путём осуществления попытки входа в ОССН в отдельном сеансе от имени учётной записи пользователя *user1*;
- снять блокировку (выполнить удаление пароля и блокировки входа, задать повторно пароль) и проверить возможность входа в ОССН с учётной записью пользователя *user1*.
- 1. Выполнить удаление учётных записей пользователей:
- удалить учётную запись пользователя *user10* с использованием графической утилиты «Политика безопасности»;

- удалить учётную запись пользователя *user2* командой *sudo deluser user2*;
- удалить учётную запись пользователя *user1* командой *sudo userdel user1*;
- проверить наличие домашних каталогов учётных записей пользователей *user1* и *user2*, после чего с использованием справочной информации по команде *userdel* определить её параметры, позволяющие удалять содержимое домашнего каталога учётной записи пользователя;
- удалить домашние каталоги учётных записей пользователей *user1* и *user2* непосредственно командами *rm -r /home/userone* и *rm -r /home/usertwo*, осуществив попытки удаления без использования и с использованием команды *sudo*;
- проверить наличие домашних каталогов учётных записей пользователей *user1*, *user2* и *user10* в каталоге */home/.pdp*.
  1. Создать новую группу *group3* (с использованием графической утилиты «Политика безопасности») и группу *group4* (командой *sudo addgroup group4*, выполненной в терминале *Fly*).
  2. Добавить учётную запись пользователя *user3* во вторичную группу *group3* командой *usermod -a -G group3 user3* и во вторичную группу *group4* с помощью графической утилиты «Политика безопасности». Проверить включение учётной записи пользователя *user3* в группы *group3* и *group4* путем просмотра содержимого файла */etc/group* командами *cat /etc/group | grep "^group3"* и *cat /etc/group | grep "^group4"*
  3. Выполнить удаление учётной записи пользователя *user3* из группы *group3* с использованием графической утилиты «Политика безопасности» и из группы *group4* командой *gpasswd -d user3 group4*.
  4. Удалить группу *group3* командой *sudo delgroup group3* в терминале *Fly* и группу *group4* с помощью графической утилиты «Политика безопасности».
  5. Изучить порядок хранения параметров мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей. Для этого выполнить следующие действия:
    - определить уровни доступа, заданные в ОСН, для этого вывести в терминал *Fly* содержимое файла */etc/parsec/mac\_levels*;
    - определить неиерархические категории, заданные в ОСН, для этого вывести в терминал *Fly* содержимое файла */etc/parsec/mac\_categories*;
    - определить идентификатор учётной записи пользователя *user1* по файлу */etc/passwd* командой *cat /etc/passwd | grep "^user1:" | cut -d : -f 3*;
    - считать параметры мандатного управления доступом и мандатного контроля целостности для учётной записи пользователя *user1* командой *cat /etc/parsec/macdb/\$(cat /etc/passwd |*

`grep "^user1:" | cut -d : -f 3)` и проверить их соответствие данным, отображаемым в графической утилите «Политика безопасности».

## Контрольные вопросы

1. Какие имеются особенности создания учётных записей пользователей с использованием команд *adduser*, *useradd* и графической утилиты «Политика безопасности» (*fly-admin-smc*), в том числе:
  - какой группе должна принадлежать учётная запись пользователя, чтобы была возможность выполнения команды *adduser*?
  - какими командами создаётся учётная запись пользователя, и какие дополнительные параметры при этом вводятся?
  - какие ограничения накладываются на пароль учётной записи пользователя при его создании?
  - в какие группы автоматически добавляется учётная запись пользователя?
1. Как выполнять привилегированные команды?
2. Создаются ли домашние каталоги учётных записей пользователей при добавлении их с использованием графической утилиты «Политика безопасности»?
3. Создаются ли домашние каталоги учётных записей пользователей при их добавлении с использованием команд *adduser* и *useradd*?
4. Какие минимальный и максимальный уровни доступа задаются по умолчанию для учётных записей пользователей, создаваемых командами *adduser* и *useradd*?
5. Какими способами можно добавить или удалить учётную запись пользователя из группы?
6. Каким образом организовано хранение сущностей файловой системы ОССН, созданных процессами, обладающими различными уровнями доступа?
7. Где и в каком формате хранятся параметры мандатного управления доступом и мандатного контроля целостности, заданные в ОССН?
8. Где и в каком формате хранятся параметры мандатного управления доступом и мандатного контроля целостности для учётных записей пользователей?
9. Какой командой задаётся максимальный набор неиерархических категорий для текущей учётной записи пользователя?
10. Каким образом осуществляется переход от текущего сеанса к сеансу, функционирующему от имени другой учётной записи пользователя?
11. Позволяют ли команды *useradd* и *adduser* задавать параметры мандатного управления доступом и мандатного контроля целостности для создаваемых учётных записей пользователей?



# ЛАБОРАТОРНАЯ РАБОТА №3.

## НАСТРОЙКА ПАРАМЕТРОВ МАНДАТНОГО УПРАВЛЕНИЯ ДОСТУПОМ И МАНДАТНО- ГО КОНТРОЛЯ ЦЕЛОСТНОСТИ.

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

**Время выполнения работы:** 4 академических часа.

### Краткие 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:

1. уровень доступа или конфиденциальности (соответствует уровню конфиденциальности сущности или доступа субъект-сессии);
2. набор неиерархических категорий сущности и субъект-сессии;
3. уровень целостности сущности и субъект-сессии;
4. специальные атрибуты сущности (*CCNR*, *CCNRI*, *E\_Hole*, *W\_Hole*).

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

5. 2 непосредственно используемых уровня целостности («Низкий» значение 0, «Высокий» – 63);
6. 4 уровня доступа/конфиденциальности («Уровень\_0» значение 0, «Уровень\_1» – 1, «Уровень\_2» – 2, «Уровень\_3» – 3);
7. 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:

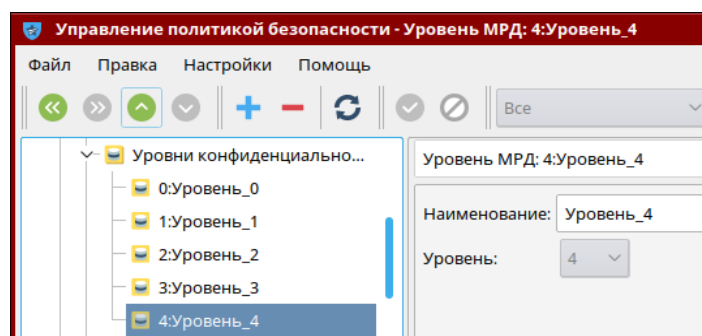
8. *pdpl-user* — команда просмотра и изменения допустимых мандатных уровней и неиерархические категорий учётных записей пользователей;
9. *pdpl-file* — команда установки параметров мандатного управления доступом на сущность файловой системы;
10. *pdp-id* — команда вывода параметров мандатных управления доступом и контроля целостности для текущей сессии;
11. *userlev* — команда просмотра и редактирования уровней доступа, заданных в ОССН;
12. *usercat* — команда просмотра и редактирования неиерархических категорий учётных записей пользователей в ОССН;
13. *usercaps* — команда просмотра и редактирования привилегий учётных записей пользователей;
14. *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.

## **Используемое методическое и лабораторное обеспечение**

1. ОССН версии 1.6, в которой создана учётная запись пользователя *user*, 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*).
2. Документация: «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя».
3. Для выполнения работы в течение двух занятий необходимо обеспечить возможность сохранения состояния ОССН за счёт применения технологий виртуализации (создания виртуальных машин с ОССН).

## Порядок выполнения работы

1. Начать работу со входа в ОСЧН 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».
1. Создать учётную запись пользователя *user1*, установив максимальный уровень доступа: «Уровень\_4».
  2. Выполнить удаление уровня доступа 4 из раздела «Уровни конфиденциальности» путём выбора в контекстном меню пункта «Удалить».
  3. 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.
  4. 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/parsecl/macdb*;

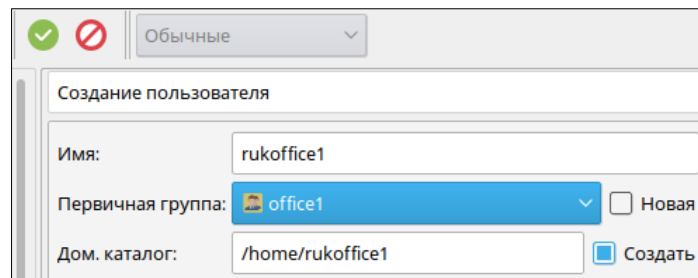
- прочитать параметры учётной записи *user1* командой *sudo grep* “*user1:*” \*;

```
user@astra:/etc/parsec/macdb$ sudo grep "^user1:" *
1001:user1:0:0:4:0
```

- 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».
  1. 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).
  1. 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».
    1. 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».
  - 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}
```

1. 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/уровеньХ* 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*).
2. 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/уровеньХ* 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*.
3. 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*.

4. 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*.
5. 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*.
6. Войти в ОССН с учётной записью пользователя *rukoffice1* (уровень доступа — 3, неиерархическая категория — «Управление»). Создать файл *u3.txt* в каталоге */home/work/lupr/U3*.
7. 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*.
8. 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*.
9. 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*.
  1. 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*.

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

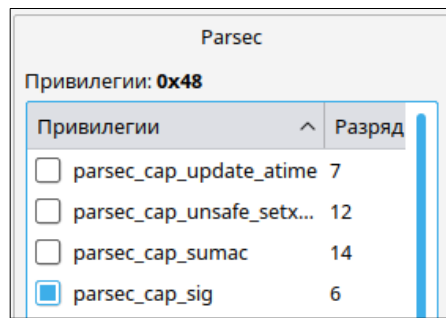
- перейти в каталог */etc/passwd/macdb* и считать минимальный и максимальный уровни доступа командами *grep "rukoffice1" \* | cut -d : -f 3* и *grep "rukoffice1" \* | cut -d : -f 5*, соответственно;
- считать минимальный и максимальный наборы неиерархических категорий командами *grep "rukoffice1" \* | cut -d : -f 4* и *grep "rukoffice1" \* | cut -d : -f 6*, соответственно.

1. 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*.
- 1. 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*.
- 1. Для настройки привилегий учётных записей пользователей осуществить следующие действия:
- вывести в терминал заданные в ОССН привилегии учётных записей пользователей командой *userscaps*, 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
```

```
root@astra:/# usercaps -l 9 user1
-----
linux-npuBunerguu:
0 cap_chown
3 cap_fowner
root@astra:/# usercaps -m 2 user1
-----
PARSEC-npuBunerguu:
1 parsec_cap_audit
root@astra:/# usercaps -m 11 user1
-----
PARSEC-npuBunerguu:
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.

### **Содержание отчёта по выполненной работе**

В отчёте о выполненной работе необходимо указать:

1. Полный перечень использованных команд с кратким описанием их назначения.
  2. Примеры выполнения команд, которые были использованы в ходе работы с описанием результатов их выполнения.
  3. 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.
1. 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.
1. Описание особенностей функционирования команд при работе в «привилегированном» и «непривилегированном» режимах.
  2. Список и назначение системных файлов, связанных с хранением параметров мандатных управления доступом и контроля целостности.
  3. Описание команд при настройке привилегий учётных записей пользователей.

### **Контрольные вопросы**

4. Какие уровни доступа и неиерархические категории создаются при установке ОССН?
5. Как настроить минимальный и максимальный уровни доступа учётной записи пользователя с использованием графической утилиты *fly-admin-smc*?
6. Как добавить новые уровни доступа и неиерархические категории в ОССН?
7. Какие имеются особенности удаления и модификации уровней доступа и неиерархических категорий в ОССН?

8. Какие команды используются для создания, модификации и удаления уровней доступа и неиерархических категорий в ОССН?
9. Какие команды используются для настройки привилегий учётных записей пользователей?
10. Как принудительно удалить все привилегии для заданной учётной записи пользователя?
11. Какие существуют особенности настройки привилегий учётных записей пользователей в «непривилегированном» режиме?





# ЛАБОРАТОРНАЯ РАБОТА №4.

## ОРГАНИЗАЦИЯ ФАЙЛОВОЙ СИСТЕМЫ

## ОССН ДЛЯ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В

## РАМКАХ МАНДАТНОГО УПРАВЛЕНИЯ

## ДОСТУПОМ И МАНДАТНОГО КОНТРОЛЯ

## ЦЕЛОСТНОСТИ.

**Цель работы:** Изучить особенности настройки мандатного управления доступом и мандатного контроля целостности к каталогам файловой системы ОССН для совместной работы от имени учётных записей пользователей с различными уровнями доступа с документами (файлами) с различными уровнями конфиденциальности.

**Время выполнения работы:** 4 академических часа.

**Краткие теоретические сведения:** В ОССН мандатное управление доступом интегрировано в файловую систему, за счёт хранения в ней не только дискреционных прав доступа, но и мандатных меток файлов с дополнительными специальными атрибутами, определёнными в рамках МРОСЛ ДП-модели. Параметрами мандатного управления доступом и контроля целостности (мандатными метками) каждой сущности файловой системы являются:

- уровень конфиденциальности;
- набор неиерархических категорий;
- уровень целостности;
- специальные атрибуты (*CCNR*, *CCNRI*, *E\_Hole*, *W\_Hole*).

При работе с сущностями файловой системы специальные атрибуты отображаются следующим образом: если установлен атрибут *E\_Hole*, то указывается *ehole* (*whole* для *W\_Hole*), для *CCNR* и *CCNRI* (данные атрибуты по сравнению заданными в МРОСЛ ДП-моделью атрибутами *CCR* и *CCRI* в ОССН реализованы инвертированными) — *ccnr* и *ccnri*, соответственно; если установлены оба атрибута (*CCNR* и *CCNRI*), то указывается *CCNRA*.

Специальный атрибут *CCNR* позволяет осуществлять доступ внутрь контейнера (читать содержимое каталога) без учёта уровня конфиденциальности каталога. Аналогично используется атрибут *CCNRI*, только для работы с мандатным уровнем целостности.

Наличие у сущности файловой системы мандатных меток целостности позволяют дополнительно усилить защиту от несанкционированной модификации файлов, влияющих на безопасность ОССН. Это реализуется установкой уровня целостности «Высокий» на критически важных сущностях (файлах) файловой системы, что предотвращает изменение или удаление таких файлов процессами с низким уровнем целостности.

Для администрирования параметров мандатного управления доступом и мандатного контроля целостности файловой системы в лабораторной работе применяются следующие команды и графические утилиты:

- *pdpl-file* — команда модификации параметров мандатного управления доступом сущностей файловой системы;
- *userlev* — команда просмотра и редактирования уровней доступа, заданных в ОССН;
- *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.

### **Используемое методическое и лабораторное обеспечение**

1. ОССН версии 1.6, в которой создана учётная запись пользователя *user*, 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*).
2. Документация: «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство администратора. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство по КСЗ. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство пользователя».
3. Для выполнения работы в течение двух занятий необходимо обеспечить возможность сохранения состояния ОССН за счёт применения технологий виртуализации (создания виртуальных машин с ОССН).

### **Порядок выполнения работы**

1. Выполнить вход в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).
2. Проверить корректность включения в ОССН мандатного контроля целостности. Для этого запустить графическую утилиту «Политика безопасности» через меню «Панель управления», «Безопасность» главного пользовательского меню. Открыть «Монитор безопасности» и убедиться в корректном статусе параметров «Режим Мандатного Контроля Целостности» и «Установленный на ФС высокий уровень Мандатного Контроля Целостности».
3. Запустить терминал *Fly* и выполнить следующие команды для создания группы пользователей:
  - выполнить попытку создания группы командой *addgroup Office*;
  - выполнить попытку создания группы командой *sudo addgroup Office*;
  - проанализировать полученные ошибки и внести корректировки в команду создания группы;
  - создать группу *office* командой *sudo addgroup office*.
1. Запустить графическую утилиту «Политика безопасности» через меню «Панель управления», «Безопасность» главного пользовательского меню.
2. Разрешить работать учётной записи пользователя *user* до мандатного уровня доступа 3 и с любыми созданными в ОССН неиерархическими категориями.
3. Создать следующие учётные записи пользователей:
  - учётную запись пользователя *manager1*, задав ей минимальный уровень доступа «Уровень\_1», максимальный уровень доступа «Уровень\_2» (при этом выявить правильную последовательность задания данных уровней), минимальная и максимальная неиерархическая категория «Категория\_1» (при этом обратить внимание на необходимость задания минимальной неиерархической категории);
  - учётную запись пользователя *manager2*, задав ей минимальный уровень доступа «Уровень\_1», максимальный уровень доступа «Уровень\_2», минимальная и максимальная неиерархическая категория «Категория\_2»;
  - с использованием команды *sudo* установить для учётной записи пользователя *manager2* первичную группу *office*, затем установить для учётной записи пользователя *manager1* первичную группу *office* (при этом использовать команды типа *usermod -g office имя\_пользователя*).
1. Создать каталог для работы пользователей с различными мандатными уровнями доступа, для этого осуществить следующие действия:
  - создать каталог */home/share* и установить на него мандатные атрибуты 2:0:3:CCNRA командой *pdpl-file 2:0:3:CCNRA /home/share*;

- разрешить пользователям группы *office* записывать и читать каталог */home/share*:  
`setfacl -m g:office:rwX /home/share`;
  - создать каталоги *otdel1* и *otdel2* внутри каталога */home/share*;
  - назначить дискреционные права доступа для каталогов */home/share/otdel1* и */home/share/otdel2*: `setfacl -m g:office:rwX /home/share/otdel1` и `setfacl -m g:office:rwX /home/share/otdel2`;
  - установить мандатные атрибуты *2:0:1:CCNRA* и *2:0:2:CCNRA* для каталогов *otdel1* и *otdel2*, соответственно.
1. Настроить каталоги *otdel1* и *otdel2* для работы пользователей с различным мандатным уровнем доступа:
- создать каталоги «ДСП» и «С» внутри каталогов *otdel1* и *otdel2* командой: `mkdir -p /home/share/otdel{1,2}/{ДСП,С}`;
  - на каталог «ДСП» внутри каталога *otdel1* назначить следующие метки *1:0:1:0*;
  - на каталог «С» внутри каталога *otdel1* назначить следующие метки *2:0:1:0*;
  - аналогично создать каталоги в */home/share/otdel2*;
  - вывести мандатные метки и дискреционные атрибуты каталога *share* рекурсивно, после чего определить назначение используемых опций команды *pdp-ls*.

```
user@astra:~$ sudo pdp-ls /home/share/ -MnR
/home/share/:
утого 16
drwxrwxr-x+m--  4 0 0 2:0:0x1:0x3 otdel1
drwxrwxr-x+m--  4 0 0 2:0:0x2:0x3 otdel2

/home/share/otdel1:
утого 16
drwxrwxr-x+m--  2 0 0 1:0:0x1:0x0 ДСП
drwxrwxr-x+m--  2 0 0 2:0:0x1:0x0 С

/home/share/otdel1/ДСП:
утого 0

/home/share/otdel1/С:
утого 0

/home/share/otdel2:
утого 16
drwxrwxr-x+m--  2 0 0 1:0:0x2:0x0 ДСП
drwxrwxr-x+m--  2 0 0 2:0:0x2:0x0 С

/home/share/otdel2/ДСП:
утого 0

/home/share/otdel2/С:
утого 0
```

1. Изучить возможность задания дискреционных атрибутов вложенных каталогов */home/share* с использованием следующих команд:

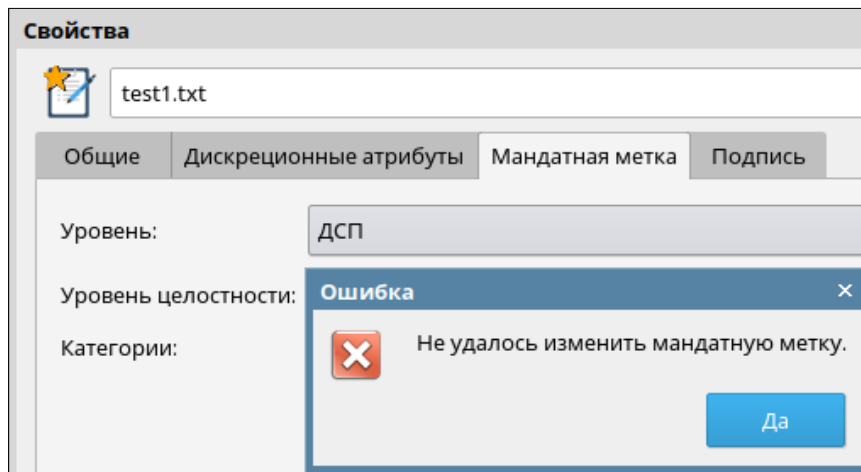
```
root@astra:~# setfacl -b /home/share/otdel{1,2}
root@astra:~# setfacl -b /home/share/otdel{1,2}/{ДСП,С}
```

- сначала очистить все созданные дискреционные атрибуты;
- выполнить команду их создания:

```
root@astra:~# setfacl -m g:office:rwX /home/share/otdel{1,2}/{ДСП,С}
root@astra:~# setfacl -m g:office:rwX /home/share/otdel{1,2}
```

1. Модифицировать уровни доступа и неиерархические категории, заданные в ОССН, путём переименования неиерархических категорий в «Отдел1» и «Отдел2», уровней 0-2 в «НС», «ДСП», «С».
2. Выполнить вход в ОССН в графическом режиме с учётной записью пользователя *manager1* (уровень доступа — «ДСП», неиерархические категории — «Отдел1», уровень целостности — «Низкий»):
  - в графической утилите *fly-fm* выполнить попытки осуществления доступа и создания файлов (*dsp-man1.txt* и *dsp-doc.odt*) в подкаталогах каталога */home/share*;
  - выполнить изменение файла *dsp-man1.txt*;
  - осуществить изменение файла *dsp-doc.odt*.
1. Выполнить вход в ОССН в графическом режиме с учётной записью пользователя *manager1* (уровень доступа — «С», неиерархические категории — «Отдел1», уровень целостности — «Низкий»):
  - в файловом менеджере *fly-fm* выполнить попытки осуществления доступа и создания файлов в подкаталогах каталога */home/share*;
  - произвести изменения файла *c-man1.txt*;
  - выполнить попытку изменения файла *dsp-man1.txt*.
1. Выявить особенность функционирования администратора ОССН, в том числе, на «Высоком» уровне целостности:
  - выполнить вход в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Низкий»);
  - осуществить доступ к каталогу */home/share* и его подкаталогам, определить возможность доступа на чтение администратора ОССН на «Низком» мандатном уровне целостности к сущностям с более высоким уровнем конфиденциальности;
  - осуществить аналогичные действия при работе через *sudo* и сравнить результат;
  - выполнить выход и вход в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);

- выполнить доступ к каталогу */home/share* и его подкаталогам, определить возможность доступа на чтение при работе от имени учётной записи пользователя *user* на «Высоком» мандатном уровне целостности к сущностям с более высоким уровнем конфиденциальности;
  - осуществить аналогичные действия при работе через *sudo*.
1. Создать учётные записи пользователей — руководителей отделов, которые могут менять мандатные метки созданных файлов:
    - создать учётную запись пользователя *seo1* и задать ей минимальный уровень доступа «НС», максимальный уровень доступа «С», минимальная и максимальная неиерархическая категория «Отдел1»;
    - установить необходимые привилегии (*cap\_chown*, *parsec\_cap\_chmac*) с использованием команды *usercaps seo1 -l 1 -m 8*;
    - аналогично создать учётную запись пользователя *seo2* и задать ей минимальный уровень доступа «НС», максимальный уровень доступа «С», минимальная и максимальная неиерархическая категория «Отдел2» и аналогичные привилегии.
  1. Установить для учётных записей пользователей *seo1* и *seo2*:
    - группу по умолчанию *office*: *usermod -g office seo1 && usermod -g office seo2*;
    - установить дополнительные группы для доступа к *fly-term* для учётных записей пользователей *seo1*, *seo2*: *astra-console* (для этого выполнить команду *usermod* с параметрами *-a -G*, группой и именем учётной записи пользователя);
    - найти в графической утилите «Политика безопасности» параметр, позволяющий отключить доступ к терминалу *Fly* для пользователей, и активировать данный параметр.
  1. Выполнить попытку изменения мандатных меток конфиденциальности файлов:
    - выполнить вход в ОССН в графическом режиме с учётной записью пользователя *seo1* (уровень доступа — «С», неиерархические категории — «Отдел1», уровень целостности — «Низкий»);
    - создать в каталоге */home/share/otdel1/C* файл *test1.txt*;
    - с использованием меню графического файлового менеджера *fly-fm* вывести дискреционные и мандатные атрибуты файла *test1.txt*.
    - выполнить попытку установки мандатных атрибутов файла *test1.txt*, при этом необходимо сменить уровень с «С» на «ДСП» (ошибка связана с уровнем конфиденциальности файла *test1.txt*);



- выполнить попытку копирования файла *test1.txt* в каталог */home/share/otdel1/ДСП* (ошибка заключается в том, что уровень доступа текущего процесса, осуществляющего копирование, выше уровня конфиденциальности каталога назначения, т. е. блокируется запись сверху вниз);
  - копировать файл *test1.txt* в каталог */home/share/otdel1* («С», CCNRA);
  - сменить мандатные атрибуты файла *test1.txt*, при этом необходимо сменить уровень с «С» на «ДСП».
1. Выполнить вход в ОССН в графическом режиме с учётной записью пользователя *seo1* (уровень доступа — «ДСП», неиерархические категории — «Отдел1», уровень целостности — «Низкий»)
  2. Скопировать (или перенести) файл *test1.txt* в каталог */home/share/otdel1/ДСП*.
  3. При необходимости удаления файла */home/share/test1.txt*: войти в ОССН с учётной записью пользователя *seo1* («ДСП», «Отдел1»).
  4. Выполнить вход в ОССН в графическом режиме с учётной записью пользователя *manager1* (уровень доступа — «С», неиерархические категории — «Отдел1», уровень целостности — «Низкий»):
    - в файловом менеджере *fly-fm* выполнить попытки доступа к файлам и создания файлов в подкаталогах «ДСП» и «С» каталога */home/share/otdel1*;
    - выполнить попытку открытия файла *dsp-doc.odt*;
    - выявить возможные ошибки работы с файлом.
  1. Возможной причиной того, что файл *dsp-doc.odt* не может быть открыт с уровня «С» является особенность работы *LibreOffice*, который создаёт в текущем каталоге файл *~.lock.Файл.о*. Для подтверждения этого необходимо войти в ОССН с использованием терминала *Fly* с учётными записями пользователей *manager1* и *manager2*:

- выполнить вход в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);
  - добавить пользователям *manager1* и *manager2* группу *astra-console* командой: `usermod -a -G astra-console manager1`, `usermod -a -G astra-console manager2` для возможности запуска терминале *Fly*;
  - выполнить повторный вход в ОССН в графическом режиме с учётной записью пользователя *manager1* (уровень доступа — «С», неиерархические категории — «Отдел1», уровень целостности — «Низкий»);
  - запустить *fly-term* с использованием комбинации клавиш «Astra»+«R».
1. С использованием меню графического файлового менеджера *fly-fm* создать «Документ *LibreOffice*» в каталоге */home/share/otdel1/C*: файл *c-doc.odt*, *1.odt*. Открыть файл *1.odt*, перейти в терминале *Fly* в каталог */home/share/otdel1/C* и вывести содержимое каталога (обратить внимание на наличие файла *~lock.1.o*).

```
manager1@astra:/home/share/otdel1/C$ ls -la
итого 28
drwxrwxr-x+ 2 root      root    4096 июн 21 19:01 .
drwxrwxr-x+ 4 root      root    4096 июн 21 13:50 ..
-rw-r--r--  1 manager1 otdel1  7620 июн 21 19:01 1.odt
-rw-r--r--  1 manager1 otdel1    0 июн 21 18:40 c-man1.txt
-rw-r--r--  1 manager1 otdel1   77 июн 21 19:01 ~lock.1.o
```

2. В *LibreOffice* открыть меню «Сервис», «Параметры», «*LibreOffice*», «Расширенные возможности», «Открыть экспертные настройки». Ввести фильтр: *uselocking*.
3. Изменить значение на *false* и сохранить изменения.
4. Ввести фильтр «*lock*» и изменить значения свойств «*UseDocumentOOoLockFile*» и «*UseDocumentSystemFileLocking*» на *false*.
5. Выполнить повторное открытие файла *c-doc.odt* и проверить отсутствие «*lock*»-файла.
6. Выполнить вход в ОССН в графическом режиме с учётной записью пользователя *manager1/manager2* (уровень доступа — «С»/«ДСП», неиерархические категории — «Отдел1»/«Отдел2», уровень целостности — «Низкий») в доступных комбинациях:
  - в соответствующем режиме проверить возможность доступа на чтение и запись к документам, созданным *LibreOffice*, с уровнем конфиденциальности, соответствующем уровню доступа учётной записи пользователя;
  - проверить необходимые настройки блокировки открываемого документа в настройках *LibreOffice* на текущем уровне;



- проверить возможность осуществления доступа на чтение (и главное проверить возможность открытия) к документам, созданным *LibreOffice*, с уровнем конфиденциальности меньше текущего уровня доступа учётной записи пользователя;
- в конце лабораторной работы вернуть ОССН к начальным настройкам.

## **Содержание отчёта по выполненной работе**

В отчёте о выполненной работе необходимо указать:

1. Полный перечень использованных команд с кратким описанием их назначения.
2. Примеры выполнения команд, которые были использованы в ходе работы с описанием их результатов.
3. Описание порядка работы с графической утилитой при выполнении следующих действий:
  - создание, изменение и удаление уровней доступа и неиерархических категорий;
  - создание и настройка групп пользователей.
1. Описание порядка работы и команд, использованных при осуществлении следующих действий:
  - настройка уровней доступа и неиерархических категорий учётных записей пользователей;
  - модификация параметров доступа к сущностям файловой системы ОССН;
  - настройка уровней доступа и неиерархических категорий в ОССН.
1. Описание особенностей настройки *LibreOffice* для работы с документами в рамках мандатного управления доступом.
2. Параметры мандатного управления доступом (метки) для каталогов, предназначенные для совместной работы от имени учётных записей пользователей с различным уровнем доступа.

## **Контрольные вопросы**

1. Какая утилита используется для модификации учётных записей пользователей?
2. С какими мандатными атрибутами должен войти администратор ОССН для настройки параметров мандатных управления доступом и контроля целостности учётных записей пользователей?
3. Какими атрибутами должны обладать каталоги для работы пользователей с различным уровнем доступа?
4. Как создать учётные записи пользователей, которые имеют возможность смены мандатных меток конфиденциальности файлов, а также владельцев файлов?

5. Как осуществляется доступ к расширенным настройкам *LibreOffice* для реализации совместного доступа к файлам в рамках мандатных управления доступом и контроля целостности?

# ЛАБОРАТОРНАЯ РАБОТА №5.

## АДМИНИСТРИРОВАНИЕ ОССН В РАМКАХ РЕАЛИЗАЦИИ МАНДАТНОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ.

**Цель работы:** Выявить особенности администрирования основных параметров мандатного управления доступом в ОССН с применением графических утилит и консольных команд при активированном мандатном контроле целостности.

**Время выполнения работы:** 2 академических часа.

### Краткие 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 и контроля целостности (мандатными метками) 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*).

Мандатное управление доступом процессов (субъект-сессий) к ресурсам (сущностям) основано на реализации соответствующего механизма в ядре ОССН. При этом, решение о запрете или разрешении доступа субъект-сессии к сущности принимается 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).

Реализация мандатного контроля целостности позволила существенно повысить защищенность ОССН. С его применением все учётные записи пользователей, субъект-сессии, сущности и роли (при установке ОССН для элементов её файловой системы задаётся два

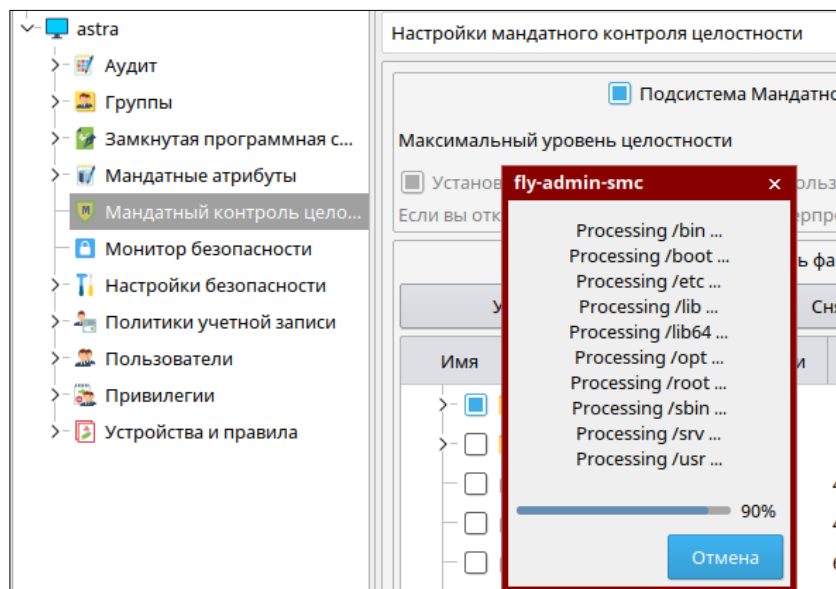
мандатных уровня целостности — 0 и 63, хотя их может быть значительно больше, в том числе, может использоваться вся решётка уровней целостности 0 до 255) чётко разделяются на два множества (отсюда и два уровня целостности: «Низкий» < «Высокий»), влияющих на целостность и безопасность ОССН или нет. Преимущества мандатного контроля целостности аналогичны преимуществам мандатного управления доступом в сравнении с дискреционным управлением доступом, т.е. обеспечивается большая ясность правил разделения компонентов системы на критичные и некритичные с точки зрения её целостности, тем самым снижается вероятность ошибок.

## **Используемое методическое и лабораторное обеспечение**

1. ОССН версии 1.6, в которой создана учётная запись пользователя *user*, 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*).
2. Документация: «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство администратора. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство по КСЗ. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство пользователя».

## **Порядок выполнения работы**

1. Включить мандатный контроль целостности в файловой системе ОССН. Для этого выполнить вход в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»). Запустить графическую утилиту «Политика безопасности» через меню «Панель управления», «Безопасность» главного пользовательского меню. Открыть «Мандатный контроль целостности» и нажать кнопку «Установить». На данном этапе для сущностей файловой системы в соответствии с шаблоном устанавливаются метки мандатного уровня целостности «Высокий». Выполнить выход из ОССН.



2. Проанализировать необходимость использования входа в систему с уровнем целостности «Высокий» для администрирования ОСЧН. Для этого, вначале, выполнить работы по администрированию, используя только уровень целостности «Низкий»:
  - начать работу со входа в ОСЧН в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Низкий»);
  - запустить графическую утилиту «Политика безопасности» через меню «Панель управления», «Безопасность» главного пользовательского меню.
1. Выполнить попытку модификации параметров мандатного управления доступом, для этого осуществить следующие действия:
  - открыть раздел «Мандатные атрибуты», «Уровни конфиденциальности» и выбрать «0: Уровень\_0» и сделать попытку переименования данного уровня доступа;
  - осуществить попытку создания мандатного уровня доступа;
  - проанализировать результат и причину невозможности выполнения данной операции.
1. Запустить терминал *Fly* и выполнить команду *pdp-id -a* для получения мандатных атрибутов текущего процесса (в данном случае они совпадают с мандатными атрибутами текущей сессии), 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*;
  - определить назначение параметров команд;

- выполнить попытку запуска команды модификации мандатных уровней: *userlev* (например, с параметрами Уровень\_4 -а 4) и проанализировать полученную ошибку.
1. Запустить терминал *Fly* с использованием команды *sudo* (использовать комбинацию клавиш на клавиатуре «Win»+«R», далее будем её называть «Astra»+«R») и выполнить следующие команды:
    - выполнить команду просмотра мандатных уровней: *userlev*;
    - определить параметры запуска команды *userlev* для создания нового мандатного уровня конфиденциальности «Уровень\_4» со значением 4 и проанализировать полученную ошибку;
    - определить текущие мандатные уровни доступа и целостности с использованием команды *pdp-id*, а также определить группы с использованием команды *id*.

```
root@astra:/home/user# pdp-id
Уровень конф.=0(Уровень_0), Уровень целостности:0(Низкий), Категории=0x0(Нет)
Ролл=: (Нет:Нет)
root@astra:/home/user# id
uid=0(root) gid=0(root) группы=0(root)
root@astra:/home/user# █
```

1. Исходя из особенностей работы от имени учётной записи пользователя администратора (*user*) в обычном режиме (без использования *sudo*) и с использованием *sudo*, можно сделать вывод, что для администрирования ОССН необходимо получение некоторых «дополнительных прав» (т.е. наличие группы с идентификатором 0 недостаточно), которые связаны с реализацией мандатного контроля целостности в ОССН. Для изучения особенностей маркировки файлов ОССН метками с высокой целостностью выполнить в запущенном терминале *Fly* следующие команды:
  - вывести в терминал *Fly* дискреционные права доступа и параметры мандатного управления доступом файлов и каталогов корня файловой системы командой *pdp-ls -M /*;
  - определить опцию команды *pdp-ls*, позволяющую осуществлять вывод меток мандатного контроля целостности в числовом формате;
  - с использованием найденной опции определить максимальное значение мандатного уровня целостности, заданное для каталога */*;

```
root@astra:/# pdp-ls -Mn / | cut -d : -f 2 | sort | grep -v "утого" | tail -1
63
```

- изучить с использованием команды *man* и справки назначение команд (*pdp-ls*, *cut*, *sort*, *grep*, *tail*) и использованных опций;
- выполнить команду получения списка имён файлов и каталогов с уровнем целостности «Высокий» для каталога / и /etc с использованием конвейера и команды *grep*;
- определить уровень целостности файла */etc/passwd*;
- выполнить попытки модификации файла */etc/passwd* путём добавления в него новых записей с использованием текстовых редакторов.

1. Выполнить выход и вход в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).

2. Запустить графическую утилиту «Политика безопасности» через меню «Панель управления», «Безопасность» главного пользовательского меню.

3. Выполнить модификацию параметров мандатного управления доступом. Для этого выполнить следующие действия:

- открыть раздел «Мандатные атрибуты», «Уровни конфиденциальности» и выбрать: «3:Уровень\_3» и переименовать данный уровень доступа: «Уровень\_Макс»;
- создать уровень доступа с именем «Уровень\_4», установив значение равное 4;
- проанализировать результат и причину отсутствия ошибок.

1. Выполнить модификацию параметров учётной записи пользователя *user*:

- открыть раздел «Пользователи», «*user*» и выбрать вкладку «МРД»;
- выполнить попытку изменения минимального уровня доступа учётной записи пользователя *user*;
- выполнить изменение максимального уровня доступа учётной записи пользователя *user*: «Уровень\_2», категории «Категория\_1»;
- выйти из графической утилиты «Политика безопасности».

1. Запустить терминал *Fly* и выполнить следующие команды для определения особенностей работы в консольном режиме на различных мандатных уровнях целостности:

- выполнить команду получения мандатных атрибутов текущей сессии (с использованием команды *pdp-idl*), и вывести только текущий уровень целостности;

•

```
user@astra:~$ pdp-idl awk '{print $3,$4}'
Уровень целостности:63(63),
```

- выполнить аналогичную команду, но с использованием команды *ps*;

```
user@astra:~$ sudo pdpl-ps $(ps auxl grep fly-term | grep -v "grep" |
awk '{print $2}') | cut -d : -f 2
Высокий
```

- изучить с использованием *man* и справки назначение применённых команд (*awk*, *pdpl-ps*, *ps*).
1. Для определения достаточности уровня целостности «Высокий» при администрировании ОССН выполнить следующие команды:
    - вывести содержимое файла */etc/passwd* и выполнить попытку его модификации: изменить *Shell* «по-умолчанию» для произвольной учётной записи пользователя;
    - выполнить попытку выдачи на экран содержимого файла */etc/shadow*.
  1. Изучить особенности работы приложений с уровнем целостности «Высокий» для пользователя администратора ОССН без и с использованием команды *sudo*:
    - запустить терминал *Fly* с использованием команды *sudo*;
    - сравнить результаты вывода команды *pdpl-ls* для каталога */etc* для режима *sudo* и без него (использовать опцию отображения мандатных меток);
    - вывести содержимое файла */etc/passwd* и выполнить модификацию: изменить *Shell* «по-умолчанию» для учётной записи пользователя «user».
  1. Проверить результаты проведённой переконфигурации ОССН:
    - выполнить вход в ОССН от имени учётной записи пользователя *user* на уровне доступа 2 в графическом и консольном режимах;
    - после выполнения соответствующего входа вывести текущие мандатные уровни доступа и целостности с использованием команды *pdpl-id*.
  1. Определить порядок хранения параметров мандатного управления доступом и мандатного контроля целостности в ОССН. Для этого проанализировать содержимое каталога */etc/parsec*:
    - с использованием контекстного поиска выделить файлы, содержащие наименования и значения мандатных уровней целостности и доступа в ОССН (например, файлы содержащие «Высокий»);
    - создать произвольную учётную запись пользователя, установить минимальный уровень доступа 1, максимальный — 2, максимальные категории «Категория\_1» и «Категория\_2»;
    - определить файлы, содержащие параметры мандатного управления доступом учётных записей пользователей (для этого выполнить поиск файлов в каталоге */etc* с именем равным идентификатору пользователя);



- самостоятельно выполнить смену максимального мандатного уровня доступа созданной учётной записи пользователя на «Уровень\_4» с использованием редактирования содержимого найденного файла;
- проверить результат изменения с использованием графической утилиты «Политика безопасности»;
- проверить возможность входа в ОССН в графическом режиме с созданной учётной записью пользователя (уровень доступа — 4, неиерархические категории — нет, уровень целостности — «Низкий»);
- определить файл, используемый для хранения параметров максимального мандатного уровня целостности созданной учётной записи пользователя;
- в конце лабораторной работы вернуть ОССН к начальным настройкам (выполнить удаление созданных мандатных уровней доступа и т.п.).

### **Содержание отчёта по выполненной работе**

В отчёте о выполненной работе необходимо указать:

1. Полный перечень использованных команд с кратким описанием их назначения.
2. Примеры выполнения команд, которые были использованы в ходе работы с описанием результатов их выполнения.
3. 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.
1. Описание порядка работы и команд, использованных при осуществлении следующих действий:
  - настройка уровней доступа и неиерархических категорий учётных записей пользователей;
  - настройка уровней доступа и неиерархических категорий в ОССН.
1. Описание особенностей функционирования команд при работе на «Высоком» и «Низком» уровнях целостности.
2. Список и назначение системных файлов, связанных с хранением параметров мандатного управления доступом и мандатного контроля целостности ОССН и пользователей.

### **Контрольные вопросы**



1. Как из *fly-term* запустить графическую утилиту «Политика безопасности»?
2. Как с использованием графического интерфейса создать мандатный уровень доступа ОССН?
3. Как определить текущие мандатные уровни доступа и целостности сессии пользователя?
4. В чем заключаются отличия работы приложений с различным мандатным уровнем целостности для пользователя администратора ОССН без и с использованием команды *sudo*?
5. Как выполнить смену максимального уровня доступа заданной учётной записи пользователя с использованием консольных команд?
6. Как определить параметры мандатного управления доступом учётных записей пользователей?
7. Какие файлы используются для хранения параметров мандатного управления доступом учётных записей пользователей?

# ЛАБОРАТОРНАЯ РАБОТА №6.

## НАСТРОЙКА МЕХАНИЗМОВ

## ОРГАНИЗАЦИИ ЗАМКНУТОЙ

## ПРОГРАММНОЙ СРЕДЫ.

## КОНТРОЛЬ ЦЕЛОСТНОСТИ КСЗ.

**Цель работы:** Изучить принципы и технологии контроля целостности данных (в том числе, комплекса средств защиты — КСЗ), реализованных в ОССН. Освоить умения, необходимые для решения задач подсчёта контрольных сумм файлов и оптических носителей, контроля соответствия дистрибутиву, регламентного контроля целостности и создания замкнутой программной среды.

**Время выполнения работы:** 2 академических часа.

### Краткие теоретические сведения

АСЗИ на базе ОССН должны обеспечивать функции, как аудита доступа к сущностям файловой системы, так и контроля целостности (*integrity*) данных и содержимого исполняемых файлов. Подобный контроль позволяет с достаточной уверенностью констатировать факт отсутствия в данных, обрабатываемых системными процессами ОССН, недекларируемых для АСЗИ возможностей.

Для решения задачи контроля целостности в состав КСЗ ОССН включены средства, реализующие частные функции управления целостностью данных:

- вычисления и проверки контрольных сумм файлов и оптических дисков;
- контроля соответствия дистрибутиву;
- регламентного контроля целостности;
- создания замкнутой программной среды.

Базовым методом контроля целостности сущностей файловой системы ОССН является контроль их модификации путём вычисления контрольных сумм.

Контрольная сумма — значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их

передаче или хранении. Она используется для быстрого сравнения двух наборов данных на эквивалентность: с очень большой вероятностью отличающиеся наборы данных будут иметь разные контрольные суммы.

Алгоритмы вычисления контрольной суммы, как правило, делятся на два вида:

- *Алгоритмы общего назначения.* К таким алгоритмам, в первую очередь, относится циклический избыточный код (*Cyclic Redundancy Check, CRC*), реализацией которого являются алгоритмы *CRC8*, *CRC16*, *CRC32*, применяющиеся для проверки целостности цифровых данных при их передаче по каналам связи;
- *Криптографические алгоритмы.* Эти алгоритмы основаны на процедуре хэширования – преобразования входного массива данных произвольной длины в выходную битовую строку фиксированной длины. К таким алгоритмам относятся, например, семейства алгоритмов *MD* (*Message Digest Algorithm – MD2-MD6*), *SHA* (*Secure Hash Algorithm – SHA-1, SHA-2*), ГОСТ Р 34.11 (ГОСТ Р 34.11-94, снятый с эксплуатации с 1 января 2013 г., ГОСТ Р 34.11-2012 «Стрибог») и другие. Областью применения этих алгоритмов является подтверждение целостности и подлинности передаваемых и хранимых данных.

В составе КСЗ ОССН включены следующие средства контроля целостности:

1. Команды, реализующие криптографические алгоритмы:
  - *md5sum* (реализация алгоритма *MD5*);
  - *shasum* (реализация семейства алгоритмов *SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256* и *SHA-512/224*).
1. Средства проверки соответствия файловых сущностей ОССН её дистрибутиву:
  - команда *gostsum* (реализация алгоритма ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 256 и 512 бит);
  - графическая утилита *fly-admin-int-check*.

Указанные команды и утилиты реализуют статический контроль целостности файловых сущностей ОССН, включающий следующие компоненты:

1. Система мониторинга целостности файлов (*FIM – File integrity monitoring*) *AFICK* (*Another File Integrity CheckKer*), реализующая регламентный (периодический) контроль целостности файловых сущностей ОССН – вариант динамического контроля целостности.
2. Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата *ELF* при запуске приложений на выполнение. Он реализован в выгружаемом модуле ядра ОССН *digsig\_verif* и обеспечивает:
  - контроль целостности исполняемых файлов и разделяемых библиотек на основе их контрольных сумм, вычисляемых в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 и электронной подписи, реализованной в соответствии с ГОСТ Р 34.10-2001 и

ГОСТ Р 34.10-2012. Контрольная сумма и электронная подпись внедрены в файлы формата *ELF* в процессе сборки ОССН;

- внедрение электронной подписи в исполняемые файлы формата *ELF*, входящие в состав устанавливаемого ПО.

Команды и утилиты статического контроля целостности функционируют в режимах вычисления (*compute*) и проверки (*check*) контрольных сумм файловых сущностей ОССН.

Например, команда *shasum* в режиме вычисления контрольной суммы файловой сущности с именем */root/file* с использованием алгоритма *SHA-256* имеет следующий синтаксис:

```
shasum -a 256 /root/file
```

В режиме проверки контрольных сумм файловых сущностей команды статического контроля целостности вычисляют их для сущностей, полный путь которых указан в текстовом файле с эталонными контрольными суммами, и сравнивают их с эталонными контрольными суммами из этого файла. Результатом их выполнения в режиме проверки контрольных сумм является передача на стандартный вывод строки формата (в случае совпадения контрольных сумм):

```
полный_путь_к_файловой_сущности: OK
```

или (в случае их несовпадения):

```
полный_путь_к_файловой_сущности: FAILED
```

Например, команда *shasum* в режиме проверки контрольных сумм файловых сущностей в каталоге */root/dir1*, с использованием алгоритма *SHA-256* и при наличии текстового файла с эталонными контрольными суммами */root/dir1.sha*, имеет следующий синтаксис:

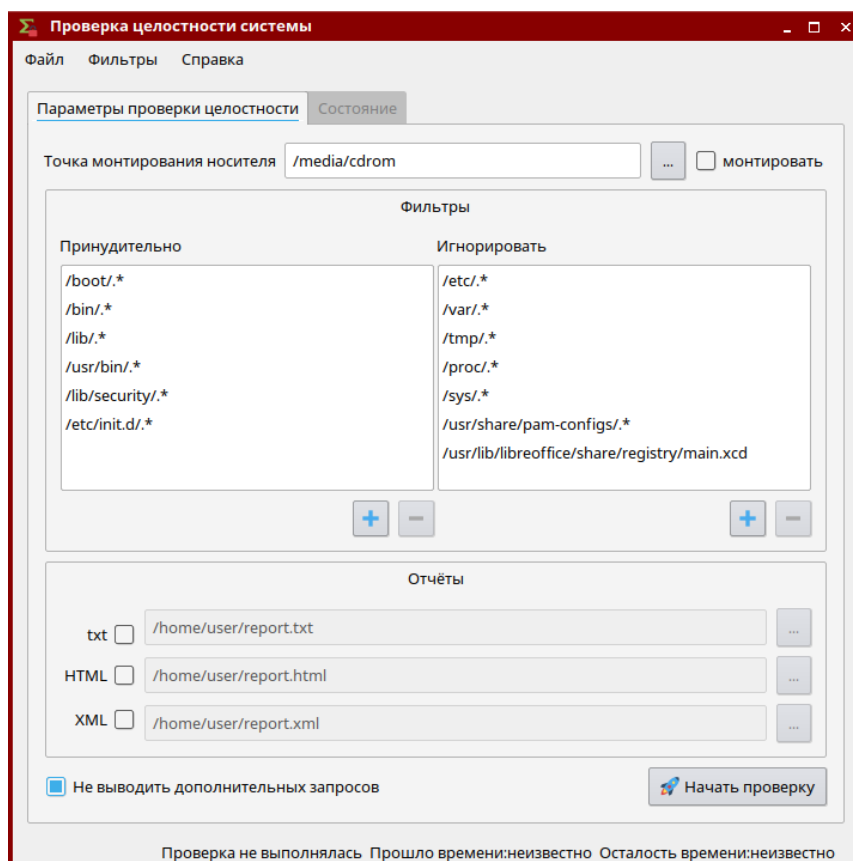
```
shasum -a 256 -c /root/dir1.sha
```

Для вычисления контрольных сумм файловых сущностей ОССН с использованием криптографического алгоритма ГОСТ Р 34.11-2012 256 бит применяется команда *gostsum*, имеющая следующий синтаксис:

```
gostsum полный_путь_к_файловой_сущности -o
```

```
полный_путь_к_файловой_сущности_с_контрольными_суммами
```

Для проверки соответствия модулей установленной ОССН модулям, входящим в состав её дистрибутива, используется графическая утилита *fly-admin-int-check*, имеющая следующий интерфейс:



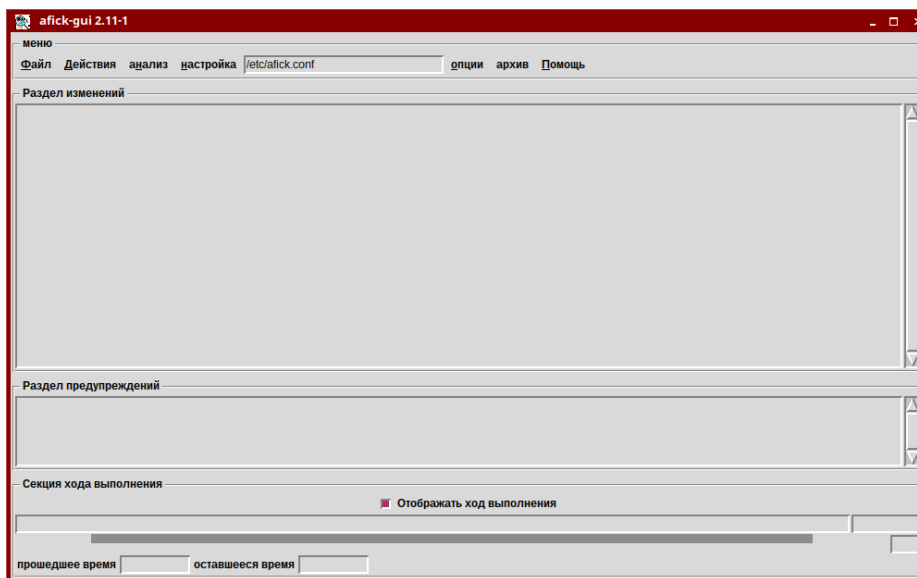
Для выполнения этой проверки в состав дистрибутива ОССН входит файл *gostsums.txt*, созданный командой *gostsum* и содержащий список контрольных сумм всех файлов, входящих в пакеты программ дистрибутива. Получаемый в результате проверки отчёт сохраняется в форматах *\*.txt*, *\*.htm* и *\*.xml*.

Проверка соответствия модулей установленной ОССН модулям, входящим в состав её дистрибутива, является вариантом статического контроля целостности и обеспечивает контроль целостности файловых сущностей, копируемых в корневой раздел ОССН на этапе установки, что позволяет убедиться в отсутствии изменений в файловых сущностях модулей, произошедших на этапе их эксплуатации.

Однако такая проверка является неэффективной для файловых сущностей, содержимое которых многократно изменяется в ходе эксплуатации ОССН, например, конфигурационных файлов. Кроме того, контроль целостности на основе только контрольной суммы файла не затрагивает проверку таких атрибутов файла, как временные метки (*timestamps*), дискреционные атрибуты (*Minimal ACL* и *EA ACL*), мандатные метки безопасности. Для выполнения расширенного контроля целостности файлов, обеспечивающего проверку перечисленных атрибутов файлов, в ОССН используется система мониторинга целостности файлов *AFICK*, реализующая функции контроля целостности файлов и их атрибутов с использованием криптографических алгоритмов *MD5* и *SHA-1*. В ОССН применяется модифицированный вариант системы *AFICK*, дополнительно реализующий криптографический алгоритм ГОСТ Р 34.11 (для приложения *gostsum* дополнительно поддерживаются алгоритмы ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 с длиной ключа 256 или 512 бит), а также контроль мандатных меток и атрибутов подсистемы аудита безопасности. Дополнительно система *AFICK* имеет возможность настройки правил проверки целостности каталогов.

Благодаря интеграции системы *AFICK* с сервисом запуска приложений по расписанию *cron* имеется возможность выполнения регламентного (периодического) контроля целостности заданных файловых сущностей ОССН.

Система *AFICK* имеет следующий интерфейс (для её запуска можно использовать команду *afick-tk*):



Конфигурационным файлом системы *AFICK* является */etc/afick.conf* – текстовый файл, структурированный по секциям.

Секция *alias* содержит перечень действий (*action*) контроля целостности, из которых формируются правила контроля каталогов и файловых сущностей.

```
#####
# alias section
#####
# action : a list of item to check :
# md5 : md5 checksum
# sha1 : sha1 checksum
# d : device
# i : inode
# p : permissions
# n : number of links
# u : user
# g : group
# s : size
# b : number of blocks
# m : mtime
# c : ctime
# a : atime
# e: parsec mac
# t: parsec aud
# gost: gost
```

Типовыми действиями является проверка:

- контрольных сумм, полученных заданным криптографическим алгоритмом (*md5*, *sha1*);
- *inode* (*i*) каталога или файловой сущности, её размера (*size*) и временных меток (*mtime*, *ctime*, *atime*);
- *UID* и *GID* (*user*, *group*) каталога или файловой сущности, а также прав доступа к ней (*permissions*).

Применительно к организации подсистемы безопасности ОССН дополнительно определены три действия:

- *e: parsec mac* – контроль целостности мандатных меток безопасности файловых сущностей;
- *t: parsec aud* – контроль целостности данных системы аудита безопасности ОССН;
- *gost: gost* – контроль целостности файловых сущностей с использованием криптографического алгоритма ГОСТ Р 34.11.

В результате этих действий в секции *alias* формируются типовые правила для каталогов (*DIR*), файлов конфигурации ОССН (*ETC*) и файлов журналов системы аудита (*Logs*).

Например, правило для каталогов вида:

*DIR = p+i+n+u+g*

указывает на необходимость выполнения проверки прав доступа, метаданных, количества ссылок и других стандартных атрибутов.

Дополнительно секция *action* включает правила, специфичные для подсистемы безопасности *PARSEC* – *PARSEConly*, *PARCEC* и *GOST*. Например, правило *PARSEC* вида:

*PARSEC = p+d+i+n+u+g+s+b+md5+m+e+t*



указывает на необходимость выполнения проверки стандартных атрибутов файловых сущностей с использованием криптографического алгоритма *MD5*, проверки расширенных атрибутов (меток безопасности и флагов аудита) и списков *ACL* этих файловых сущностей.

В правиле *GOST* вида:

$$GOST = p+d+i+n+u+g+s+b+gost+m+e+t$$

параметр *gost* указывает на необходимость выполнения проверки стандартных атрибутов файловых сущностей с использованием криптографического алгоритма ГОСТ Р 34.11.

В секции *files to scan* задаются полные пути и правила, применяемые к каталогам и файловым сущностям, для которых выполняется регламентный контроль целостности. Формат записей секции *files to scan* следующий:

*file action* – проверяются каталоги, подкаталоги и файловые сущности с параметром «действия»;

*!file* – из проверки каталогов и подкаталогов исключается файловая сущность *file*;

*=directory action* – с параметром «действия» проверяется только каталог, и из проверки исключаются подкаталоги.

Например:

*/boot GOST* – проверка в каталоге */boot* всех подкаталогов и файловых сущностей с помощью правила *GOST*;

*=/ DIR* – проверка с помощью правила *DIR* только корневого каталога, исключая подкаталоги;

*!/root/.bash\_history* – исключение проверки в каталоге */root* файловой сущности *.bash\_history*.

Эталонные значения контрольных сумм и атрибутов файловых сущностей и каталогов хранятся в базе данных системы *AFICK* в файле с расширением *ndbm*. Эта база данных создаётся в соответствии с параметрами секции «*files to scan*» файла */etc/afick.conf*.

Результаты контроля целостности оформляются в виде *log*-файлов и сохраняются:

- в случае принудительного (инициированного администратором) контроля – в каталоге */var/lib/afick/archive* в *log*-файлах с форматом имени *afick.YYYYMMDDHHMMSS*. В аналогичных *log*-файлах сохраняются результаты обновления (*update*) базы данных системы *AFICK*;
- в случае регламентного (периодического, инициированного сервисом *cron*) контроля – в каталоге */var/log/afick* в *log*-файлах с форматом имени *afick.log.N* (где *N* принимает значения от 1 до 7).

Средство создания замкнутой программной среды в ОССН – невыгружаемый модуль ядра ОССН *digsig\_verif* функционирует в трёх режимах (аналогично применяются режимы проверки подписи в расширенных атрибутах, т. е. не только для *ELF*-файлов, с использованием параметра *DIGSIG\_XATTR\_MODE*):

- *Штатный режим* – исполняемым файловым сущностям формата *ELF* и разделяемым библиотекам, не имеющим ЭП или имеющим некорректную ЭП, исполнение запрещается (*DIGSIG\_ELF\_MODE* = 1);
- *Режим проверки ЭП в комплексе средств системного ПО* – исполняемым файловым сущностям формата *ELF* и разделяемым библиотекам, не имеющим ЭП или имеющим некорректную ЭП, исполнение разрешается, но при этом выводится сообщение об ошибке проверки ЭП (*DIGSIG\_ELF\_MODE* = 2);
- *Отладочный режим для тестирования комплекса средств системного ПО* (установлен по умолчанию) – ЭП исполняемых файловых сущностей формата *ELF* и разделяемых библиотек не проверяется (*DIGSIG\_ELF\_MODE* = 0).

Для выбора одного из указанных выше режимов функционирования модуля *digsig\_verif* необходимо отредактировать конфигурационный файл */etc/digsig/digsig\_initramfs.conf*.

Управление модулем *digsig\_verif* осуществляется через графический интерфейс *fly-admin-smc* либо через интерфейс файловой системы *sysfs* с использованием следующих файлов:

- */sys/digsig/enforce* – в данном файле задаются указанные выше режимы работы;
- */sys/digsig/key* – файл загрузки мастер-ключа ЭП;
- */sys/digsig/additional* – файл загрузки дополнительных ключей ЭП.

Каждый дополнительный ключ для подписи системного ПО должен быть помещён в каталог */etc/digsig/keys*.

Создание дополнительных ключей выполняется с помощью команды *gpg* (*GNU Privacy Guard*), модифицированной для использования криптографических алгоритмов ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012.

При администрировании средств контроля целостности данных и средств контроля соответствия дистрибутиву, а также при работе со средствами создания замкнутой программной среды используются следующие команды:

- *afick* — команда управления параметрами системы контроля целостности файловых сущностей;
- *bsign* — команда создания и проверки ЭП в файлах формата *ELF*;
- *digsig\_initramfs* — команда загрузки ключей ЭП и инициализация режима *Enforce* модуля *digsig\_verif*;
- *fly-admin-int-check* — графическая утилита администрирования контроля целостности файловых сущностей;
- *gpg* — команда работы с сертификатами пользователей;
- *lsmod* — команда получения списка загруженных модулей ядра;
- *modinfo* — команда получения информации о заданном модуле ядра;

- *md5sum*, *gostsum*, *shasum* — команда вычисления контрольных сумм;
- *update-initramfs* — команда инициализации начального загрузочного образа ОССН (*initrd*).

## Используемое методическое и лабораторное обеспечение

1. ОССН версии 1.6, в которой создана ученная запись пользователя *user*, 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*).
2. Дистрибутив ОССН.
3. Документация: «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».
4. Для выполнения этапа работы необходимо наличие дополнительных ключей ЭП (ключи должны быть получены у разработчика и подписаны мастер-ключом «JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018)»).

## Порядок выполнения работы

1. Начать работу со входа в ОССН в графическом режиме 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*.
2. В домашнем каталоге создать подкаталог *checksum* и скопировать в него все файлы (включая вложенные каталоги) из каталога */etc*.
3. Используя алгоритм MD5, вычислить контрольные суммы всех файлов в каталоге */home/user/checksum* и перенаправить результат их вычисления в файл */home/user/md5check*, а поток с перечнем ошибок в файл */home/user/error.md5*, командой *md5sum /home/user/checksum/\* > /home/user/md5check 2>/home/user/error.md5*.

```

root@astra:/home/user# cat md5check
470c4dc7cb89f4f59f3d40af24438f4c /home/user/checksum/adduser.conf
d41d8cd98f00b204e9800998ecf8427e /home/user/checksum/adjtime
6daf827d6d70c8e2be08b81338b8586b /home/user/checksum/afick.conf
61e28705bd00f4410e182eeeb5469be1 /home/user/checksum/aliases
00ff43422e8756204113c5546b00d529 /home/user/checksum/anacrontab
21767f2203d324c988256b07f2634708 /home/user/checksum/astra-safepolicy.conf
37d875e620170c9ed2ff3b8884b23b73 /home/user/checksum/astra_version
87b895cef45b8090d628a1d9a0f4bfb8 /home/user/checksum/bash.bashrc
a81b3f1cb197219b815942f4fc7fa94e /home/user/checksum/bash_completion
4c09213317e4e3dd3c71d74404e503c5 /home/user/checksum/bindresvport.blacklist

```

4. Вывести в терминал содержимое файлов `/home/user/md5check` и `/home/user/error.md5` цепочкой команд `cat /home/user/md5check ; cat /home/user/error.md5` и указать, для каких объектов в каталоге `/home/user/checksum` контрольные суммы не были созданы.
5. Используя алгоритм *SHA-512/256*, вычислить контрольные суммы всех файлов в каталоге `/home/user/checksum` и перенаправить результат вычислений в файл `/home/user/sha512256check` командой `shasum -a 512256 /home/user/checksum/* > /home/user/sha512256check`. Вывести на экран содержимое файла `/home/user/sha512256check` командой `less /home/user/sha512256check`.
6. Используя редактор *vim*, изменить содержимое файла `/home/user/checksum/passwd`, удалив из него учётную запись суперпользователя (строку `root:x:0:0:root:/root:/bin/bash`).
7. Используя алгоритм *MD5*, проверить контрольные суммы всех файлов в каталоге `/home/user/checksum` и перенаправить результат проверки в файл `/home/user/fullcheck` командой `md5sum -c ./md5check > /home/user/fullcheck`.
8. Используя алгоритм *SHA-512/256*, проверить контрольные суммы всех файлов в каталоге `/home/user/checksum` и перенаправить результат проверки (с добавлением) в файл `/home/user/fullcheck` командой `shasum -a 512256 -c ./sha512256check >> /home/user/fullcheck`.
9. Найти в файле `/home/user/fullcheck` строки, указывающие на файлы с нарушением целостности (содержащие слова *ПОВРЕЖДЁН* и *FAILED*), вывести в терминал их содержимое и количество цепочкой команд `grep 'ПОВРЕЖДЁН' /home/user/fullcheck > /home/user/tmpcheck ; grep 'FAILED' /home/user/fullcheck >> /home/user/tmpcheck ; wc -l /home/user/tmpcheck ; less /home/user/tmpcheck`.
10. Используя алгоритм ГОСТ Р 34.11-2012 (256 бит), вычислить контрольную сумму файла `/home/user/checksum/shadow`, перенаправить результат проверки в файл `/home/user/gostcheck` и вывести в терминал содержимое файла `/home/user/gostcheck` цепочкой команд `gostsum /home/user/checksum/shadow -o ./gostcheck ; less /home/user/gostcheck`.

11. Установить оптический диск с дистрибутивом ОССН и, используя алгоритм ГОСТ Р 34.11-2012 (256 бит), вычислить его контрольную сумму (по умолчанию файл устройства оптического диска `/dev/sr0`) и перенаправить результат вычисления в файл `/home/user/isocheck` командой `gostsum -d /dev/sr0 > /home/user/isocheck` (выполнение команды занимает длительное время).
12. Запустить графическую утилиту `fly-admin-int-check` и во вкладке «Параметры проверки целостности»:
  - выбрать точку монтирования устройства «Astra smolensk amd64» (по умолчанию это, чаще всего, каталоги `/media/cdrom` или `/media/cdrom0`) и выполнить монтирование;
  - настроить фильтр проверки целостности в разделе «Принудительно», добавив регулярное выражение, содержащее абсолютный путь ко всем файлам каталога `/usr/lib: /usr/lib/*`;
  - настроить фильтр проверки целостности в разделе «Игнорировать», удалив регулярное выражение, содержащее абсолютный путь к каталогу `/tmp`;
  - в разделе «Отчёты» задать только текстовый формат файла отчёта, определив путь размещения файла `report.txt` в каталоге `/home/user/report`;
  - изменить содержимое файла `/usr/share/doc/libcap2/copyright` командой `vim /usr/share/doc/libcap2/copyright`, удалив в нем две первые строки;

```
Upstream-Contact: Andrew G. Morgan <morgan@kernel.org>
Source: https://www.kernel.org/pub/linux/libs/security/linux-privs/libcap2/
:d2
```

- начать проверку и зафиксировать предполагаемое время проверки, перейти во вкладку «Состояние» и проконтролировать статус проверки, после окончания проверки завершить работу графической утилиты;
  - в файле `/home/user/report.txt` найти строки, содержащие текст: «Файлы, целостность которых нарушена», «Контр. сумма» и «`/usr/share/doc/libcap2/copyright`» и сохранить результаты поиска в файл `/home/user/report-2` цепочкой команд: `grep 'Файлы, целостность которых нарушена' /home/user/report.txt -A 4 > /home/user/report-2; grep 'Контр. сумма' /home/user/report.txt -A 4 >> /home/user/report-2; grep '/usr/share/doc/libcap2/copyright' /home/user/report.txt >> /home/user/report-2.`
1. Отредактировать секцию `directives` конфигурационного файла `/etc/afick.conf` системы AFICK, отменив проверку выполняющихся приложений: исходный вариант секции `directives`: `running_files := yes`, отредактированный вариант секции `directives`: `running_files := 0`.

2. Отредактировать секцию *alias* конфигурационного файла */etc/afick.conf* системы *AFICK*:
  - изменить правило *ETC*, удалив из него проверку размера файловых сущностей и добавив проверку времени их модификации: исходный вариант правила: *ETC = p+d+i+u+g+s+md5*, отредактированный вариант правила: *ETC = p+d+i+u+g+m+md5*;
  - отредактировать правило *MyRule*, удалив из него проверку для файловых сущностей количества ссылок на них и добавив проверку контроля целостности мандатных меток безопасности, контроля целостности данных системы аудита безопасности и контроля целостности с использованием криптографического алгоритма ГОСТ Р 34.11-2012 вместо алгоритма *MD5*: исходный вариант правила: *MyRule = p+d+i+n+u+g+s+b+md5+m*, отредактированный вариант правила: *MyRule = p+d+i+u+g+s+b+gost+m+e+t*.
1. Отредактировать секцию *file section* конфигурационного файла */etc/afick.conf*:
  - заменить для каталога */boot* правило проверки *GOST* на правило проверки *PARSEC*: исходный вариант: */boot GOST*, отредактированный вариант: */boot PARSEC*;
  - добавить для файловой сущности */etc/fstab* правило проверки *MyRule*: отредактированный вариант: */etc/fstab MyRule*;
  - активировать правило проверки по умолчанию для каталога */lib*: исходный вариант: *#/lib MyRule*, отредактированный вариант: */lib MyRule*.
1. Обновить базу данных системы *AFICK* с учётом выполненных изменений в секции *file section* командой *afick -u*.
2. Изменить содержимое файла */etc/fstab*, удалив в нем две первые строки.
3. Запустить графическую утилиту «Контроль целостности файлов» (*afick-tk*) управления системой *AFICK* из меню «Системные» главного пользовательского меню и выполнить принудительную проверку целостности, выбрав действие – сравнение с базой.
4. После завершения контроля целостности:
  - в меню утилиты *afick-tk* «Файл — история» определить дату и время последнего принудительного контроля целостности;
  - найти в каталоге */var/lib/afick/archive* *log*-файл, соответствующий выполненной принудительной проверке (значение *YYYYMMDDHHMMSS* в имени *log*-файла должно совпадать с найденными в предыдущем пункте датой и временем проверки);
  - просмотреть найденный *log*-файл с помощью команды *less* и в его секции *#detaled changes* найти запись о нарушении целостности файловой сущности */etc/fstab* (раздел *changed file : /etc/fstab*);



- проанализировать найденную запись о нарушении целостности и определить параметры, соответствующие действиям (*action*) нарушения целостности, и их текущие значения.

1. Запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*.
2. Просмотреть загруженные модули ядра ОСЧН и вывести в терминал данные о невыгружаемом модуле *digsig\_verif* конвейером команд *lsmod | grep "digsig\_verif"*. Ответить на вопрос: связан ли модуль *digsig\_verif* с другими загружаемыми (невыгружаемыми) модулями?

```
root@astra:/etc/digsig# lsmod | grep "digsig_verif"
digsig_verif          491520  0
```

3. Просмотреть информацию о модуле *digsig\_verif* командой *modinfo digsig\_verif*. Определить расположение модуля *digsig\_verif* и информацию о разработчике.
4. Выполнить импорт открытых ключей, используемых для проверки ЭП файлов. Для этого выполнить следующие действия:
  - инициализировать каталог */root/.gnupg* при просмотре текущих ключей командой *gpg --list-sigs*;
  - импортировать открытый мастер-ключ «JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018)» командой *gpg --import letcdigsig/primary\_key\_2018.gpg*;
  - импортировать открытые ключи *partners\_rbt\_root\_key\_2018.gpg* и *build\_system\_rbt\_root\_key\_2018.gpg* (данный ключи используется для подписи файлов ОСЧН), командой *gpg --import letcdigsig/имя\_файла\_ключа*.

```
root@astra:/etc/digsig# gpg --list-keys
/root/.gnupg/pubring.kbx
-----
pub   gP256 2018-06-17 [SC]
      8066E9BD2201D9783E2D842BD2B6689A37DB8024
uid   [ неизвестно ] JSC RPA RusBITech (BUILD-SYSTEM RBT ROOT KEY 2018) <mail@rusbitech.ru>

pub   gP256 2018-06-17 [SC]
      A12D7B5BAFCE40D87FD41DAFC82D49FC3675B6FA
uid   [ неизвестно ] JSC RPA RusBITech (PARTNERS RBT ROOT KEY 2018) <mail@rusbitech.ru>

pub   gP256 2018-06-17 [SC]
      8E839E2F389F882A259F47997285E858DB069FF5
uid   [ неизвестно ] JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018) <mail@rusbitech.ru>
```

1. Вывести текущие ключи командой *gpg --list-sigs*. Определить идентификатор мастер-ключа «JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018)». Используется ли он для подписи других загруженных ранее ключей?

```

root@astra:/etc/digisig# gpg --list-sigs
/root/.gnupg/pubring.kbx
-----
pub   gP256 2018-06-17 [SC]
      8066E9BD2201D9783E2D0842BD2B6689A37DB8024
uid   [ неизвестно ] JSC RPA RusBITech (BUILD-SYSTEM RBT ROOT KEY 2018) <mail@rusbitech.ru>
sig 3   D2B6689A37DB8024 2018-06-17  JSC RPA RusBITech (BUILD-SYSTEM RBT ROOT KEY 2018) <mail@rusbitech.ru>
sig     7285E858DB069FF5 2018-06-17  JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018) <mail@rusbitech.ru>

pub   gP256 2018-06-17 [SC]
      A12D7B5BAFCE40D87FD41DAFC82D49FC3675B6FA
uid   [ неизвестно ] JSC RPA RusBITech (PARTNERS RBT ROOT KEY 2018) <mail@rusbitech.ru>
sig 3   C82D49FC3675B6FA 2018-06-17  JSC RPA RusBITech (PARTNERS RBT ROOT KEY 2018) <mail@rusbitech.ru>
sig     7285E858DB069FF5 2018-06-17  JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018) <mail@rusbitech.ru>

pub   gP256 2018-06-17 [SC]
      8E839E2F389F882A259F47997285E858DB069FF5
uid   [ неизвестно ] JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018) <mail@rusbitech.ru>
sig 3   7285E858DB069FF5 2018-06-17  JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018) <mail@rusbitech.ru>

```

2. Проверить корректность ЭП файла `/bin/dash` командой `bsign -w $(which dash)`. Определить каким ключом был подписан данный файл по его идентификатору в строке «`signer:`».
3. Переписать открытый ключ `/etc/digisig/build_system_rbt_root_key_2018.gpg` в каталог `/etc/digisig/keys` командой `cp /etc/digisig/build_system_rbt_root_key_2018.gpg /etc/digisig/keys`.
4. Перейти в каталог `/etc/digisig` и изменить файл `digisig_initramfs.conf` (значение `DIGSIG_ELF_MODE` установить равным 1).
5. Проверить корректность установки данного параметра путём открытия настройки «Замкнутой программной среды» в «Панели управления».
6. Проверить корректность ключа путём его загрузки в модуль `digisig_verif` командой `digisig_initramfs` (для поиска этой команды можно использовать команду `find`).
7. Создать дополнительный ключ ЭП командой `gpg --full-generate-key`. В диалоге команды `gpg`:
  - выбрать пункт 15 «GOST R 34.10-2012», указать неограниченный срок действия дополнительного ключа ЭП, выбрав значение 0;
  - указать параметры `Real Name: rootserver`, `Email: root@server.test` и получить `User ID: «rootserver <root@server.test>»`.
1. Вывести текущие ключи командой `gpg --list-sigs` и определить идентификатор ключа «`rootserver <root@server.test>`».
2. Скопировать файл `/bin/dash` в каталог `/root`, указав при этом новое имя файла `1.elf`.
3. Подписать файл `1.elf` новым ключом «`rootserver <root@server.test>`» командой `bsign --sign /root/1.elf`.



4. Вывести новую подпись файла командой `bsign -w /root/1.elf` и проверить соответствие идентификатора ключа ЭП в строке «*signer:*» данным ключа «*rootserver <root@server.test>*».
5. Включить штатный режим проверки ЭП с использованием модуля *digsig\_verif*, установив значение ключа *DIGSIG\_ELF\_MODE=1* в конфигурационном файле */etc/digsig/digsig\_initramfs.conf*.
6. Активировать настройки командой `sudo update-initramfs -u -k all`, затем выполнить перезагрузку и повторный вход в ОСН.
7. Запустить терминал *Fly* в «привилегированном» режиме командой `sudo fly-term`.
8. Проверить включение штатного режим функционирования модуля *digsig\_verif* (в файле */sys/digsig/elf\_mode* должно быть установлено значение «1») командой `cat /sys/digsig/elf_mode`.
9. Выполнить попытку запуска файла */root/1.elf*, который был подписан с использованием ключа «*rootserver <root@server.test>*» (данный ключ не был подписан мастер-ключом «*JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018)*»), и проанализировать выводимые ошибки.
10. Установить значение ключа *DIGSIG\_ELF\_MODE=0* в конфигурационном файле */etc/digsig/digsig\_initramfs.conf*, активировать настройки командой `update-initramfs -u -k all`, затем выполнить перезагрузку и повторный вход в ОСН.
11. В «привилегированном» режиме терминала *Fly* выполнить команду */root/1.elf* и проанализировать выводимые ошибки.
12. Выйти из запущенного интерпретатора «*dash*» (файл *1.elf*) командой `exit`. Активировать настройки командой `update-initramfs -u -k all`, затем выполнить перезагрузку и повторный вход в ОСН.
13. При наличии дополнительных ключей ЭП (ключи должны быть получены у разработчика и подписаны мастер-ключом «*JSC RPA RusBITech (PRIMARY RBT ROOT KEY 2018)*») выполнить следующие действия (далее имена файлов ключей *sign\_public.gpg* – открытый ключ, *sign\_secret.gpg* – закрытый ключ):
  - в «привилегированном» режиме терминала *Fly* выполнить очистку ключей в папке */root/.gnupg* командой `rm -r /root/.gnupg`;
  - импортировать ключи командами `gpg --import sign_public.gpg ; gpg --import sign_secret.gpg`;
  - импортировать открытый мастер-ключ командой `gpg --import /etc/digsig/primary_key_2018.gpg`;
  - проверить импорт ключей командой `gpg --list-sigs`, при этом должно отобразиться два ключа;

- добавить действующий ключ ЭП в модуль *digsig\_verif* командой `cat /etc/digsig/build_system_rbt_root_key_2018.gpg > /sys/digsig/keys;`
  - добавить новый ключ ЭП в модуль *digsig\_verif* командой `cat sign_public.gpg > /sys/digsig/keys;`
  - выполнить команду `echo "1" >/sys/digsig/elf_mode` для активации режима проверки ЭП файлов;
  - скопировать файл */root/1.elf* в новый файл командой `cp /root/1.elf /root/1signed.elf;`
  - выполнить команду */root/1.elf* и проанализировать выводимые ошибки (данный файл не должен запускаться по причине использования ЭП ключом «*rootserver <root@server.test>*»);
  - подписать файл *1signed.elf* командой `bsign --sign /root/1signed.elf`, затем проверить ЭП командой `bsign -w /root/1signed.elf;`
  - запустить подписанный файл командой */root/1signed.elf* и проверить отсутствие ошибок;
  - выполнить перезагрузку и повторный вход в ОСН, запустить терминал *Fly* в «привилегированном» режиме командой `sudo fly-term;`
  - проверить текущий режим модуля *digsig\_verif* командой `cat /sys/digsig/elf_mode` (режим должен быть равен 0);
  - перейти в каталог */root*, осуществить запуск файлов *1signed.elf* и *1.elf*, затем проанализировать полученные результаты и выводимые ошибки;
  - добавить ключи ЭП в модуль *digsig\_verif* командой `cat /etc/digsig/build_system_rbt_root_key_2018.gpg > /sys/digsig/keys` и `cat sign_public.gpg > /sys/digsig/keys`, осуществить повторный запуск файлов *1signed.elf*, *1.elf*; а затем проанализировать полученные результаты.
1. Создать ключи и выполнить подпись файла конфигурации.
    - запустить терминал *Fly* от имени учётной записи пользователя *user* командой `fly-term;`
    - скопировать файлы */etc/passwd* и */bin/dash* в каталог *~* и сменить владельца на *user:user*;
    - выполнить команду генерации мастер-ключа для подписи в *xattr* командой `gpg --full-generate-key`, выбрать алгоритм (15) и установить имя: *xattr-key*;
    - выполнить команду генерации ключа для подписи в *xattr* командой `gpg --full-generate-key`, выбрать алгоритм (15) и установить имя: *xattr-key-sign*;
    - выполнить подпись ключа «*xattr-key-sign*» командой `gpg --sign-key "xattr-key-sign" > xattr-key-sign.gpg;`
    - экспортировать ключ «*xattr-key*» командой `gpg --export "xattr-key" xattr-key.gpg;`
    - проверить наличие подписанного ключа «*xattr-key-sign*» командой `gpg --list-sigs` (при этом ключ «*xattr-key-sign*» должен быть подписан ключом «*xattr-key*»);

- запомнить идентификаторы ключей «*xattr-key*» и «*xattr-key-sign*» (8 байт в шестнадцатеричном формате — 16 символов);
- создать хэш файла *~/.passwd* и записать его в расширенные атрибуты командой *bsign --hash ~/.passwd* (обратить внимание, что никаких ключей разблокировки секретного ключа при этом не запрашивается у пользователя);
- создать файл *~/.gnupg/gpg.conf* с содержимым: *default-key идентификатор\_ключа\_xattr-key-sign*;
- выполнить подпись файла *passwd* командой *bsign --sign ~/.passwd*;
- выполнить проверку подписи файла *passwd* командой *bsign -w ~/.passwd*;
- скопировать ключи (*xattr-key-sign.gpg* и *xattr-key.gpg*) для работы с подписями файлов в каталог */etc/digisig/xattr\_keys*;
- в графическом файловом менеджере *fly-fm* перейти в каталог «Домашний» и открыть в контекстном меню «Свойства», «Подпись» файла *passwd*;
- нажать кнопки «Загрузить ключи» и «Информация», при этом проверить корректность созданного хэш и наличие подписи.

## Содержание отчёта по выполненной работе

В отчёте по выполненной работе необходимо указать:

1. Полный перечень использованных команд с описанием их назначения.
2. Примеры выполнения команд, которые были использованы в ходе работы, с описанием результатов их выполнения.
3. Описание порядка работы с графическим интерфейсом при выполнении следующих операций:
  - конфигурирование обязательных для проверки и игнорируемых путей в графической утилите *fly-admin-int-check*;
  - конфигурирование пути размещения файла отчёта в графической утилите *fly-admin-int-check*;
  - просмотр текущих правил проверки в графической утилите «Контроль целостности файлов» (*afick-tk*) системы регламентного контроля целостности *AFICK*;
  - запуск проверки целостности данных в графической утилите *afick-tk*.
1. Описание порядка работы с командами при выполнении следующих операций:
  - вычисление контрольной суммы файла с использованием команды *md5sum*;
  - вычисление контрольной суммы файла с использованием команды *shasum*;
  - вычисление контрольной суммы файла с использованием команды *gostsum*;
  - проверка целостности файлов с использованием команды *md5sum*;

- проверка целостности файлов с различными алгоритмами вычисления контрольной суммы с использованием утилиты *shasum*.
1. Описание особенностей конфигурирования и режимов функционирования модуля *digsig\_verif*.

### Контрольные вопросы

1. В чем заключается отличие команд *md5sum*, *shasum* и *gostsum* с точки зрения вычисления контрольной суммы файлов?
2. В каком формате организован вывод команд *md5sum*, *shasum* и *gostsum* при вычислении контрольной суммы файлов?
3. Какая из команд *md5sum*, *shasum* или *gostsum* выполняет только вычисление контрольной суммы файлов и не выполняет проверку их целостности?
4. В какой из команд *md5sum*, *shasum* или *gostsum* возможно изменение алгоритма хэширования?
5. Каково назначение файла *gostsum.txt*, и где этот файл располагается?
6. Какие псевдонимы (*aliases*) в конфигурационном файле системы регламентного контроля целостности *AFICK* соответствуют правилам проверки целостности мандатных меток безопасности файлов и контроля целостности данных системы аудита безопасности?
7. Какие правила в конфигурационном файле системы регламентного контроля целостности *AFICK* сформированы по умолчанию, а какие являются специфическими для подсистемы безопасности *PARSEC*?
8. В каких средствах контроля целостности используется библиотека *libgost*?
9. Как инициализировать базу данных системы регламентного контроля целостности *AFICK* после внесения изменений в её конфигурационный файл?
10. Каким образом реализована взаимосвязь системы регламентного контроля целостности *AFICK* и сервиса *cron*?
11. Каким видом модулей ядра ОССН является модуль *digsig\_verif*?
12. Какой формат файлов ключей ЭП СПО использует модуль *digsig\_verif*?
13. Какая специализированная файловая система применяется для хранения данных о состоянии и функционировании модуля *digsig\_verif*?
14. Какой файл сценария командного интерпретатора *bash* применяется при добавлении дополнительных ключей ЭП для модуля *digsig\_verif*?



# ЛАБОРАТОРНАЯ РАБОТА №7.

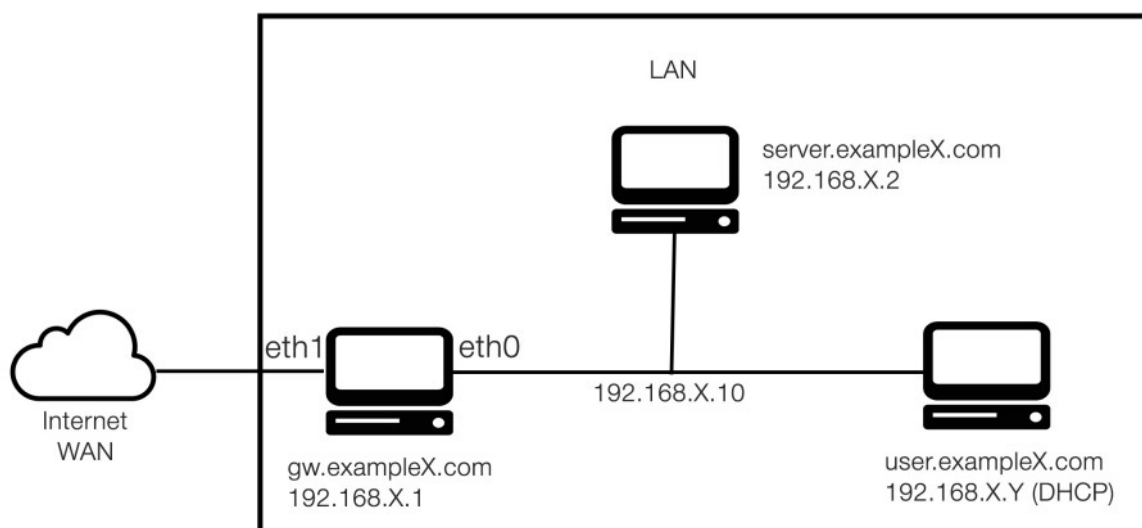
## РАЗВЕРТЫВАНИЕ СТЕНДА. НАСТРОЙКА DNS СЕРВЕРА

**Цель работы:** Подготовить стенд для дальнейшего использования. Настроить DNS-сервер

**Время выполнения работы:** 2 академических часа.

### Краткие теоретические сведения

Схема стенда:



компьютер слушателя

### Используемое методическое и лабораторное обеспечение

1. Два компьютера (либо виртуальные машины) с ОССН версии 1.6 с графическим интерфейсом, соединённые в сеть: gate, server. При этом компьютер с ОССН gate имеет два сетевых интерфейса.
2. В каждой ОССН создана учётная запись пользователя *student*, 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*).

3. Дистрибутив ОССН.
4. Документация: «Операционная система специального назначения «Astra Linux Special Edition». Описание применения», «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».
5. Для выполнения работы в течение двух занятий необходимо обеспечить возможность сохранения состояния ОССН за счёт применения технологий виртуализации (создания виртуальных машин с ОССН).

### Порядок выполнения работы

1. В работе используем стенд, развернутый вместе с преподавателем, в соответствии со схемой указанной выше
2. Настройте сервер gw в соответствии с конфигурацией указанной выше. Номер Вашей сети обозначатся X, и указан на Вашем системном блоке

Ваша сеть: 192.168.X.0/24 Домен: exampleX.com

IP адрес для gw: 192.168.X.1

Маска сети: 255.255.255.0

Имя хоста для gw: gw.exampleX.com

3. На компьютере gw.exampleX.com:

#### **# cat /etc/hosts**

127.0.0.1 localhost

192.168.X.1 gw.exampleX.com gw

#### **# cat /etc/resolv.conf**

search exampleX.com

nameserver 192.168.X.1

#### **# cat /etc/hostname**

gw

#### **# cat /etc/network/interfaces**

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.X.1

netmask 255.255.255.0

auto eth1

iface eth1 inet dhcp

#### **# init 6**

...

4. По аналогии настройте server

IP адрес для server: 192.168.X.2

Маска сети: 255.255.255.0

Имя хоста для server: server.exampleX.com

На компьютере server.exampleX.com (проверьте настройки сети для сервера):

**# cat /etc/hosts**

127.0.0.1 localhost

192.168.X.2 server.exampleX.com server

**# cat /etc/resolv.conf**

search exampleX.com

nameserver 192.168.X.1

**# cat /etc/hostname**

server

**# cat /etc/network/interfaces**

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.X.2

netmask 255.255.255.0

gateway 192.168.X.1

**# init 6**

...

**# apt-get update**

5. При необходимости перезагрузите виртуальную машину и отключите

**NetworkManager**

**# systemctl stop NetworkManger**

**# systemctl disable NetworkManger**

6. Настройте первичный DNS — сервер на компьютере **gw** для Вашего домена exampleX.com в соответствии с конфигурацией, указанной ниже. Проверьте работу DNS-сервера с компьютера server и с клиентской виртуальной машины Windows.

7. На компьютерах server.exampleX.com и gw.exampleX.com: откройте терминал, введите sudo su и ваш пароль для получения прав суперпользователя.

8. Установите пакет bind9 при помощи пакетного менеджера в системе.

**# apt-get install bind9**

8. Укажите основной dns-сервер



```
# vi /etc/resolv.conf
search exampleX.com
nameserver 192.168.X.1
```

9. Настройте журналирование. Права могут быть максимальными на этапе изучения

```
# touch /var/log/bind.log
# chmod 777 /var/log/bind.log
# ls -l /var/log/bind.log
```

10. Перейдем к редактированию основного конфигурационного файла и добавим ссылку на наш журнал

```
# vi /etc/bind/named.conf
logging {
    channel bind.log {
        file "/var/log/bind.log" versions 10 size 20m;
        severity notice;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    category queries { bind.log; };
    category default { bind.log; };
    category config { bind.log; };
};
```

11. Добавим общие настройки к нашей конфигурации. Укажем место расположение временных файлов сервера, используя параметр **directory**. С помощью параметра **listen-on** укажем какие интерфейсы будут отвечать на запросы пользователей по 53 порту. Также можно добавить параметр **forwarders**, и указать внешний dns, куда будем переадресовывать наши запросы если сервер не может их обработать. Разрешим кто может обращаться к нашему серверу (параметр **allow-query**) и куда можно передавать зоны **allow-transfer** (нужен если есть slave-сервер)

```
# vi /etc/bind/named.conf.options

options {
    directory "/var/cache/bind";
    listen-on { 192.168.X.1; 127.0.0.1; };
    max-cache-size 10m;
    forwarders {
        8.8.8.8;
    };
};
```

```

allow-query {
    192.168.X/24;
    127.0.0.1;
};
allow-transfer {
    192.168.X/24;
    127.0.0.1;
};
dnssec-validation auto;
auth-nxdomain no; # conform to RFC1035
};

```

13. Теперь можно проверить конфигурацию на наличие ошибок и если ошибок нет перезапустить dns-сервер. Также, если Вы не изменяли `resolv.conf`, можно сгенерировать его

```
# named-checkconf
```

```
# systemctl restart bind9
```

14. В конфигурационный файл `named.conf.local` добавим информацию о прямой и обратной зонах, которые создадим далее

```
# vi /etc/bind/named.conf.local
```

```

zone "exampleX.com" {
    type master;
    file "/var/lib/bind/db.exampleX.com";
    allow-update { key rndc-key; };
};

zone "X.168.192.in-addr.arpa" {
    type master;
    file "/var/lib/bind/db.192.168.X";
    allow-update { key rndc-key; };
};

```

15. Следующим шагом создадим прямую зону:

```
# vi /var/lib/bind/db.exampleX.com
```

```

$TTL 604800 ; 1 week
@      IN      SOA  exampleX.com. root.exampleX.com. (
                        2020052201 ; serial
                        604800 ; refresh (1 week)
                        86400  ; retry (1 day)
                        2419200 ; expire (4 weeks)
                        604800 ; minimum (1 week)
                        )
@      IN      NS   gw.exampleX.com.

```

```
@      IN A  192.168.X.1
gw      IN A  192.168.X.1
server  IN A  192.168.X.2
user    IN A  192.168.X.100
```

16. Создаем обратную зону

# vi /var/lib/bind/db.192.168.X

```
$TTL 604800 ; 1 week
@ IN SOA  exampleX.com. root.exampleX.com. (
                                2020052701 ; serial
                                604800 ; refresh (1 week)
                                86400 ; retry (1 day)
                                2419200 ; expire (4 weeks)
                                604800 ; minimum (1 week)
                                )
@      IN  NS   gw.exampleX.com.
1      IN  PTR  gw.exampleX.com.
2      IN  PTR  server.exampleX.com.
100    IN  PTR  user.exampleX.com.
```

17. Теперь можно проверить конфигурацию файлов зон на наличие ошибок и если ошибок нет перезапустить dns-сервер.

**# named-checkconf -z**

**# systemctl restart bind9**

18. Используйте команды для тестирования dns-сервера:

```
# ping gw.exampleX.com
# ping test.exampleX.com
# dig ya.ru
# nslookup ya.ru 127.0.0.1
# rndc status
# systemctl status bind9
# netstat -lnp | grep :53
```

19. Настройте клиентскую машину. Если Вы используете виртуальную машину с курса ALSE-1604 и у Вас настроен DHCP-сервер. Клиентская машина должна получать адрес с этого сервера.

Если у Вас DHCP-сервер не настроен. Клиентская машина должна получать статический адрес, например:

Ваша сеть: 192.168.X.0/24 Домен: exampleX.com

IP адрес для user: 192.168.X.100

Маска сети: 255.255.255.0

Имя хоста для user: user.exampleX.com

## Контрольные вопросы

1. Каково назначение пакета *iproute2*?

2. Каково назначение конфигурационных файлов в каталоге */etc/NetworkManager*?
3. Какие параметры ядра обеспечивают включение функции «*IP forwarding*»?
4. Какими командами осуществляется проверка и управление характеристиками сетевых интерфейсов?
5. Какие особенности настройки работы сетевых служб с использованием механизма *privsock*?
6. Какой пакет используется для настройки DNS-сервера?

# ЛАБОРАТОРНАЯ РАБОТА №8.

## КОНФИГУРИРОВАНИЕ СЛУЖБЫ

### ASTRA LINUX DIRECTORY.

**Цель работы:** Получить практический опыт установки и настройки параметров службы *Astra Linux Directory (ALD)* в ОССН.

**Время выполнения работы:** 6 академических часов.

#### Краткие теоретические сведения

В компьютерных сетях, построенных на основе ОССН, имеется возможность организовать централизованное хранение учётных записей пользователей в домене *ALD* (далее – домене), а также развёртывать централизованный защищённый файловый сервер, содержащий сетевые домашние каталоги данных учётных записей пользователей. Таким образом, у учётных записей пользователей *ALD* появляется возможность регистрации и доступа к своим сетевым объектам с любого компьютера, входящего в домен. Это особенно актуально, в случае территориальной удалённости между контроллером *ALD* и компьютерами, входящими в состав домена.

Хотя в ОССН версии 1.6 также реализована более современная доменная инфраструктура *FreeIPA*, которая подробно рассмотрена в главах 1 и 3, её конфигурирование и настройка являются гораздо более сложными, чем *ALD*, и поэтому выходят за рамки лабораторной работы.

Администратор домена *ALD* выполняет следующие функции по управлению доменом:

- централизованное управление учётными записями пользователей домена с использованием команды *ald-admin* и графической утилиты «Политика безопасности» (для этого необходимо установить расширение *smolensk-security-ald*);
- настройка СЗИ, управляющих их доступом к файловым сущностям защищённого файлового сервера.

Централизованная база данных учётных записей пользователей домена (*DIB – Domain Information Base*) создаётся на основе службы *LDAP (Lightweight Directory Access Protocol)*, обеспечивающей, как организацию хранилища учётных записей пользователей *ALD*, так и процедуру аутентификации пользователей на компьютере с использованием *ALD*. Безопасность процедуры аутентификации пользователей домена обеспечивается

применением протокола доверенной аутентификации *Kerberos*. Для синхронизации временных меток при взаимодействии контроллера и клиентов *Kerberos* используется протокол *NTP (Network Time Protocol)*.

При доступе к сущностям файловой системы компьютера, с которого осуществлён вход в домен с некоторой учётной записью пользователя, для неё применяются настройки управления доступом, хранящиеся на контроллере *ALD*. Если же на контроллере *ALD* (или на специально выделенном компьютере) организуется защищённый файловый сервер, то настройки управления доступом для этой учётной записи пользователя применяются также к сущностям файловой системы этого контроллера. При этом доступ к ним от имени учётной записи пользователя *ALD* осуществляется по протоколу *CIFS (Common Internet File System)*, являющемуся развитием протокола сетевого файлового обмена *SMB*.

Служба *ALD* обладает расширяемой архитектурой, состоящей из ядра, отвечающего за основную функционал системы, ряда интерфейсов (*LDAP*, *Kerberos*) и модулей расширения, команд и графических утилит настройки служб и подсистем *ALD*, что позволяет расширять функциональность *ALD*, устанавливая дополнительные пакеты. Основные пакеты, используемые при установке и настройке *ALD*, являются:

- *ald-client-common* – клиентская часть *ALD* (можно также использовать метапакет *ald-client*);
- *ald-admin* – команды администрирования *ALD*;
- *ald-server-common* – серверная часть *ALD* (можно также использовать метапакет *ald-server*);
- *smolensk-security-ald* – расширения графической утилиты «Политика безопасности», позволяющие осуществлять управление доменом (можно также использовать метапакеты *ald-admin-ald-se* или *ald-admin-ald-server*).

На компьютере, осуществляющем функции контроллера *ALD*, операции по администрированию *ALD* выполняются от имени учётных записей пользователей, обладающих соответствующими административными полномочиями. В зависимости от назначенных привилегий администраторов *ALD* можно разделить на следующие группы по полномочиям:

- корневой администратор (имя *admin/admin*, администратор *ALD*) – обладает всеми полномочиями по управлению доменом;
- администраторы (пользователи с привилегией *admin*) – обладают полномочиями по управлению конфигурацией домена и учётными записями пользователей;
- ограниченные администраторы (учётные записи пользователей с привилегиями *hosts-add* или *ald-hosts-add*) – обладают полномочиями по добавлению компьютеров в домен;

- пользователи утилит администрирования (пользователи с привилегией *adm-user*) – обладают полномочиями по запуску утилит администрирования;
- обычные пользователи.

Для администрирования домена используются команды *ald-admin* и графическая утилита «Политика безопасности», которая позволяет выполнять следующие действия с доменом:

- создание и администрирование учётных записей пользователей;
- создание и администрирование групп;
- добавление и удаление компьютеров;
- резервирование и восстановление учётной информации баз данных домена;
- конфигурирование привилегий и политик СЗИ для учётных записей пользователей и групп;
- конфигурирование политик паролей *Kerberos*;
- администрирование доступа к съёмным устройствам;
- администрирование учётных записей сетевых служб (сервисов);
- контроль целостности (аудит) конфигурации домена.

При создании нового домена используется следующая последовательность действий:

- настройка сетевого соединения на контроллере *ALD* и компьютерах, которые будут включены в *ALD*;
- настройка именования контроллера и клиентов *ALD* для поддержки функционирования службы *LDAP*;
- конфигурирование и запуск контроллера *ALD*;
- запуск клиентов *ALD* на компьютерах, входящих в *ALD*.

Данная последовательность действий рассматривается при выполнении лабораторной работы.

При развёртывании средств обеспечения единого пространства пользователей с применением *ALD* используются следующие команды (примеры применения которых также рассмотрены в главе 3):

- *hostname* — команда вывода в терминал текущего имени компьютера;
- *apt-get* — команда управления пакетами;
- *ping* — команда отправки и получения пакетов *ICMP* (*Echo Request/ Echo Reply*);
- *ald-init* — команда инициализации базы данных *ALD*;
- *ald-client* — команда управления клиентом *ALD*;
- *ald-admin* — команда управления доменом *ALD*.

## Используемое методическое и лабораторное обеспечение

1. Три компьютера с ОССН версии 1.6, объединённые в сеть. Первый предназначен для использования в качестве контроллера *ALD* — далее обозначается *gw.exampleX.com*; остальные — компьютеры, подключаемые в домен (*server.exampleX.com*, *user.exampleX.com*). В ОССН настроена синхронизация времени с использованием протокола *NTP*, либо, при использовании виртуальных машин временные метки считываются автоматически из единого системного времени.
2. В каждой ОССН создана учётная запись пользователя *student*, 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*).
3. Дистрибутив ОССН.
4. Документация: «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство администратора. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство по КСЗ. Часть 1».
5. Для выполнения работы в течение двух занятий необходимо обеспечить возможность сохранения состояния ОССН за счёт применения технологий виртуализации (создания виртуальных машин с ОССН).

## Порядок выполнения работы

1. Для настройки сетевого соединения на контроллере и клиентах *ALD* начать работу со входа в ОССН *server*, *user* и *gw* в графическом режиме с учётной записью пользователя *student* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).
2. В ОССН *server*, *user* и *gw* выполнить настройку статических сетевых адресов в соответствии с предыдущим модулем.
3. Выполнить перезагрузку и повторный вход в каждую ОССН с учётной записью пользователя *student* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»), затем запустить терминал *Fly*.
4. Выполнить проверку корректности настроек командой *ping*. При этом проверить доступность *server*, *user* с *gw* по сети командами: *ping 192.168.X.2* и *ping 192.168.X.Y*.
5. Выполнить настройку имени контроллера и клиентов *ALD* для поддержки функционирования службы *LDAP*. Для этого необходимо, чтобы разрешение сетевых имён было настроено таким образом, чтобы сетевое имя компьютеров разрешалось, в первую очередь, как полное имя (например, *gw.exampleX.com*). При этом команда



*hostname* должна возвращать короткое сетевое имя (например, gw). Для этого выполнить следующую последовательность действий:

- в ОССН *server*, *user* и *gw* в «привилегированном» режиме терминала *Fly* выполнить проверить настройки файла */etc/hostname* в соответствии с предыдущей лабораторной работой;
- в ОССН *server*, *user* и *gw* в «привилегированном» режиме проверить настройки файла */etc/hosts* в соответствии с предыдущей лабораторной работой и закомментировать строку, содержащую запись «127.0.1.1» (для этого поставить в начале данной строки «#»);
- выполнить перезагрузку ОССН *server*, *user* и *gw* и войти в ОССН в графическом режиме с учётной записью пользователя *student* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);
- в каждой ОССН запустить терминал *Fly*, выполнить команду *hostname* и проверить, что она возвращает короткие имена *server*, *user* и *gw*.

```
root@gw:~# hostname
gw
root@gw:~#
```

6. Выполнить установку, конфигурирование и запуск контроллера. Для этого реализовать следующую последовательность действий в ОССН *gw*:

- войти в графическом режиме с учётной записью пользователя *student* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);
- запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*;
- выполнить установку пакетов для работы с контроллером (если ALD сервер не был установлен при инсталляции ОС) командой:

**# apt -y install ald-server-common ald-admin-common ald-admin smolensk-security-ald fly-admin-ald-server**

- при наличии ошибок запустите команду:

**# apt --fix-broken install**

- перезагружаем ОС;
- выполнить команду *vim /etc/ald/ald.conf* и проверить наличие параметров «*SERVER=gw.exampleX.com*» и «*DOMAIN=.exampleX.com*»;

```

VERSION=1.7
# Version of ald

DOMAIN=.example2.com
# The name of your domain (also used as Kerberos realm in upper-case).
# Should be in the form:
# .example.com
# !NOTE! (for ald-server). If this value is changed – the server should be
# reinitialized by:
# $ ald-init init
# Or you should use the commands 'ald-init backup-ldif' and
# 'ald-init restore-backup-ldif'.

SERVER=gw.example2.com
# Fully qualified name of Astra Linux Directory server.
# Should be in the form:
# my-ald-server.example.com

SERVER_ID=1

```

- также проверьте в файле наличие параметра `SERVER_ON=1` и `CLIENT_ON=1`, при необходимости сделайте изменения;
- для того, чтобы служба *ALD* заново считала изменения в файле `/etc/ald/ald.conf` (если они реально делались, иначе пропустить указанную далее команду) выполнить инициализацию командой `ald-init commit-config` (результатом будет информация об успешном конфигурировании службы *ALD*);

```

root@gw:~# vi /etc/ald/ald.conf
root@gw:~# ald-init commit-config
ВНИМАНИЕ! Некоторые необходимые сервисы (OpenLDAP, Kerberos, nslcd, nscd) могут быть перезапущены!
Выполнение smbstatus -d 0 -p
Продолжить? (yes/no) [no]: yes
Обработка шаблона конфигурационного файла '/etc/ald/config-templates/ldap.conf' в '/etc/ldap/ldap.conf'...
Переименование '/etc/ldap/ldap.conf' в '/etc/ldap/ldap.conf.before_ald'...
Переименование '/etc/ldap/ldap.conf.tmp' в '/etc/ldap/ldap.conf'...
Обработка шаблона конфигурационного файла '/etc/ald/config-templates/krb5.conf' в '/etc/krb5.conf'...

```

- выполнить команду инициализации `ald-init init` и по требованию этой команды подтвердить повторную инициализацию баз данных *LDAP* и *Kerberos*, ввести и подтвердить новый *Kerberos*-пароль «*kerberosroot*», ввести и подтвердить новый пароль администратора *ALD* «*aldroot*».

```

root@gw:~# ald-init init
ВНИМАНИЕ! Команда 'init' УНИЧТОЖИТ ВСЮ БАЗУ ДАННЫХ LDAP и Kerberos!
Также во время выполнения этой команды могут быть остановлены и перезапущены LDAP, Kerberos, NFS/Samba и некоторые другие службы.
Разыменованное имя компьютера: gw.example2.com

Контроллер домена '.example2.com' будет создан со следующими параметрами:
Сервер: gw.example2.com
Роль сервера: Первичный контроллер домена
ID сервера: 1
Первичный контроллер домена: gw.example2.com

Вы УВЕРЕНЫ, что хотите ВЫПОЛНИТЬ эту операцию? (yes/no) [no]: yes
Введите новый главный пароль к базе данных Kerberos (НЕ ЗАБУДЬТЕ ЕГО!): *****
Повторите пароль: *****
Введите новый пароль администратора Astra Linux Directory (НЕ ЗАБУДЬТЕ ЕГО!): *****
Повторите пароль: *****
Сохранение конфигурации...
Обработка конфигурационного файла '/etc/ald/ald.conf'...

```

.....

```

Обработка конфигурационного файла '/etc/exports'...
Переименование '/etc/exports.tmp' в '/etc/exports'...
Запуск сервиса nmbd...
Запуск сервиса smbd...
Перезапуск сервиса nscd...
Перезапуск сервиса nslcd...
Перезапуск сервиса aldd...

```

```

Astra Linux Directory сконфигурирована.
Сервер ALD активен.
Клиент ALD включен.

```

Astra Linux Directory сервер успешно инициализирован.

- Правильно ли установился сервер можно проверить с помощью следующих команд **ald-client status** и **ald-admin test-integrity**

```

student@gw:~$ sudo su -
root@gw:~# ald-client status
Текущие установки, основанные на конфигурационном файле '/etc/ald/ald.conf':
ALDD_USER=aldd
ALD_CC_PREFIX=admin_tickets
ALD_CFG=/etc/ald/ald.conf
ALD_CFG_DIR=/etc/ald/config-templates
ALD_CFG_MODULES_DIR=/usr/lib/x86_64-linux-gnu/ald/config-modules
ALD_CFG_ROOT_DIR=/etc/ald
ALD_CFG_TEMPL_DIR=/usr/share/ald/config-templates

```

.....

```

USE_DNS=0
USE_DOCUMENTS=1
USE_RPC=1
UTF8_GECOS=1
VALID_GROUP_NAMES=[A-Za-z][A-Za-z0-9\.\_\-\ ]*$
VALID_USER_NAMES=[a-z][a-z0-9\.\_\-\ ]*$
VERSION=1.7

```

```

Astra Linux Directory сконфигурирована.
Сервер ALD активен.
Клиент ALD включен.

```

```

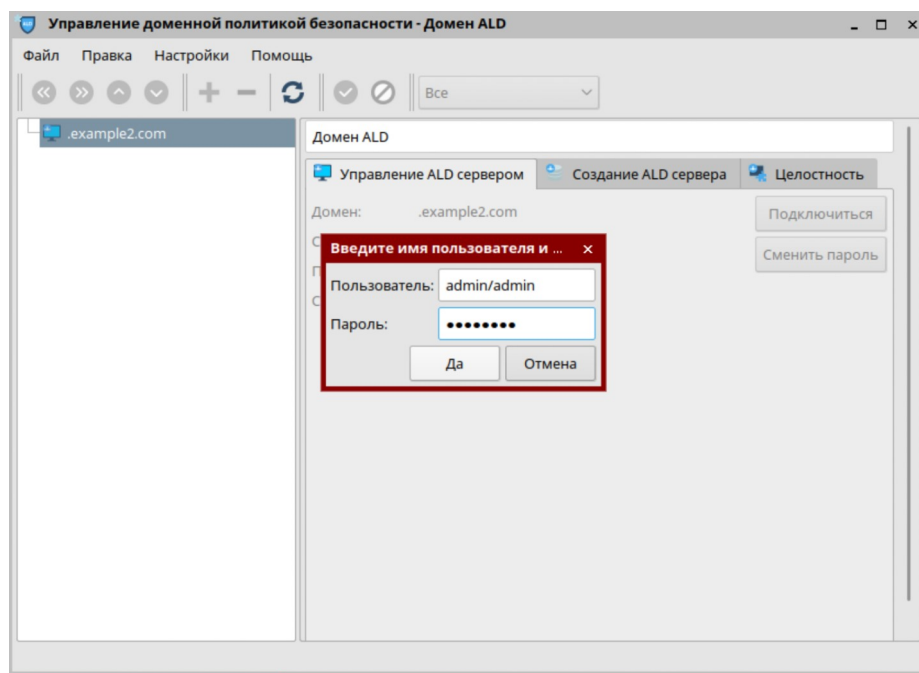
root@gw:~# ald-admin test-integrity
Введите пароль администратора ALD: *****
Проверка конфигурации домена.....ok
Проверка модулей LDAP.....ok
Проверка индексов LDAP.....ok
Проверка ограничений уникальности LDAP.....ok
Проверка системных принципов.....ok
Проверка компьютеров.....ok
Проверка имени сервера.....ok
Проверка групп компьютеров.....ok
Проверка серверов ALD.....ok
Проверка политик паролей.....ok
Проверка пользователей.....ok
Проверка групп.....ok
Проверка администраторов.....ok
Проверка сервисов.....ok
Проверка групп сервисов.....ok
Проверка доменных документов.....ok
Проверка доверенных доменов.....ok
Проверка серверных заданий.....ok
Проверка политики регистрации событий по умолчанию.....ok
Проверка политик регистрации событий пользователей.....ok
Проверка групповых политик регистрации событий.....ok
Проверка правил доступа к устройствам.....ok
Проверка устройств.....ok
Проверка мандатных уровней.....ok
Проверка мандатных категорий.....ok
Проверка мандатных прав пользователей.....ok
root@gw:~#

```

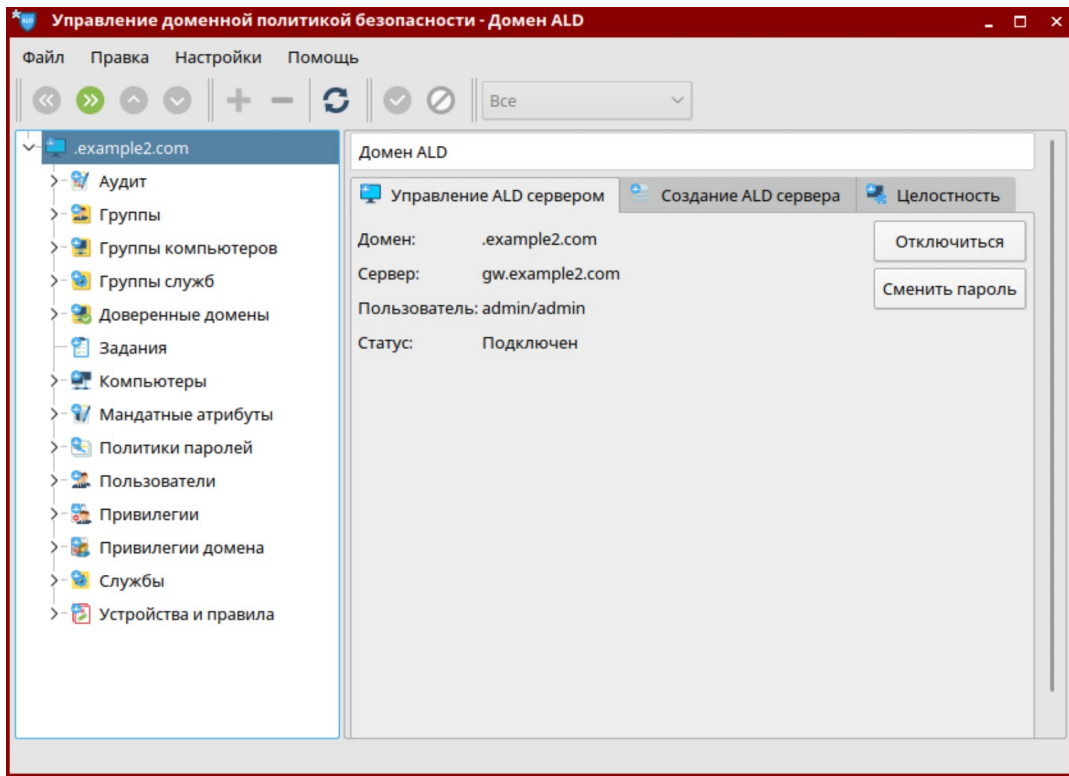
- Если возникают ошибки, следует перезагрузить ОС

7. Если предыдущие команды были выполнены успешно, находясь в графическом режиме на компьютере gw проверьте работу ALD следующим образом:

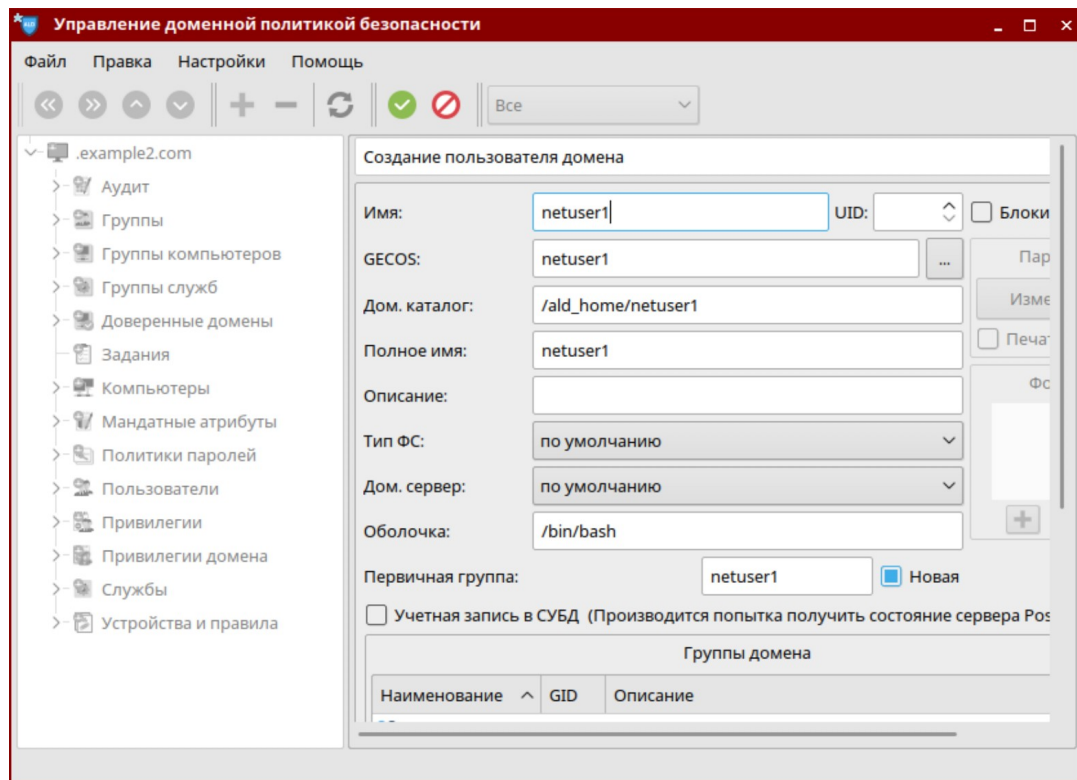
- Открываем на сервере приложение Управление доменной политикой безопасности:  
Пуск -> Панель управления -> Сеть -> Доменная политика безопасности



- Вводим логин и пароль, который задавали ранее



- Создайте доменного пользователя netuser1 и задайте ему пароль. А Во вкладке Привилегии домена разрешите вход на нужные ПК



- После этого можно выйти из под пользователя *student* и попробовать зайти в систему под доменным пользователем

8. Следующим шагом необходимо выполнить установку, конфигурирование, запуск клиентов *ALD*. Для этого реализовать следующую последовательность действий:

- в ОСCH server запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*;
- выполнить установку пакета *ald-client-common* командой *apt-get install ald-client-common*;
- выполнить команду *nano /etc/ald/ald.conf* и отредактировать следующие параметры: «*SERVER=astra-server.example.ru*» и «*DOMAIN=.example.ru*»;
- выполнить инициализацию настроек и подключение к контроллеру командой *ald-client commit-config*;
- в качестве имени учётной записи пользователя администратора ввести пробел или *admin/admin*, далее ввести пароль администратора *ALD aldroot*;
- выполнить запуск клиента *ALD* командами *ald-client start* (для включения компьютера в домен может отдельно использоваться команда *ald-client join*).

1. Осуществить проверку функционирования и настройку контроллера и клиентов *ALD*. Для этого выполнить следующую последовательность действий:

- в ОСCH *AstraServer* выполнить установку расширения графической утилиты «Управление политикой безопасности», используемого для конфигурирования контроллера *ALD* командой *apt-get install smolensk-security-ald*;
- запустить графическую утилиту «Политика безопасности» через меню «Панель управления» главного пользовательского меню и открыть вкладку «Домен *ALD*», соответствующую настройкам созданного домена;
- для администрирования домена необходимо выполнить подключение, проверить имя пользователя «*admin/admin*», ввести пароль администратора *ALD* «*aldroot*», а затем проверить, что контроллер *ALD* активирован (при этом должна отображаться надпись «Сервер домена: *astra-server.example.ru*»);
- в дереве элементов вкладки политик безопасности контроллера *astra-server.example.ru* выбрать узел «Компьютеры» и проверить, что в состав домена с именем «*.example.ru*» входят контроллер *ALD* «*astra-server.example.ru*» и клиент «*astra-client1.example.ru*»;

1. Создать новую учётную запись пользователя *ALD* и осуществить вход с ней в ОСCH *AstraClient1*. Для этого осуществить следующие действия:



- в ОСН AstraServer запустить графическую утилиту «Политика безопасности» через меню «Панель управления» главного пользовательского меню и открыть вкладку «Домен ALD» в разделе «Элементы»;
  - осуществить подключение с учётной записью пользователя «admin/admin»;
  - в дереве элементов вкладки политик безопасности контроллера *astra-server.example.ru* выбрать узел «Пользователи» и создать новую учётную запись пользователя *userald*, при этом, задав её пароль (обратить внимание на требование политики по сложности пароля);
  - в учётной записи пользователя *userald* в вкладке «Привилегии домена» выбрать «Компьютеры» добавить только *astra-server.example.ru* и применить изменения;
  - в ОСН AstraClient1, AstraClient2 выйти из ОСН;
  - осуществить попытку входа в ОСН AstraClient1 с новой учётной записью пользователя *userald* и проанализировать выводимые ошибки;
  - теперь в учётной записи пользователя *userald* в вкладке «Привилегии домена» выбрать «Компьютеры» и добавить *astra-client1.example.ru*;
  - войти в ОСН AstraClient1 с учётной записью пользователя *userald*;
  - осуществить попытку входа в ОСН AstraClient2 с учётной записью пользователя *userald* и проанализировать выводимую ошибку.
1. Осуществить установку, конфигурирование, запуск клиента ALD на AstraClient2. Для этого выполнить следующую последовательность действий:
    - войти в ОСН AstraClient2 в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);
    - запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*;
    - выполнить установку пакета *ald-client-common* командой *apt-get install ald-client-common*;
    - выполнить подключение к домену командой *ald-client join astra-server.example.ru*;
    - проверить корректность модификации файла настройки клиента ALD, выполнив команду *head -25 /etc/ald/ald.conf*, при этом должны быть установлены следующие параметры: «SERVER=*astra-server.example.ru*» и «DOMAIN=*example.ru*».
  1. Проверить корректность включения компьютера *astra-client2.example.ru* в домен «*example.ru*». Для этого выполнить следующую последовательность действий:
    - в ОСН AstraServer перезапустить графическую утилиту «Политика безопасности», затем открыть вкладку «Домен ALD» и выполнить подключение к домену;
    - выбрать узел «Компьютеры» и проверить, что в состав домена с именем «*example.ru*» входит клиент ALD *astra-client2.example.ru*;

- открыть узел «Привилегии домена» – «*userald*», в поле «Компьютеры» добавить «*astra-client2.example.ru*» к списку разрешённых компьютеров;
  - выйти из ОССН.
1. Проверить функционирование сетевой файловой системы при доступе к домашним каталогам учётных записей пользователей *ALD*. Для этого выполнить следующую последовательность действий:
    - войти в ОССН *AstraClient2* в графическом режиме с учётной записью пользователя *userald*;
    - в ОССН *AstraClient2* в графической утилите «Менеджер файлов» открыть каталог «Документы», создать в нем текстовый файл с именем *file-from-a/3.txt*, затем открыть данный файл в редакторе *Juffed* и добавить строку «Создан на ЦК 3»;
    - в ОССН *AstraClient1* в сессии, функционирующей от имени учётной записи пользователя *userald*, в графической утилите «Менеджер файлов» открыть каталог «Документы» и проверить наличие файла с именем *file-from-a/3.txt*;
    - в ОССН *AstraServer* запустить терминал *Fly* и перейти в каталог */ald\_export\_home* командой *cd /ald\_export\_home*;
    - вывести содержимое текущего каталога командой *ls*, проанализировать результат;
    - определить дискреционные и мандатные атрибуты каталога *userald* командой *pdp-ls -M*;
    - выполнить попытку перехода в каталог *userald* и проанализировать выводимые ошибки;
    - запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*, запустить *Midnight Commander* командой *mc* и перейти в каталог */ald\_export\_home/userald/IOi0c0x0t0x0/Документы*;
    - вывести в терминал содержимое файла *file-from-a/3.txt* командой *cat file-from-a/3.txt*.
  1. Осуществить настройку политики паролей учётных записей пользователей *ALD*. Для этого выполнить следующую последовательность действий:
    - в ОССН *AstraServer* в графической утилите «Политика безопасности» выбрать «Домен *ALD*» (при необходимости выполнить подключение к домену), далее «Политики паролей» – «*default*»;
    - во вкладке «Общие» в поле «Минимальная длина» ввести значение 5;
    - перейти к узлу «Пользователи» – «*userald*» и сменить пароль на «1234», затем на «*Asdf1*».
  1. Создать учётную запись пользователя *ALD* с использованием утилиты *ald-admin*. Для этого выполнить следующую последовательность действий:
    - в ОССН *AstraServer* запустить терминал *Fly*;



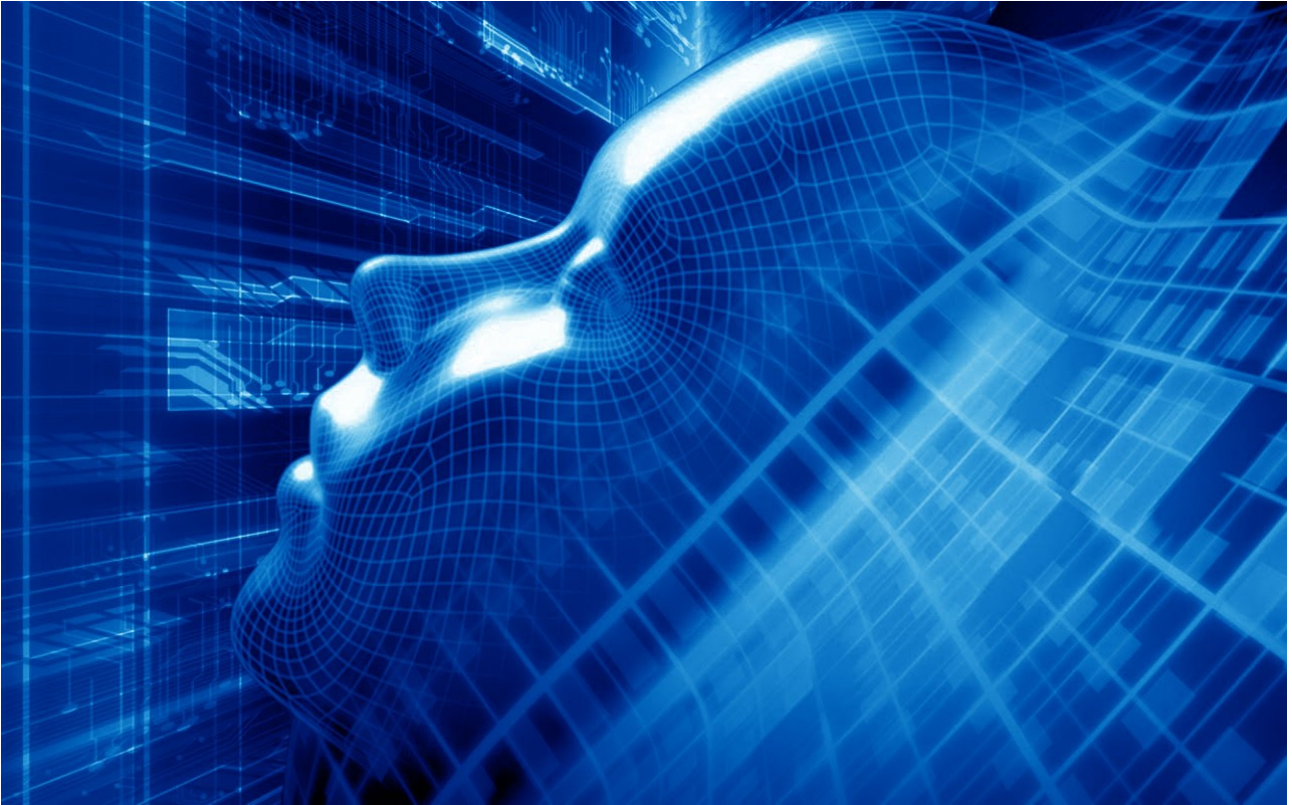
- создать новую учётную запись пользователя *ALD* командой *ald-admin user-add userald2*, задать новый пароль в соответствии с требованиями политики безопасности (не менее 5 символов): «Qwer1»;
  - далее все параметры учётной записи пользователя *ALD*, установленные по умолчанию, за исключением последнего (там значение «yes»);
  - вывести список учётных записей пользователей и компьютеров *ALD* командами *ald-admin user-list* и *ald-admin host-list*, соответственно;
  - создать группу компьютеров *ald\_host\_group1* со следующим составом: *astra-client1.example.ru*, *astra-client2.example.ru*, командой *ald-admin hgroup-add ald\_host\_group1 --host=astra-client1.example.ru --host=astra-client2.example.ru* (также второй узел можно включить в группу командой *ald-admin hgroup-mod ald\_host\_group1 --add-hosts --host=astra-client2.example.ru*);
  - в графической утилите «Политика безопасности» проверить наличие узла «Группы компьютеров/*ald\_host\_group1*»;
  - модифицировать группу компьютеров *ald\_host\_group1*, добавив в неё компьютер *astra-server.example.ru* командой *ald-admin hgroup-mod ald\_host\_group1 --add-hosts --hosts=astra-server.example.ru*;
  - добавить учётной записи пользователя *userald2* привилегию доступа к группе компьютеров *ald\_host\_group1* командой *ald-admin user-ald-cap userald2 --host-group=ald\_host\_group1 --add-hosts*;
  - в графической утилите «Политика безопасности» проверить наличие компьютера *astra-server.example.ru* в узле «Группы компьютеров» – «*ald\_host\_group1*» и наличие привилегии доступа к группе компьютеров *ald\_host\_group1* у учётной записи пользователя *userald2*;
  - проверить возможность входа в ОСН *AstraClient1* и *AstraClient2* с учётной записью пользователя *userald2*, после успешной проверки выйти из ОСН *AstraClient1* и *AstraClient2*.
1. Осуществить проверку целостности и настроек *ALD*, для чего выполнить команду *ald-admin test-integrity* и обратить внимание на выдаваемые предупреждения.
  2. Перейти к администрированию учётной записи пользователей домена:
    - в ОСН *AstraServer* в графической утилите «Политика безопасности» выбрать «Домен *ALD*»;
    - настроить параметры мандатного управления доступом учётной записи пользователя *userald2*: установить в вкладке «МРД» максимальный уровень доступа 3, минимальный — 0;

- настроить параметры мандатного управления доступом учётной записи пользователя *userald*: установить в вкладке «МРД» максимальный уровень доступа 2, минимальный — 0;
  - для проверки войти в ОСН *AstraClient1* в графическом режиме с учётной записью пользователя *userald* (уровень доступа — 2, неиерархические категории — нет, уровень целостности — «Низкий»);
  - выполнить команду *ald-admin test-integrity* и проверить отсутствие предупреждений.
1. Выполнить проверку функционирования единого задания устройств в *ALD*:
    - в ОСН *AstraServer* в графической утилите «Политика безопасности» выбрать «Домен *ALD*»;
    - открыть «Устройства и правила», «Правила», создать новое правило: выбрать импорт свойств, затем выполнить подключение *USB*-носителя, в появившемся дереве выбрать устройство, ввести имя правила «*Rule1*», отметить «Включено» и применить изменения;
    - открыть «Устройства и правила», «Устройства», выполнить добавление *USB*-носителя через импорт свойств, затем установить для него разрешения на чтение и запись для учётной записи пользователя *userald*, группы «*Domain Users*» и всех остальных, установить уровень конфиденциальности — 1, выбрать правило «*Rule1*» и активировать данное устройство, установив флаг «Включено»;
    - войти в ОСН *AstraClient1*, в сессии, функционирующей от имени учётной записи пользователя *userald* на уровнях доступа 0, 1 и 2, выполнить подключение *USB*-носителя, при этом проверить возможность монтирования (в соответствии с «Руководством администратора. Часть 1» монтирование учтённого носителя с файловой системой *VFAT* возможно только при входе в ОСН на том же уровне, с которым данный носитель учтён) и корректность (соответствие МРОСЛ ДП-модели) выполнения операций записи и чтения файлов на *USB*-носитель для каждого уровня доступа.

## Содержание отчёта по выполненной работе

В отчёте о выполненной работе необходимо указать:

1. Полный перечень использованных команд с кратким описанием их назначения.
2. Примеры выполнения команд, которые были использованы в ходе работы с описанием результатов их выполнения.
3. Описание порядка работы с командами *ALD* (*ald-admin*, *ald-init*, *ald-client*) и графической утилитой «Политика безопасности» (*fly-admin-smc*) при осуществлении следующих действий со службой *ALD*:



- настройка адресации сетевого интерфейса;
- настройка контроллера *ALD*;
- настройка клиента *ALD*;
- управление параметрами контроллера *ALD*.

### **Контрольные вопросы**

1. Каково назначение служб контроллера *ALD*?
2. Какие службы устанавливаются на контроллере *ALD*?
3. Какие особенности настройки имён компьютеров, входящих в домен *ALD*?
4. Каковы особенности настройки контроллера *ALD*?
5. Каковы особенности настройки клиента *ALD*?
6. Чем отличаются настройки *ALD* в режиме контроллера и в режиме клиента?
7. Какие основные настройки домена можно выполнять с использованием команды *ald-admin*?

# ЛАБОРАТОРНАЯ РАБОТА №9.

## УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ. НАСТРОЙКА СИСТЕМНЫХ СЛУЖБ.

**Цель работы:** Изучить порядок администрирования пакетов ОССН, в том числе используемых для этого команд и графических утилит, а также особенности настройки системных служб (демонов).

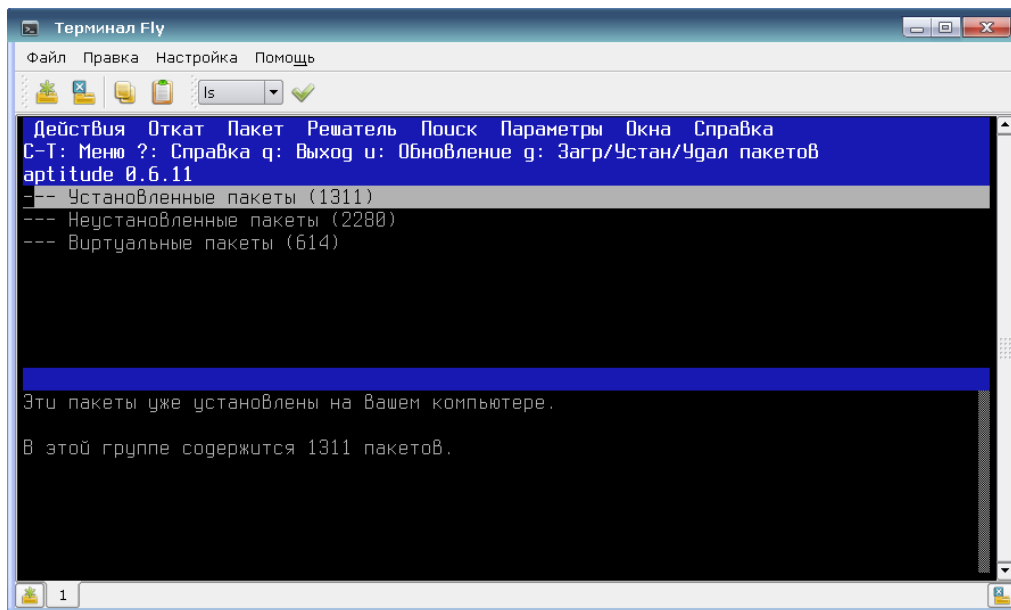
**Время выполнения работы:** 4 академических часа.

### Краткие теоретические сведения

Система управления пакетами ОССН включает несколько команд и утилит, которые могут работать в режиме командной строки, в псевдографическом и графическом режимах. При этом порядок действий при их использовании для изменения состава установленных в ОССН пакетов принципиально не отличается, за исключением, возможно, установки взаимосвязанных пакетов.

Для управления пакетами используются утилиты *aptitude*, «Менеджер пакетов *Synaptic*», команды системы управления пакетами *APT* и команда *dpkg*.

Утилита *aptitude* имеет следующий интерфейс.



Она позволяет осуществлять установку, удаление, поиск по именам (в том числе неустановленных) и управление зависимостями пакетов.

При просмотре пакетов отображается состояние каждого пакета (первый символ в списке): *v* — виртуальный, *B* — неработоспособный, *u* — «распакованный», *C* — недонастроенный, *H* — недоустановленный, *s* — удалённый, но с сохранёнными файлами настроек, *i* — установленный и *E* — внутренняя ошибка. Вторым символом может быть указан флаг автоматизации, означающий, что пакет был установлен как зависимость. Удобство использования данной утилиты также заключается в автоматическом формировании набора пакетов, которые являются зависимыми от удаляемого пакета. Это позволяет предотвратить нежелательное удаление используемых пакетов при настройке других пакетов. После выбора необходимого набора действий их выполнение производится по нажатию «*g*» — загрузка/установка/удаление пакетов. Кроме графического представления утилита *aptitude* может быть использована как консольная команда с параметрами.

Управление пакетами посредством *APT* выполняется командами, основными из которых являются: *apt-get*, *apt-cdrom*, *apt-cache* и *apt-config*.

Команда *apt-cdrom* предназначена для добавления в систему нового источника пакетов (репозитория), как правило диска *CD/DVD*. По умолчанию при установке ОССН один источник уже добавлен — это установочный диск ОССН. Настройки источников пакетов хранятся в файле */etc/apt/sources.list*. Данный файл настроек используется как командами вида *apt\**, так и утилитой *aptitude*. После установки ОССН он содержит единственную запись: *deb cdrom:[Название диска]/ smolensk contrib main non-free*. Первый элемент со значением *deb* указывает на тип источника — *debian package*. При использовании диска с исходными текстами вместо записи *deb* будет стоять *deb-src*. Второй элемент со значением *cdrom* указывает носитель источника — устройство типа *cdrom*. Для установке по сети может

использоваться значение *http*. Далее указана метка диска в квадратных скобках и путь: «/». Затем расположен элемент с указанием названия дистрибутива: *smolensk*. После этого поля указываются наборы установочных пакетов: *contrib*, *main*, *non-free*. Данные названия наборов для источника *cdrom* соответствуют подкаталогам каталога *pool*, расположенного в корне диска. Каждый новый источник заносится новой строкой в данный файл. Для игнорирования строки поддерживаются комментарии (в начале строки указывается символ «#»).

В случае, если файл */etc/apt/sources.list* редактируется вручную, то для обновления списка пакетов необходимо выполнить команду *apt-get update*. Данная команда по списку активных источников, полученных из этого файла, считывает соответствующие наборы пакетов, которые далее используются для выбора устанавливаемых пакетов при выполнении команды *apt-get install* имя\_пакета.

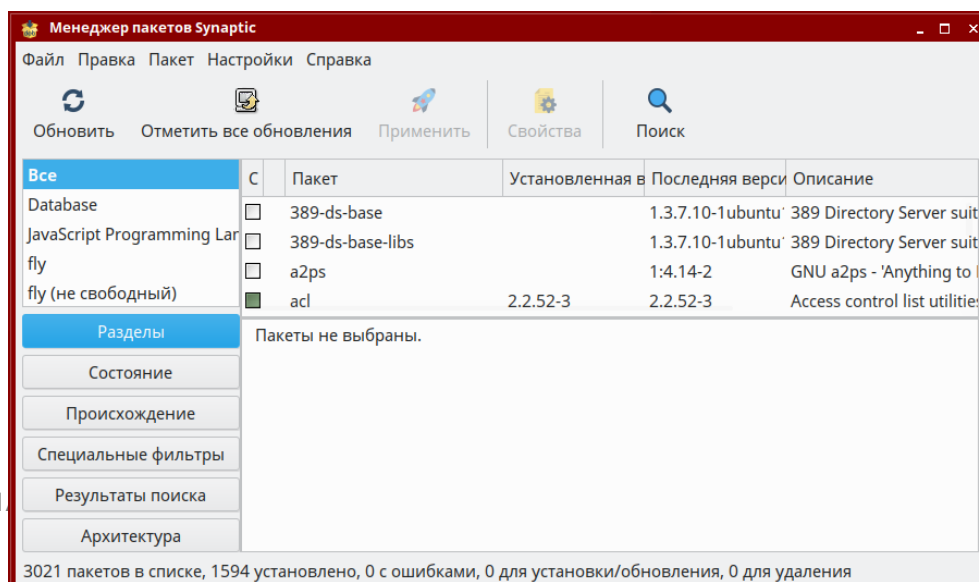
Для непосредственного управления пакетами используются команды *apt-get install* имя\_пакета (установка), *apt-get remove* имя\_пакета (удаление).

Команда *apt-cache* применяется для работы с кэшем пакетов. Она позволяет вывести список пакетов – *apt-cache pkgnames*, зависимости отдельного пакета – *apt-cache depends* имя\_пакета, найти пакет в кэше по его имени – *apt-cache search*.

Команда *dpkg* реализует следующие основные действия:

- *dpkg -i* имя\_файла\_deb\_пакета — установка пакета, находящегося в файле имя\_файл\_deb\_пакета (данный файл имеет расширение *deb*);
- *dpkg -r* имя\_пакета — удаление пакета;
- *dpkg -L* имя\_пакета — вывод файлов, содержащихся в пакете;
- *dpkg -S* имя\_файла — поиск принадлежности заданного файла конкретному пакету.

Управление пакетами с использованием графического интерфейса осуществляется графической утилитой «Менеджер пакетов *Synaptic*» (*synaptic*), имеющей следующий интерфейс.



Она позволяет осуществлять фильтрацию пакетов по состоянию, устанавливать зависимости, устанавливать, переустанавливать, удалять и полностью удалять пакеты. В свойствах пакетов, отображаемых утилитой, содержится информация о файлах, которые были установлены этим пакетом с их расположением в ОССН, зависимости пакетов и доступные версии пакетов.

Для настройки системных служб в ОССН используются команды *service* (устаревшая) и *systemctl*, а также графическая утилита *systemdgenie* (запуск с использованием графического меню осуществляется в меню «Система», «Инициализация системы»). В ОССН версии 1.6 используется новый менеджер загрузки *Systemd*. С этим связаны значительные изменения порядка управления и создания сервисов.

Для управления запуском системных служб как и ранее может использоваться команда *service* имя\_службы <команда>. В качестве параметров команды используются *start*, *stop*, *restart*, *status* для запуска, останова, перезапуска или определения статуса системной службы, соответственно. С использованием утилиты *systemctl* запуск сервиса (в данном случае — юнита) выполняется командой *systemctl start* имя\_юнита (аналогичные команды используются для останова — *stop*, перезапуска — *restart*). Просмотр уровней запуска системных служб может быть осуществлён с использованием команд *service --status-all* или более наглядной *systemctl --all list-units*. Аналогичные функции реализует графическая утилита *systemdgenie*.

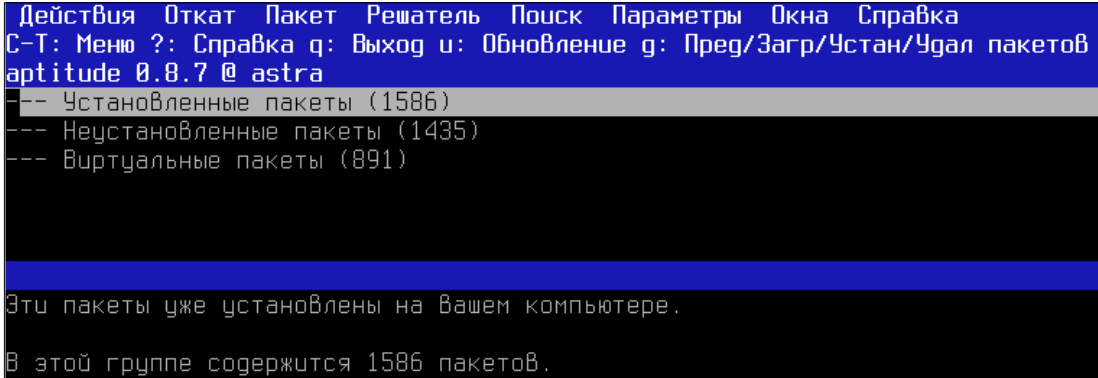
## **Используемое методическое и лабораторное обеспечение**

1. ОССН версии 1.6, в которой создана учётная запись пользователя *user*, 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*).
2. Дистрибутив ОССН.
3. Документация: «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1», «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя».

4. Для выполнения работы в течение двух занятий необходимо обеспечить возможность сохранения состояния ОССН за счёт применения технологий виртуализации (создания виртуальных машин с ОССН).

### Порядок выполнения работы

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 терминал *Fly* и перейти в каталог */etc/apt*.
3. Вывести дискреционные права доступа к файлу *sources.list* командой *ls -l sources.list*. Определить возможность изменения файла при работе от имени данной учётной записи пользователя.
4. Выполнить команду *sudo fly-term* и перейти в каталог */etc/apt*.
5. Запустить *Midnight Commander* командой *mc*. Открыть для редактирования файл *sources.list* и закомментировать строку *deb cdrom...* путём установки символа *#* в начале строки.
6. Выполнить команду *apt-get update*, и с использованием дистрибутива ОССН добавить источник пакетов *cdrom* командой *apt-cdrom add*.
7. Установить пакет *vim-gtk* командой *apt-get install vim-gtk*. Проверить возможность работы в редакторе *vim-gtk*, выполнив команду *vim.gtk 1.txt*. Выйти из редактора, набрав «:wq». Проверить наличие файла *1.txt* и удалить его командой *rm 1.txt*.
8. Запустить второй терминал *Fly* командой *sudo fly-term* и в нём выполнить команду *aptitude*.



```

Действия Откат Пакет Решатель Поиск Параметры Окна Справка
C-T: Меню ?: Справка q: Выход u: Обновление g: Прег/Загр/Устан/Удал пакетов
aptitude 0.8.7 @ astra
-- Установленные пакеты (1586)
--- Неустановленные пакеты (1435)
--- Виртуальные пакеты (891)

Эти пакеты уже установлены на Вашем компьютере.
В этой группе содержится 1586 пакетов.

```

9. В первом терминале выполнить попытку удаления пакета *vim-gtk* командой *apt-get remove vim-gtk*, проанализировать выводимые ошибки.



```

root@astra:/# apt-get remove vim-gtk
E: Не удалось получить доступ к файлу блокировки /var/lib/dpkg/lock
- open (11: Ресурс временно недоступен)
E: Не удалось выполнить блокировку управляющего каталога (/var/lib/dpkg/); он уже используется другим процессом?
root@astra:/# apt-get remove vim-gtk
E: Не удалось получить доступ к файлу блокировки /var/lib/dpkg/lock
- open (11: Ресурс временно недоступен)
E: Не удалось выполнить блокировку управляющего каталога (/var/lib/dpkg/); он уже используется другим процессом?

```

10. Завершить *aptitude* во втором терминале. В первом терминале повторить удаление пакета *vim-gtk* командой *apt-get remove vim-gtk* и *apt-get remove vim-gui-common*. Проанализировать отображаемые в терминале сообщения и определить количество удалённых пакетов.
11. Выполнить настройку пакетов с использованием *APT*, для этого осуществить следующую последовательность действий:
  - найти пакеты, содержащие модули для Web-сервера *Apache2*, командой *apt-cache search libapache2-mod-\**, и определить их назначение по описанию;
  - выполнить установку пакета *texstudio* командой *apt-get install texstudio*;
  - выполнить очистку локального хранилища файлов пакетов за исключением */var/cache/apt/archives/* и */var/cache/apt/archives/partial/* командой *apt-get clean*;
  - выполнить очистку локального хранилища командой *apt-get autoclean*;
  - удалить пакет *texstudio* с удалением конфигурационных файлов командой *apt-get purge libquazip5-1*;
  - выполнить повторную установку пакета *texstudio* командой *apt-get install texstudio* и определить количество установленных пакетов;
  - проверить назначение и зависимости пакета *texstudio* командами *apt-cache show texstudio* и *apt-cache showpkg texstudio*;
  - выполнить удаление пакета *texstudio* с сохранением конфигурационных файлов командой *apt-get remove texstudio* и проанализировать количество удаляемых пакетов и отсутствие сообщения об очистке файлов настроек;
  - проверить наличие ошибок в зависимостях пакетов командой *apt-get -f install*;
  - выполнить удаление лишних пакетов, которые были установлены автоматически, но теперь не требуются командой *apt-get autoremove*.
1. В первом терминале выполнить команду *aptitude* и открыть раздел «Неустановленные пакеты» — «*Editors*» — «*main*».
2. Для работы с пакетом *vim-gtk* осуществить следующие действия:
  - выполнить просмотр следующих свойств пакета *vim-gtk*: описание назначения, размер в сжатом и распакованном виде, версии и зависимости;

```
--\ vim-gtk                                     <отсутствует> 2:8.0.019
Описание: Vi IMproved - enhanced vi editor - with GTK2 GUI
Vim is an almost compatible version of the UNIX editor Vi.

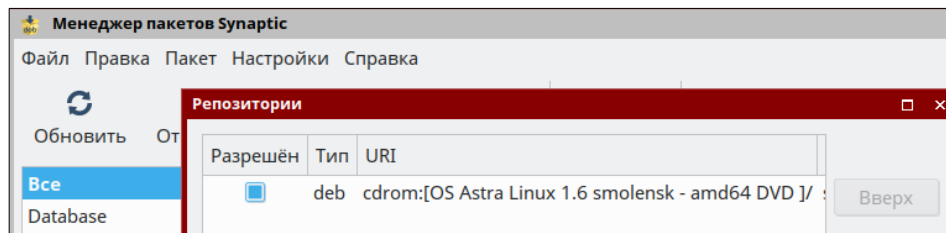
Many new features have been added: multi level undo, syntax highlighting, command
history, on-line help, filename completion, block operations, folding, Unicode sup
etc.

This package contains a version of vim compiled with a GTK2 GUI and support for
scripting with Lua, Perl, Python, Ruby, and Tcl.
Домашняя страница: http://www.vim.org/
Приоритет: дополнительный
Раздел: editors
Сопровождающий: Debian Vim Maintainers <pkg-vim-maintainers@lists.alioth.debian.org>
Архитектура: amd64
Размер в сжатом виде: 1 263 k
Размер в распакованном виде: 3 040 k
Пакет с исходным кодом: vim
Происхождение: 1.6/stable [amd64]
URI происхождения: cdrom:[OS Astra Linux 1.6 smolensk - amd64 DVD ]/pool/main/v/vim/
Vi IMproved - enhanced vi editor - with GTK2 GUI
```

- в третьей строке в псевдографическом интерфейсе перейти к вкладке «Пакет» и выбрать данный пакет для установки нажатием клавиши «+», обратив внимание, что одновременно с его установкой были добавлены его зависимости: пакет *vim-gui-common*;
  - определить статус установки пакетов: *vim-gtk* — *pi* (пакет помечен для установки), *vim-gui-common* — *piA* (пакет помечен для установки и выбран автоматически в качестве зависимого);
  - выполнить установку и получить следующие данные: перечень устанавливаемых пакетов (1 пакет — *vim-gtk*), пакеты, которые устанавливаются автоматически, список пакетов, предлагаемых другими пакетами (первые две группы пакетов устанавливаются полностью, а последняя может быть дополнительно выбрана при установке).
1. С использованием утилиты *aptitude* выполнить следующие действия:
    - в разделе «Установленные пакеты» выбрать пакет *vim-gtk* и проверить статус автоматической установки («A») пакета *vim-gui-common*;
    - выполнить попытку удаления («-») пакета *vim-gui-common* и проанализировать выведенные предупреждения;
    - нажать клавишу «e» для того, чтобы определить какие дополнительные действия необходимо будет выполнить совместно с удалением пакета *vim-gui-common*, затем нажать клавишу «TAB» для выбора «Удалить *vim-gtk*», далее нажать «.» для выбора решения удалить «Действия: 1 оставить неизменным», затем «!» и «g» для применения предложенных действий;
    - проверить, какие пакеты были дополнительно помечены для удаления, и удаляются ли при этом пакет *vim-gtk*;

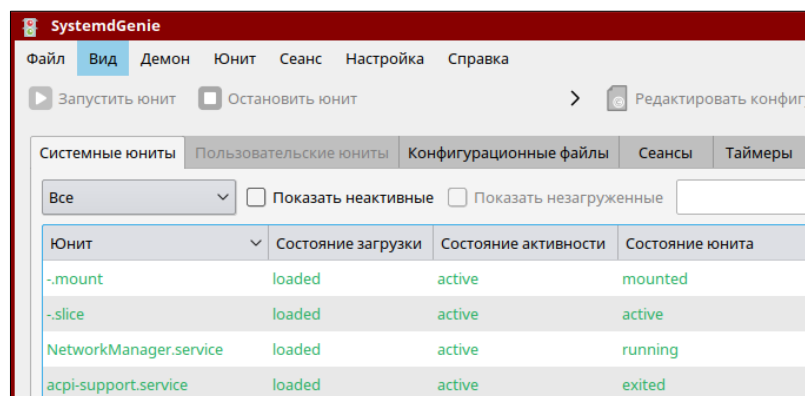
- выделить для удаления пакет *nano* и в строке статуса (третья строка) определить размер освобождаемого места на диске.
1. Выполнить попытку удаления пакета *vim-gui-common*, при этом осуществить следующие действия:
    - отметить для удаления пакет *vim-gui-common* выбором пункта меню «Пакет/Удалить» и проверить выделение для удаления зависимых пакетов;
    - отменить данные действия выбором пункта меню «Действия/Отменить незаконченные действия» и выйти из утилиты *aptitude*.
  1. Выполнить удаление пакета *vim-gui-common* командой *apt-get remove vim-gui-common*, проверить список удаляемых пакетов.
  2. Выполнить удаление пакета *nano* командой *apt-get remove nano* и проверить список удаляемых пакетов.
  3. Выполнить установку пакетов с использованием команды *dpkg*, при этом осуществить следующие действия:
    - в «привилегированном» режиме терминала *Fly* перейти в каталог */media/cdrom/pool/main/n* подключённого DVD с дистрибутивом ОССН;
    - для установки пакета *nano* найти соответствующий каталог командой *ls | grep "^nano"* и перейти в него;
    - установить пакет *nano* командой *dpkg -i имя\_файла\_пакета*, затем проверить работу редактора *nano*;
    - выполнить переход в каталог *pool/main*;
    - перейти в каталог *v/vim* и осуществить попытку установки пакета *vim-gtk* командой *dpkg --install имя\_файла\_пакета* и проанализировать результат (пакет *vim-gtk* будет не настроен).
  1. Выполнить проверку статуса установленных пакетов, для чего осуществить следующие действия:
    - в «привилегированном» режиме терминала *Fly* запустить утилиту *aptitude* и проанализировать предупреждения;
    - нажать клавишу «е» для просмотра решений: первое решение — это установка пакета *vim-gui-common*;
    - выполнить просмотр следующего решения и выйти из утилиты *aptitude*.
  1. Вернуться в терминал *Fly* и выполнить следующую последовательность действий:
    - установить недостающий пакет (*vim-gui-common*) командой *dpkg --install имя\_файла\_пакета*;
    - запустить утилиту *aptitude* и проанализировать причину отсутствия ошибочных зависимостей и требований установки дополнительных пакетов;

- вернуться к вкладке «Пакеты» и перейти «Установленные пакеты» — «*editors*» — «*main*», далее выделить в списке пакет *vim-gtk* и определить его статус;
  - выйти из утилиты *aptitude* и в терминале *Fly* выполнить конфигурацию *vim-gtk* командой *dpkg --configure vim-gtk* и проверку возможности запуска командой *vim.gtk*;
  - проверить в приложении *aptitude*, что статус пакета *vim-gtk* изменился на «*i*» (т. е. пакет был сконфигурирован и теперь успешно установлен).
1. Вывести в терминал *Fly* информацию об установленном пакете *vim*, для чего осуществить следующие действия:
    - вывести в терминал содержимое пакета *vim-gtk* командой *dpkg -L vim-gtk*;
    - вывести в терминал содержимое пакета *vim-gtk* командой *aptitude show vim-gtk*;
    - вывести в терминал список пакетов, имя которых начинается с *vim*, командой *aptitude search "^vim"* и определить статусы их установки;
    - вывести в терминал список пакетов, имя которых содержит *gtk*, командой *aptitude search "gtk"*;
    - определить принадлежность файла */usr/share/llintian/overrides/vim-gtk* пакету *vim*, для чего выполнить команду *dpkg -S /usr/share/llintian/overrides/vim-gtk*;
    - вывести в терминал список пакетов, содержащих файлы, полный путь с именем которых заканчивается на «*/vim*» командой *dpkg -S "\*/vim"*.
  1. Выполнить настройку пакетов в графической утилите *Synaptic*, для чего осуществить следующие действия:
    - запустить графическую утилиту *Synaptic*, при этом ввести пароль текущей учётной записи пользователя для возможности работы в «привилегированном» режиме;
    - открыть меню «Настройки», «Репозитории» и проверить наличие неактивного репозитория, который был ранее закомментирован в файле *sources.list*;
    - скопировать *URI* для неактивного репозитория;
    - удалить неактивный и активный репозитории.
  1. В графической утилите *Synaptic* через меню «Настройки», «Репозитории» выбрать действие «Создать», при этом:
    - в элемент *URI* ввести запись *cdrom:[OS Astra Linux 1.6 smolensk - amd64 DVD ]/*;
    - в элемент «Дистрибутив» — *smolensk*;
    - в элемент «Разделы» — *contrib main non-free*;
    - закончить изменения и выполнить обновление для повторного считывания источника пакетов.



1. В графической утилите *Synaptic* выполнить следующую последовательность действий:
  - в элемент «Быстрый фильтр» ввести «*vim*» и отметить пакет *vim-common* для полного удаления с использованием контекстного меню, после удаления проанализировать предупреждения ОССН;
  - выбрать в списке фильтров «Ошибки зависимостей» и отметить пакет *vim* для полного удаления, и после удаления проанализировать список полностью удаляемых пакетов, их число и суммарный объем дискового пространства;
  - в «привилегированном» режиме терминала *Fly* выполнить попытку удаления пакета *nano* командой `apt-get remove nano` и проанализировать предупреждения ОССН;
  - завершить работу с графической утилитой *Synaptic*, выполнить удаление пакета *nano* командой `apt-get remove nano`.
1. Для управления системными службами выполнить следующую последовательность действий:
  - в «привилегированном» режиме терминала *Fly* получить текущие статусы запускаемых системных служб командой `service --status-all`;
  - выполнить попытку определения статуса системной службы *avahi-daemon* командой `service avahi-daemon status` и проанализировать результат;
  - для анализа порядка вызова команды `service` вывести на экран содержимое файла *avahi-daemon* командой `cat /etc/ini.d/avahi-daemon`;
  - аналогично по содержимому файла *avahi-daemon* найти реализацию вызова команды `status`;
  - вывести в терминал содержимое файла *avahi-daemon* командой `cat /etc/ini.d/avahi-daemon` и проанализировать его структуру, при этом найти особенности реализации вызова команды `status`.
1. Для управления запуском системных служб в «привилегированном» режиме терминала *Fly* осуществить следующие действия (при этом проверяется обратная совместимость со службой инициализации):
  - определить статус загрузки системной службы *ssh* командой `service --status-all | grep ssh` и командой `ls /etc/rc2.d | grep ssh`;

- установить запуск службы сервера *ssh* на уровнях по умолчанию командой *update-rc.d ssh enable*;
  - определить изменения в статусе системной службы *ssh* командой *service --status-all | grep ssh* и командой *ls /etc/rc2.d | grep ssh*;
  - выполнить остановку, запуск и перезапуск системной службы *ssh* командами *service ssh stop*, *service ssh start*, *service ssh restart*.
1. Осуществить запуск системных служб из графической утилиты «Инициализация системы» (*systemdgenie*), осуществив следующие действия:
- в «привилегированном» режиме терминала *Fly* запустить графическую утилиту «Инициализация системы» командой *systemdgenie &*;



- запретить запуск системной службы *ssh*, для этого выделить юнит *ssh.service*, в контекстном меню выбрать «Отключить юнит»;
- выполнить перезагрузку и повторный вход в ОССН;
- проверить настройку службы *ssh* командой *service --status-all* и с использованием графической утилиты «Инициализация системы» (при этом юнит *ssh.service* должен отсутствовать);
- повторно активировать службу *ssh* с использованием *update-rc.d*, выполнить перезагрузку;
- запустить графическую утилиту «Инициализация системы» в столбце «Юнит» выделить *ssh*, в контекстном меню выбрать «Редактировать файл юнита» и определить зависимость запуска данной службы от других служб в открывшемся окне (раздел [Unit] параметр After);
- вывести в терминале *Fly* содержимое начала файла */etc/init.d/ssh* командой *head /etc/init.d/ssh* и сравнить запись *Required-Start* с содержимым окна *ssh* в графической утилите «Инициализация системы»;
- активировать службу *ntp* с использованием *update-rc.d*, выполнить перезагрузку;

```
root@astra:/home/user# update-rc.d ntp enable
```

- в графической утилите «Инициализация системы» в столбце «Юнит» найти службу *ntp*, затем в контекстном меню выбрать «Маскировать юнит»;

Системные юниты			
Пользовательские юниты			
Конфигурационные файлы			
Сеансы			
Таймеры			
Все			
<input type="checkbox"/> Показать неактивные <input type="checkbox"/> Показать незагруженные			
Юнит	Состояние загрузки	Состояние активности	Состояние юнита
network.target	loaded	active	active
networking.service	loaded	active	exited
ntp.service	loaded	active	running

- проверить статус системной службы *ntp* командой *systemctl list-units* (для этого выполнить поиск «*ntp*» с использованием комбинации клавиш «/» и «*ntp*»), что системная служба замаскирована, выполнить перезагрузку и проверить статус загрузки службы.

## Содержание отчёта по выполненной работе

В отчёте о выполненной работе необходимо указать:

1. Полный перечень использованных команд с кратким описанием их назначения.
2. Примеры выполнения команд, которые были использованы в ходе работы с описанием результатов их выполнения.
3. Описание порядка работы при осуществлении следующих действий:
  - удаление пакета без зависимостей;
  - удаление пакета с зависимостями;
  - установка новых пакетов;
  - создание новых репозитория;
  - редактирование действующих репозитория и обновление информации о пакетах.
1. Описание порядка работы при установке и удалении пакетов с использованием утилит *aptitude*, «Менеджер пакетов *Synaptic*», команд *APT* и команды *dpkg*.
2. Описание особенностей функционирования команды *dpkg* при установке пакетов с зависимостями.
3. Описание порядка работы с командами и графической утилитой «Инициализация системы» (*systemdgenie*) при осуществлении следующих действий с системными службами:
  - просмотр статуса;

- просмотр настроек запуска системных служб;
- управление (запуск, перезапуск, останов, просмотр состояния).

### **Контрольные вопросы**

1. Каковы особенности одновременной работы нескольких утилит управления пакетами?
2. Где и в каком формате хранятся настройки репозитория?
3. Каким образом добавляются новые источники пакетов и осуществляется их повторное считывание?
4. Какие команды позволяют работать с зависимыми пакетами в автоматическом режиме?
5. Какие особенности выполнения команд удаления пакетов?
6. Как определить статус установленного пакета с использованием команды *dpkg* и утилиты *aptitude*?
7. Как определить статус запуска системной службы?
8. Каким образом можно произвести останов, запуск, перезапуск системной службы?
9. Какие команды используются для просмотра состояния и уровней запуска системной службы?



# ЛАБОРАТОРНАЯ РАБОТА №10.

## НАСТРОЙКА ЗАЩИЩЕННОГО РЕЖИМА РАБОТЫ ОССН В СООТВЕТСТВИИ С ASTRA LINUX RED-BOOK.

**Цель работы:** Изучить особенности настройки безопасной конфигурации компьютера для работы с ОССН в соответствии с *Astra Linux Red-Book*.

**Время выполнения работы:** 6 академических часов.

### Краткие теоретические сведения

Выполнение лабораторной работы основывается на описании настройки безопасной конфигурации компьютера для работы с ОССН *Astra Linux Special Edition* с использованием материалов справочного центра *Astra Linux Red-Book*.

Совокупность данных настроек позволяет достичь режима работы ОССН, когда все её механизмы защиты будут активированы и полнофункциональны.

Настройки включают конфигурирование ОССН по следующим направлениям:

- доверенная загрузка ОССН;
- конфигурирование оборудования компьютера с ОССН;
- защитное преобразование данных на жёстком диске;
- полнофункциональный режим работы мандатного контроля целостности;
- контроль цифровой подписи *ELF*-файлов;
- отключение терминалов для непривилегированных учётных записей пользователей;
- блокировка командных интерпретаторов и макросов для непривилегированных учётных записей пользователей;
- блокировка установки бита исполнения;
- блокировка трассировки исполнения программ;
- использование межсетевого экрана;
- работа в режиме киоска.

Детали работы ОССН по большинству перечисленных направлений подробно рассмотрены в главах 1 и 3. Дополнительно справочные материалы по настройке защищён-

| СПЕЦИАЛЬНЫЙ КУРС ALSE-1605 | ВЕРСИЯ 2 (16.06.2020)

ного режима работы ОССН также приведены в документации «Руководство по КСЗ. Часть 1».

### **Используемое методическое и лабораторное обеспечение**

1. Подготовленный компьютер для установки ОССН *Astra Linux Linux Special* версии 1.6, отвечающий требованиям к оборудованию для использования ОССН (при разбиении диска требуется жёсткий диск объёмом от 20 Гб).
2. Дистрибутив ОССН.
3. Документация: «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство администратора. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство по КСЗ. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство пользователя».
4. Для выполнения всей лабораторной работы необходимо использовать отдельный компьютер, а не виртуальные машины.

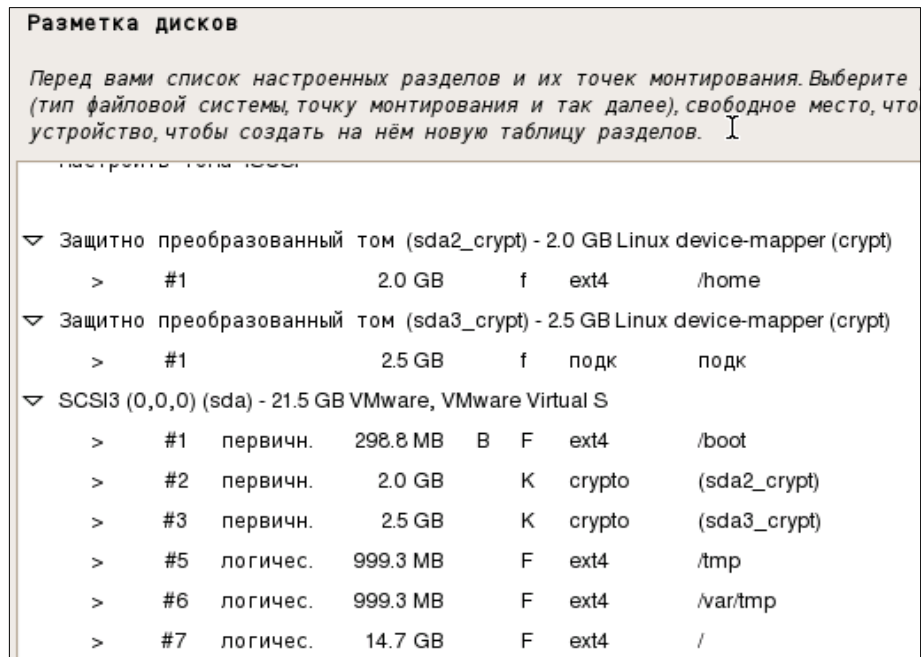
### **Порядок выполнения работы**

1. Для обеспечения доверенной загрузки ОССН выполнить установку и настройку (при наличии) аппаратно-программного модуля доверенной загрузки (АПМДЗ).
2. Выполнить предварительную конфигурацию оборудования компьютера:
  - настроить *BIOS*: установить пароль блокировки входа в *BIOS* (при задании пароля руководствоваться требованиями к генерации паролей, аналогичные требованиям к сложности паролей учётных записей пользователей ОССН);
  - при наличии в *BIOS* опций блокировки установки битов исполнения (для процессоров *Intel Execute Disable Bit* и для процессоров *AMD No Execute Bit*) включить их;
  - при наличии на серверах «недоверенных» систем контроля и управления вида *ILO*, *RSA*, *iDRAC*, *ThinkServer EasyManage*, *AMT*, *iMana* необходимо выполнить их отключение, и использовать, при необходимости, альтернативные решения вида *IP KVM*;
  - для *Intel* платформ необходимо устранить уязвимость *Intel-SA-00086* в *Intel Management Engine* (если он интегрирован в процессор) посредством установки обновления микропрограммы *Intel Management Engine* (производитель оборудования должен обеспечить данную возможность: для этого могут использоваться либо обновления *BIOS*, либо дополнительное ПО для интеграции обновлений); для проверки можно использовать утилиту *Intel-SA-00086 Detection Tool*.
1. Перейти к установке ОССН, используя для этого первый установочный диск. Далее необходимо выполнить установку ОССН с включённым защитным преобразованием

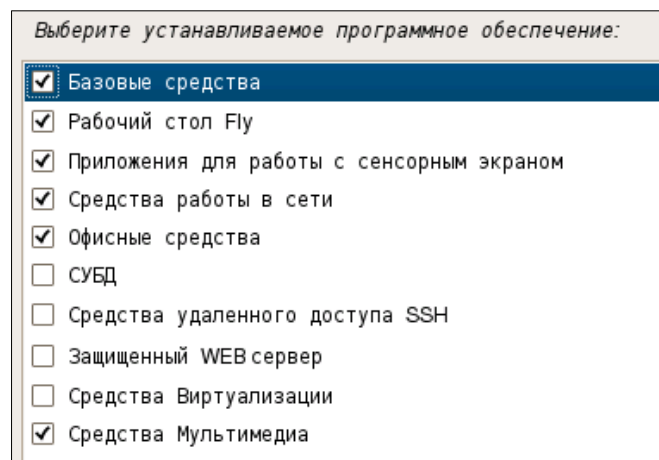
диска (для упрощения процесса установки может также быть использован режим «Авто — использовать весь диск с защитным преобразованием *LVM*», т.к. данный режим содержит отключаемую стадию перезаписывания диска случайными данными перед установкой ОССН, стадию формирования ключевой фразы преобразования — длина от 20 символов, которая будет использоваться для защиты разделов с использованием *dm-crypt*) и обеспечить невозможность физического доступа к жёсткому диску, на котором установлена ОССН. В рамках работы используется метод разметки «Вручную». Для выполнения всех вышеперечисленных операций необходимо выполнить:

- осуществить загрузку с основного (установочного) диска ОССН;
- выбрать язык «Русский», затем «Графическая установка»;
- принять лицензионное соглашение, установить способ переключения языка, задать имя компьютера «astra», имя учётной записи администратора «user», задать и подтвердить пароль администратора (который удовлетворяет требованиям сложности), выбрать часовой пояс;
- выбрать метод разметки «Вручную» и удалить все имеющиеся разделы;
- в «свободном месте» выполнить создание нового раздела размером 300Мб («Первичный»), задать для него файловую систему *Ext4* и точку монтирования */boot*, включить метку «загрузочный» и закончить изменения раздела;
- в «свободном месте» выполнить создание нового раздела размером 2Гб («Первичный», позже он будет использоваться для каталога */home*), задать точку монтирования «отсутствует», закончить изменение раздела;
- выполнить создание нового раздела размером 2,5Гб («Первичный», он будет использоваться для подкачки), указать использовать как «раздел подкачки»;
- аналогично создать два логических раздела объёмом по 1Гб (при выборе размера разделов следует помнить, что при размере раздела */tmp* менее 250Мб вероятно возникновение ошибок при работе с графикой или с большими объёмами данных), задать для них файловую систему: *Ext4* и точки монтирования */tmp* и */var/tmp* (вводится вручную);
- в свободном месте создать раздел «/» («Логический») и задать для него файловую систему *Ext4*;
- выбрать «Настроить защитное преобразование для томов», сохранить сделанные изменения разделов;
- затем «Создать защитное преобразованные тома» и выбрать разделы, доступ к которым будет задаваться паролем: второй раздел с каталогом */home* (выбрать «Ключ защитного преобразования» — «Ключевая фраза»), третий раздел с подкачкой (выбрать «Ключ защитного преобразования» — «Произвольный ключ»);

- закончить создание разделов;
- выполнить стирание разделов;
- задать «ключевую фразу для защитного преобразования» второго раздела (проверить, что запрос выдаётся именно для этого раздела) в соответствии с требованиями к сложности паролей;
- задать тип использования и точки монтирования, созданные с применением защитного преобразования томов: *sda2\_crypt* — */home*, *sda3\_crypt* — подкачка;



- по окончании выбрать «Закончить разметку и записать изменения на диск»;
- выбрать необходимые для работы наборы пакетов, *ALD* не устанавливать, дополнительные параметры настройки ОССН не устанавливать, установить *GRUB* в главную загрузочную запись;



- установить пароль блокировки входа в настройке *GRUB* (при задании пароля руководствоваться требованиями к генерации паролей).
1. Для дальнейшей настройки параметров ОССН выполнять вход от имени учётной записи администратора *user* на уровне целостности «Высокий».
  2. Установить все доступные обновления безопасности ОССН с сайта <http://astralinux.ru/update.html> (при наличии доступа к сети Интернет).
  3. Настроить загрузчик на ядро *Hardened*, и убрать из меню все другие варианты загрузки, включая режимы восстановления:
    - запустить графическую утилиту «Панель управления», «Система», «Загрузчик *GRUB2*» в вкладке «Основное», «Время ожидания», установить требование автоматической загрузки пункта меню «*Hardened*» (без режима восстановления): «Немедленно»;
    - отключить поиск дополнительных ОС (включен опцией «Проверка наличия операционных систем») и генерацию *recovery-mode* (включена опцией «Сгенерировать записи для восстановления системы»), при этом произойдёт переформирование файла */boot/grub/grub.cfg*;
    - нажать «Применить» и далее для выполнения настроек выполнить редактирование файла */boot/grub/grub.cfg*, для этого запустить терминал *Fly* в «привилегированном» режиме;
    - выполнить создание резервной копии файла */boot/grub/grub.cfg*;
    - выполнить редактирование файла */boot/grub/grub.cfg*, исключив из него опцию загрузки (последний параметр *menuentry*, начиная со строки «*menuentry ... generic ... {*», до символа «*}}*») ядра *Generic* (тем самым будут удалены лишние варианты загрузки ОССН).
  1. Выполнить перезагрузку и дополнительную настройку *BIOS*:
    - при использовании архитектур, отличных от *Intel*, установить пароль на загрузчик согласно документации;
    - установить единственным устройством для загрузки ОССН — жёсткий диск, на который была произведена установка ОССН;
    - при поддержке компьютером соответствующих технологий включить режим загрузки *secureboot* с использованием ключей учётной записи пользователя компьютера (создать *USB*-носитель с помощью *astra-secureboot*, и далее импортировать ключи в *BIOS* в соответствии с инструкциями <https://wiki.astralinux.ru/pages/viewpage.action?pageId=20217938>).
  1. Проверить параметры монтирования разделов в файле */etc/fstab*:

- раздел */boot* рекомендуется монтировать с опциями *ro* (перед обновлением ядра смонтировать в *rw*), для этого параметр монтирования указанного каталога в файле */etc/fstab* изменить с *defaults* на *ro*;
- разделы */home*, */tmp*, */var/tmp* рекомендуется монтировать с опциями *noexec,nodev,nosuid*, для чего параметры монтирования указанных каталогов в файле */etc/fstab* изменить с *defaults* на *rw,noexec,nodev,nosuid*.

1. Включить блокировку интерпретаторов:

- при использовании графического интерфейса запустить утилиту *fly-admin-smc*, открыть «Монитор безопасности» и выбрать пункт 5 «Блокировка интерпретаторов», нажать «Настроить блокировку интерпретаторов» и далее выбрать «Включить блокировку интерпретаторов»;
- при настройке из терминала *Fly* необходимо в «привилегированном» режиме выполнить команду просмотра текущих настроек командой *systemctl is-enabled astra-interpreters-lock* (если блокировка не настраивалась, то выводится предупреждения об ее отсутствии *astra-interpreters-lock.service*); для включения выполнить команду *astra-interpreters-lock enable* (отключение производится запуском данной команды с параметром *disable*); после настройки для проверки повторить команду *systemctl is-enabled astra-interpreters-lock*.

```
root@astra:/home/user# systemctl is-enabled astra-interpreters-lock
enabled
```

1. Выполнить настройку блокировки консоли (блокировка настраивается автоматически при установке ОССН):

- запустить графическую утилиту «Политика безопасности» (раздел «Настройки безопасности / Политика консоли и интерпретаторов»);
- включить блокировку консоли.

1. Включить блокировку установки бита исполнения:

- для блокировки только до перезагрузки ОССН выполнить команду *echo 1 > /parsecfs/nochmodx*;
- для полной блокировки во всех сессиях ОССН выполнить команду *echo 1 > /etc/parsec/nochmodx* (настройка действует только после перезагрузки ОССН) или *astra-nochmodx-lock enable* (блокировка действует сразу, в том числе в текущей сессии ОССН);
- данные настройки доступны в графической утилите «Политика безопасности» (раздел «Настройки безопасности / Системные параметры»).

1. Включить блокировку макросов:

- данная настройка («Макросы / Блокировка макросов») доступна в графической утилите «Политика безопасности» (раздел «Настройки безопасности / Системные параметры») и с помощью утилиты *astra-macros-lock*;
- в офисном пакете *LibreOffice* выбрать меню «Сервис», «Параметры», далее «*LibreOffice*», «Безопасность», «Безопасность макросов» и выбрать параметр «Очень высокий».

1. Включить блокировку трассировки *ptrace*:

- в терминале *Fly* в «привилегированном» режиме выполнить команду просмотра текущих настроек *systemctl is-enabled astra-pttrace-lock* (если блокировка не настраивалась, то выводится предупреждение об отсутствии *astra-pttrace-lock.service*);
- для включения выполнить команду *astra-pttrace-lock enable* (отключение производится запуском данной команды с параметром *disable*);
- после настройки для проверки повторить команду *systemctl is-enabled astra-pttrace-lock*.

```
root@astra:/home/user# systemctl is-enabled astra-pttrace-lock
enabled
```

1. Включить контроль цифровой подписи *ELF*-файлов (исполняемых файлов):

- установить в файле */etc/digsig/digsig\_initramfs.conf* значение параметра *DIGSIG\_ELF\_MODE=1*;
- выполнить перемонтирование каталога */boot* с доступом на чтение и запись командой *mount -o remount,rw /boot*;
- выполнить команду *update-initramfs -u -k all* и перезагрузить ОС.

1. Включить гарантированное удаление файлов и папок:

- в файле */etc/fstab* добавить параметр *secdel=x* (где *x* определяет количество стираний фиксированными последовательностями вида «11111111», «01010101», «10101010», «00000000») или *secdelrnd* (стирание псевдослучайной последовательностью) к параметрам монтирования разделов (например для каталога */home*).

1. Включить межсетевой экран *ufw* (графическая утилита *gufw*):

- в меню «Панель управления», «Прочее», «Настройка межсетевого экрана» выбрать необходимый профиль и изменить статус на «Включено»;
- при необходимости задания уровня журналирования выбрать его в меню «Правка», «Параметры»;
- настроить межсетевой экран (модуль ядра *NetFilter* с использованием консольной команды *iptables*) в минимально необходимой конфигурации (т.е. настроить режим,

когда по умолчанию все запрещено, кроме необходимых исключений, для чего могут также использоваться команды *iptables*, *ufw*).

1. Включить системные ограничения *ulimits*:

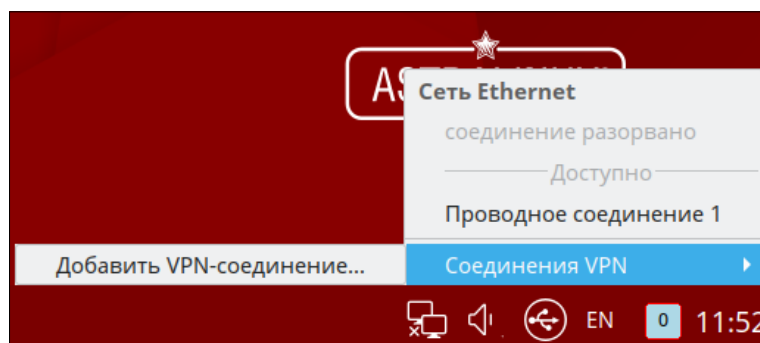
- установить в файле */etc/security/limits.conf* параметры системных ограничений: *\* hard core 0*, *\* hard fsize 50000000*, *\* hard nproc 1000*;
- из терминала *Fly* в «привилегированном» режиме выполнить команду просмотра текущих настроек *systemctl is-enabled astra-ulimits-control* (если блокировка не настраивалась, то выводится предупреждение об отсутствии *astra-ulimits-control.service*);
- для включения выполнить команду *astra-ulimits-control enable* (отключение производится запуском данной команды с параметром *disable*);
- после настройки для проверки повторить команду *systemctl is-enabled astra-ulimits-control*.

```
/etc/security/limits.conf
# End of file
* hard fsize 50000000
* soft fsize 25000000
* hard nofile 4096
* soft nofile 2048
* hard nproc 2000
* soft nproc 1000
* hard core 0
```

1. Включить режим киоска для непривилегированных учётных записей пользователей (пользователей с уровнем целостности «Низкий»), для чего использовать графическую утилиту *fly-admin-kiosk* (порядок включения режима киоска для учётной записи пользователя описан в документации «Руководство по КСЗ. Часть 1»).
2. Включить графический киоск *Fly* с помощью графической утилиты *fly-admin-smc* (порядок включения режима графического киоска для учётной записи пользователя описан в документации «Руководство по КСЗ. Часть 1»).
3. Включить контроль подписей (в настройках модуля *digsig*: *DIGSIG\_XATTR\_MODE=1*) в расширенных атрибутах (*xattr*), для чего сгенерировать ключи и подписать цифровой подписью в *xattr* все основные файлы ОС/СН (рекомендуемые каталоги для подписи: */lib*, */lib64*, */lib32*, */bin*, */sbin*, */boot*, */opt*, */srv*, */usr*).
4. При использовании мандатного управления доступом и обработке файлов с уровнем конфиденциальности выше минимального настроить дополнительное защитное преобразование файлов (с использованием команды *gpg* или встроенных функций файлового менеджера *fly-fm*):
  - открыть в файловом менеджере *fly-fm* каталог «Документы» и с использованием контекстного меню создать файл «Документ LibreOffice»;



- с использованием контекстного меню файла «Документ *LibreOffice.odt*» выбрать пункт меню «Действия», «Защитное кодирующее преобразование», ввести 2 раза пароль; в результате будет создан файл «Документ *LibreOffice.odt.gpg*», теперь данный файл может быть «открыт» (при этом будет восстановлен исходный файл), либо выполнено «Защитное раскодирующее преобразование» (при этом после восстановления файл «Документ *LibreOffice.odt.gpg*» будет удалён) с использованием ввода пароля.
1. Для работы с конфиденциальной информацией в сети настроить защитное преобразование пакетов с помощью создания доверенной сети VPN:
    - осуществить настройку VPN соединения в меню сетевого подключения (по нажатию левой кнопки мыши на значке сети) с помощью меню «Соединения VPN», «Добавить VPN соединение...»;
    - выбрать соединение *OpenVPN*, установить параметры соединения в соответствии с параметрами сервера VPN, к которому осуществляется подключение;
    - в вкладке «VPN» для установки соединения ввести адрес сервера VPN в поле «Шлюз», указать соответствующий тип аутентификации на сервере в поле «Тип» и задать параметры подключения, соответствующие данному типу;
    - дополнительные параметры (такие как сжатие, используемые алгоритмы шифрования, протокол и пр.) задать после нажатия кнопки «Дополнительно...» в вкладке «VPN» в соответствии с настройками VPN;
    - задать параметры получения адреса сети VPN в вкладках «Параметры IPv4» или «Параметры IPv6».



1. Настроить обработку конфиденциальной информации при обмене почтовыми сообщениями, используя защитные GPG-преобразования писем с помощью плагина для почтового приложения *Thunderbird Enigmail*, для чего при создании каждого сообщения электронной почты использовать быструю кнопку доступа «Защита» и выбирать «Шифровать это сообщение» и/или «Подписывать это сообщение».

2. При создании новых учётных записей пользователей формировать пароли с заданным уровнем сложности в соответствии с политикой безопасности, для чего использовать графическую утилиту «Политика безопасности».

Настроить  *pam\_tally*  для задан