Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

Специальность 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

**ОТЧЕТ**

**ПО УЧЕБНОЙ ПРАКТИКЕ**

Профессиональный модуль УП.01.01

*(наименование профессионального модуля)*

Выполнил:

обучающийся учебной группы № 1222

А.А.Солодовников

*(И.О. Фамилия)*

Проверил:

руководитель практики от колледжа:

\_\_\_\_\_\_\_\_\_\_\_\_\_

*(И.О. Фамилия)*

\_\_\_\_\_\_\_\_\_\_\_\_\_

*(И.О. Фамилия)*

**Москва**

**20­­­­24**

**Перечень заданий/работ, выполненных в ходе учебной практики**

Специальность 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

*(наименование специальности)*

Профессиональный модуль УП.01.01

*(наименование профессионального модуля)*

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Темы учебной практики** | **Выполненные задания/работы** |
| 1 | Тема 1. «Управление учетными записями пользователей» | - Исследуйте основные виды и настройки управления учетными записями пользователей СВОЕЙ операционной системы  - Выполните действия по созданию и управлению учетными записями пользователей |
| 2 | Тема 2. создание и управление квотами для общих ресурсов на базе Windows | - Создание общего ресурса на файловом сервере  - Создание подразделения, пользователя и группы в Active Directory Windows Server 2016  - Создание и конфигурирование групповой политики Windows Server 2016  - Создание и настройка квот дискового пространства |
| 3 | Тема 3. Создание и настройка параметров мандатного управления доступом | В ходе лабораторной работы необходимо произвести установку и настройку пакетов OpenLDAP, Kerberos, NSS, PAM, NFS, SMB, NMBD. |
| 4 | Тема 4. Мандатный контроль целостности в Astra Linux 1.6 | Реализация мандатного контроля целостности в Astra Linux 1.6 |
| 5 | Тема 5. Настройка механизма замкнутой программной среды | В лабораторной работе продемонстрирована организация замкнутой программной среды  для пользователей |
| 6 | Тема 6. Установка и настройка сервера DNS | научиться устанавливать сервер имён, добавлять зоны расширения имён, включать автоматическое обновление зон. |
| 7 | Тема 7. Служба каталогов Astra Linux Directory | Создание единого пользовательского пространства ALD. |
| 8 | Проектная работа по созданию баз данных | Разработать и создать базу данных магазина одежды и программы для взаимодействия с ней |

# Тема 1. «Управление учетными записями пользователей»

**Цель работы:** Сформировать навык студентов по созданию и управлению учетными записями пользователей.

Для перехода в режим настройки и редактирования учетных записей необходимо в панели управления выбрать категорию Учетные записи пользователей, и в этой категории щелкнуть на ссылке Добавление и изменение учетных записей пользователей. В результате на экране откроется окно, изображенное на рис. 1.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок

В данном окне содержится перечень созданных ранее учетных записей, а также меню Выберите задание. Вы можете самостоятельно создавать новые и редактировать имеющиеся записи, а также удалять их. Далее мы рассмотрим каждый из этих режимов.

**Ввод новой учетной записи**

Чтобы создать новую учетную запись, щелкните мышью на ссылке Создание учетной записи – при этом на экране отобразится окно, показанное на рис. 2.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Автоматически созданное описание

Рисунок

В данном окне необходимо с клавиатуры ввести имя создаваемой учетной записи. В качестве имени можно использовать любое слово, произвольный набор символов и т. д. Например, на рис. 3 созданным учетным записям присвоены имена Alex, Запись для сети, Администратор и Гость.

После этого с помощью соответствующего переключателя необходимо выбрать тип создаваемой учетной записи; возможные значения – Обычный доступ и Администратор (функциональные различия между типами учетных записей пользователей приведены выше).

Завершается процесс создания учетной записи пользователя нажатием кнопки Создание учетной записи – после этого новая учетная запись отобразится в списке учетных записей (рис. 3). Кнопка Отмена предназначена для выхода из данного режима без сохранения изменений.

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

Рисунок

**Редактирование и удаление учетных записей**

Для перехода в режим редактирования учетной записи необходимо щелкнуть мышью на ее значке. В результате в открывшемся окне будет выдан запрос на выполнение дальнейших действий; для выбора необходимо щелкнуть на одной из следующих ссылок:

• Изменение имени учетной записи;

• Создание пароля;

• Изменение рисунка;

• Установить родительский контроль;

• Изменение типа учетной записи;

• Удаление учетной записи.

Если для выбранной учетной записи пароль был задан ранее, то вместо ссылки Создание пароля в списке будут присутствовать ссылки Изменение пароля и Удаление пароля.

При щелчке на ссылке Изменение имени учетной записи на экране откроется окно, похожее на окно, изображенное на рис. 5.2. Разница заключается в том, что в нем будет отсутствовать переключатель выбора типа учетной записи, а вместо кнопки Создание учетной записи находится кнопка Переименовать.

При выборе ссылки Создание пароля на экране откроется окно, которое показано на рис..4.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Автоматически созданное описание

Рисунок

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Автоматически созданное описание

Рисунок

**Родительский контроль**

В любой семье, где есть несовершеннолетние дети, рано или поздно возникает проблема ограничения доступа ребенка к компьютеру. Не секрет, что в последние годы серьезно обострилась проблема компьютерной зависимости детей и подростков. Над этой проблемой работают психологи, педагоги и другие специалисты, и все они отмечают: компьютерная зависимость – это болезнь. Причем она влечет за собой возникновение еще целого ряда расстройств, которые в общем случае можно разделить на две категории: психические и физические.

Среди психических расстройств среди детей и подростков, возникновение которых обусловлено компьютерной зависимостью, можно отметить следующие:

• отсутствие интереса к «живому» общению и, напротив – чрезмерное увлечение виртуальным общением (электронная почта, чаты, и т. п.);

• неумение на словах выразить свои мысли;

• молчаливость, замкнутость;

• раздражительность;

• явное снижение интереса к окружающей действительности, стремление в любую свободную минуту сесть за компьютер;

• утомляемость, снижение успеваемости в школе, неумение сосредоточиться;

• нарушение сна;

• ухудшение аппетита.

Что касается физических расстройств у детей, страдающих компьютерной зависимостью, то среди них в первую очередь можно выделить:

• ухудшение зрения (несмотря на то, что жидкокристаллические мониторы считаются почти безвредными, глаза при работе за компьютером в любом случае находятся в напряжении, особенно при увлечении различными играми, «стрелялками», и т. п., не говоря уже об ЭЛТ – мониторах);

• изменение осанки вплоть до искривления позвоночника;

• головные боли;

• проблемы в области таза.

Но любое заболевание, как известно, легче предупредить, чем излечить. В данном разделе мы расскажем о том, как с помощью реализованной в Windows 7 функции родительского контроля ограничить использование ребенком компьютера (это касается как времени работы за компьютером, так и доступа к тем или иным приложениям и материалам).

Родительский контроль позволяет регулировать использование компьютера детьми. В частности, можно определить промежутки времени, на протяжении которых дети могут работать за компьютером, а также установить, какими играми и приложениями они могут пользоваться.

Если ребенок попытается запустить запрещенную игру или открыть запрещенную программу, то на экране отобразится информационное сообщение о том, что данное приложение заблокировано. В данном случае ребенок с помощью соответствующей ссылки может запросить разрешение на доступ к приложению, и вы можете предоставить этот доступ, указав свои учетные данные.

**Настройка ограничения времени работы за компьютером**

Чтобы ограничить время нахождения ребенка за компьютером, щелкните на ссылке Ограничение по времени (см. рис. 7). В результате на экране отобразится окно, изображенное на рис. 8.

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Автоматически созданное описание

Рисунок

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

Рисунок

**Настройка ограничения доступа к играм**

В настоящее время на IT – рынке представлено великое множество самых разнообразных компьютерных игр. Среди них есть как полезные для детей и подростков игры, так и те, доступ к которым имеет смысл ограничить. Среди полезных компьютерных игр можно отметить, например, развивающие и обучающие игры, а среди вредных для детской психики – разные «стрелялки», игры со сценами насилия, интимных сцен, разжигающие национальную рознь, и т. д.

Чтобы ограничить доступ ребенка к установленным на компьютере играм, щелкните на ссылке Игры (см. рис. 7). В результате на экране откроется окно, изображенное на рис. 9.

Изображение выглядит как текст, снимок экрана, дизайн

Автоматически созданное описание

Рисунок

**Настройка ограничения доступа к приложениям**

Как мы уже отмечали ранее, вы можете настроить для вашего ребенка ограничение на доступ к имеющимся на компьютере программам. Это полезно нее только для того, чтобы запретить ребенку пользоваться сомнительными приложениями, но и с целью защиты своих данных от порчи или утраты. Например, если у вас хранится много важных данных в разных Excel – документах, то можно от греха подальше вообще заблокировать для ребенка запуск табличного редактора Excel. Как вариант – можно настроить ограничение прав доступа к конкретным файлам и папкам, но о том, как это делать, мы расскажем позже.

Чтобы ограничить доступ к установленным на компьютере приложениям, щелкните на ссылке Разрешение и блокировка отдельных программ (см. рис. 7). В результате на экране откроется окно, которое показано на рис. 11.

Изображение выглядит как текст, снимок экрана, чек, меню

Автоматически созданное описание

Рисунок

**Настройка ограничения доступа к приложениям**

Изображение выглядит как текст, снимок экрана, Шрифт, веб-страница

Автоматически созданное описание

Рисунок

**Вывод:** научились манипулировать учетными записями в windows.

# Тема 2. Создание и управление квотами для общих ресурсов на базе Windows

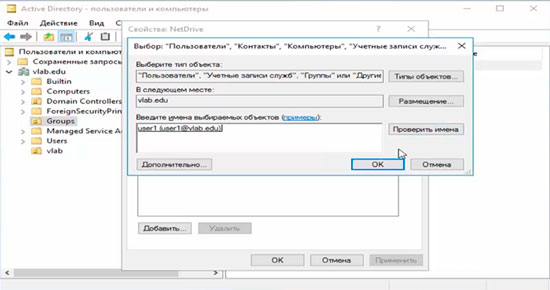
Создаю общий ресурс на файловом сервере

Изображение выглядит как снимок экрана, текст

Автоматически созданное описание

Рисунок

Захожу в Диспетчер серверов, перехожу в раздел "Общие ресурсы", щелкаю правой кнопкой мыши и создаю ресурс. Оставляю параметры по умолчанию.



Рисунок

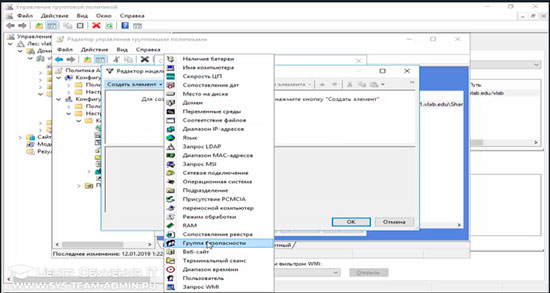
Создаю подразделение, пользователя и группу в Active Directory Windows Server 2016

Открываю оснастку "Пользователи и компьютеры", щелкаю правой кнопкой мыши на домене и создаю новое подразделение. Называю его "vlab".

В этом подразделении создаю нового пользователя "user1". Под ним буду входить в домен на клиентской машине.

В разделе групп создаю группу "NetDrive" и добавляю в нее пользователя "user1". Эта группа понадобится как фильтр безопасности для применения групповой политики.

Создаю и конфигурирую групповую политику Windows Server 2016



Рисунок

Открываю оснастку "Управление групповой политикой" и в разделе объектов создаю новую групповую политику. Называю ее "AddNetDrive".

Меняю содержимое групповой политики. В разделе конфигурации пользователя перехожу в раздел "Настройки", затем в "Конфигурация Windows" и выбираю "Сопоставление дисков".

Создаю элемент "Сопоставленный диск". В параметрах указываю путь к общему ресурсу (например, \\ad1\share), букву диска и устанавливаю флажок "Выполнять в контексте пользователя".

Привязываю объект к подразделению "vlab" и указываю в фильтре безопасности группу "NetDrive".

Вхожу в систему и проверяю подключение сетевого диска

Изображение выглядит как снимок экрана, текст, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок

Ввожу учетные данные и вхожу в систему под доменной учетной записью "user1". Проверяю, подключился ли сетевой диск. Диск подключен.

Устанавливаю квоту на дисковое пространство

Изображение выглядит как снимок экрана, программное обеспечение, текст, веб-страница

Автоматически созданное описание

Рисунок

Открываю Диспетчер ресурсов файлового сервера, перехожу в раздел квот и создаю новую квоту. Назначаю ей параметры по умолчанию.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок

Этого достаточно, чтобы изучить принцип действия квотирования.

Проверяю применение квоты

Изображение выглядит как снимок экрана, текст, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок

Возвращаюсь на клиентский ПК и проверяю, что квота применена и функционирует. Доступное для использования пространство общего ресурса ограничено размером в 100 МБ. убери звездочки

# Тема 3. Создание и настройка параметров мандатного управления доступом

**Цель работы:** изучить и освоить администрирование основных параметров мандатного управления доступом в ОССН Astra Linux Special Edition с применением графических утилит и консольных команд.

**Порядок выполнения работы**

1. Отключил блокировку экрана. Для этого щелкнул ПКМ на рабочем столе и выбрал «Свойства».
2. Создал учётную запись «user» c паролем «Student123». Добавил учетную запись «user» во вторичную группу astra-admin.

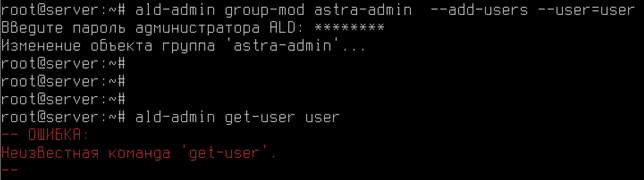


Рис. 1. Добавление учётной записи «user» во вторичную группу astra-admin

1. Начал работу со входа в ОССН в графическом режиме с учётной записью пользователя «user».

https://studfile.net/html/47320/250/html_48yoYFzjSP.jjR2/htmlconvd-PyvDzF_html_4836ed7d9bab7063.png

Рис. 2. Вход в учётную запись пользователя «user»

1. Запустил графическую утилиту редактирования учетных записей пользователей «Управление политикой безопасности» через команду sudo fly-admin-smc.

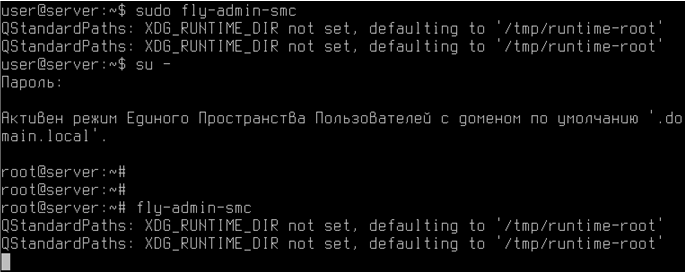


Рис. 3. Запуск графической утилиты

1. Модифицировал параметры мандатного управления доступом, для этого осуществил следующие действия:
   1. открыть раздел «Уровни» и выбрать «0: Уровень\_0» и переименовать данный уровень доступа: «Уровень0»;
   2. выполнить создание уровня доступа с именем «Уровень\_4», задав значение равное 4, после чего проверить наличие записи «Уровень\_4» в списке «Уровни»;
   3. выполнить обратное переименование: «Уровень0» в «Уровень\_0».



Рис.4. Создание уровней доступа

1. Создал учётную запись пользователя user1, установив максимальный уровень доступа (конфиденциальности): «Уровень\_4».

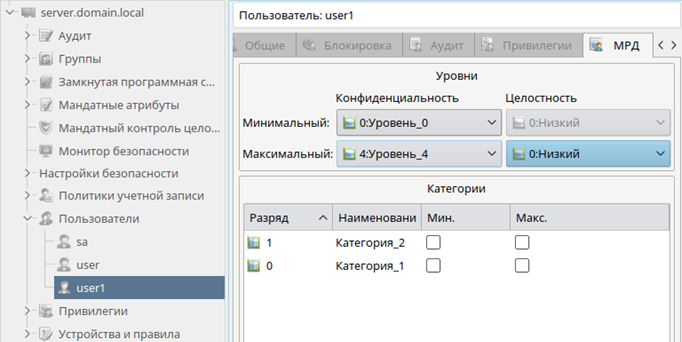


Рис. 5. Создание пользователя user1 с уровнем доступа 4

1. Выполнил удаление уровня доступа 4 из раздела «Уровни» путем выбора в контекстном меню пункта «Удалить».

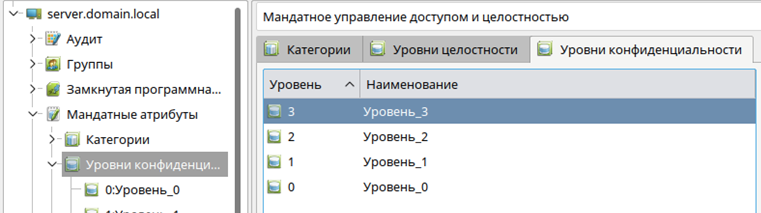


Рис. 6. Удаление уровня доступа

1. Открыл учётную запись пользователя user1 и в закладке «Дополнительные» в элементе «Максимальный уровень» проверил наличие записи «(4)», при этом, в списке выбора уровня «Уровень\_4» будет отсутствовать. Создал учетные записи user20, user30, user40. Задал в произвольном порядке значения для параметров «Конфиденциальность», «Целостность», «Категории».

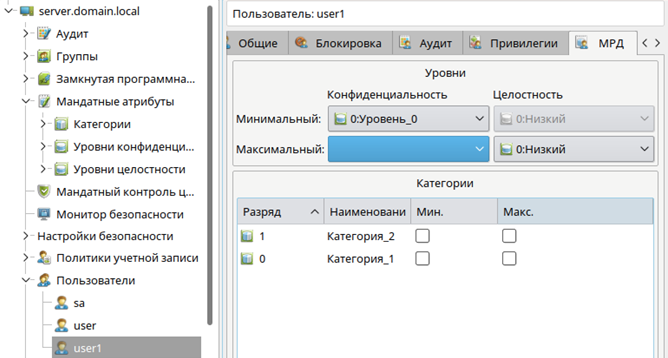


Рис. 7. Проверка отсутствия уровня 4

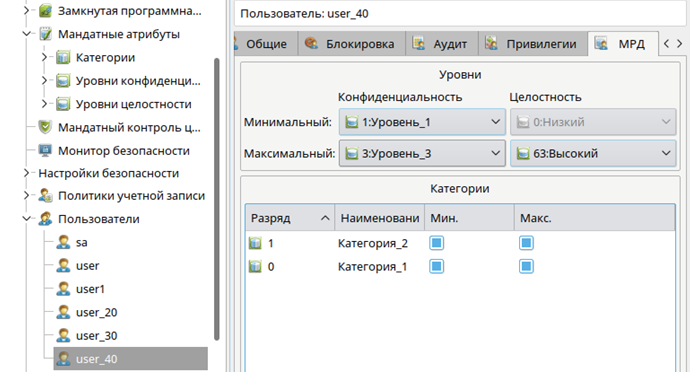


Рис. 8. Создание новых учётных записей

1. Ознакомился с содержимым каталога etc/parsec/macdb. Вывел в терминал Fly параметры мандатного управления доступом для учётной записи пользователей user1, user20, user30, user40. Мандатные атрибуты, назначенные конкретным учётным записям пользователей, перечисляются в каталоге /etc/parsec/macdb. Для выполнения задания 7 осуществил следующие действия:
   1. запустить терминал Fly и перейти в каталог /etc/parsec/macdb (команда cd /etc/parsec/macdb )
   2. вывести на экран содержимое каталога /macdb ( ls )
   3. просмотреть содержимое файлов в каталоге /macdb ( sudo cat “имя файла” )
   4. прочитать параметры учётной записи user1 командой sudo grep “user1” \*
   5. определить максимальный уровень доступа учётной записи user1 командой sudo grep «user1» \* | cut -d : -f 5
   6. определить минимальный уровень доступа учётной записи user1 командой sudo grep «user1» \* | cut -d : -f 3 и проверить его соответствие данным, отображаемым в графической утилите «Управление политикой безопасности».

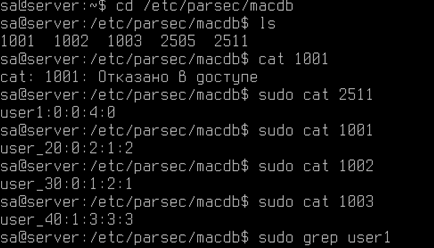


Рис. 9. Пункты a-c

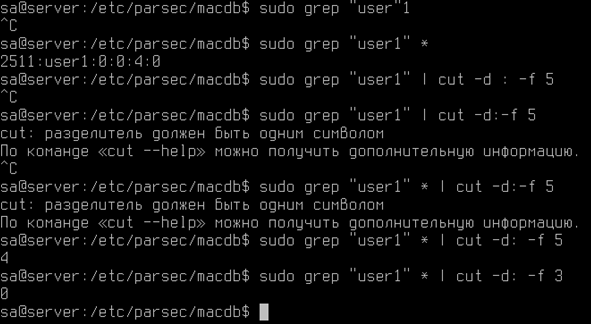


Рис. 10. Пункты d-f

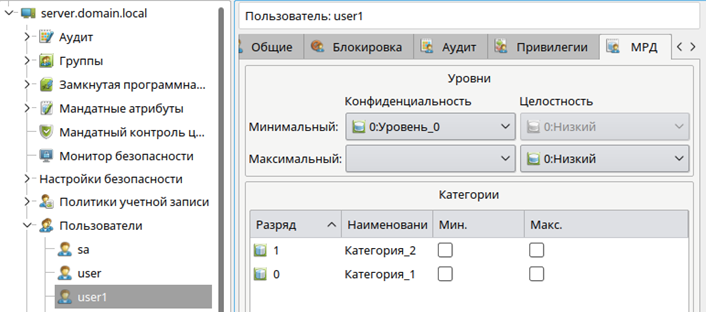


Рис. 11. Проверка вывода команд на соответствие выводу графической утилиты

1. Создал неиерархические категории с использованием графической утилиты «Управление политикой безопасности». Для этого выполниk следующие действия:
   1. в разделе «Категории» удалить все Категории.
   2. в разделе «Категории» создать новую неиерархическую категорию с именем «Otdel1», «Разряд» — 0;
   3. в разделе «Категории» создать новые неиерархические категории: «Otdel2» («Разряд» — 1), «Upravlenie» («Разряд» — 2).

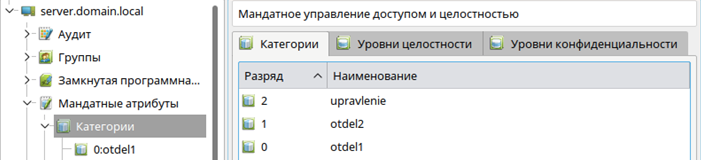


Рис. 12. Создание новой иерархической категории

1. Изменил набор неиерархических категорий с использованием графической утилиты «Управление политикой безопасности» (sudo fly-admin-smc), для этого выполниk следующие действия в разделе «Категории»:
   1. выбрать неиерархическую категорию «Otdel1» и ввести наименование «Отдел\_1»;
   2. аналогично переименовать неиерархические категории «Otdel2» и «Upravlenie» в «Отдел\_2» и «Управление» соответственно;
   3. проанализировать возможность одновременного изменения элемента «Разряд».

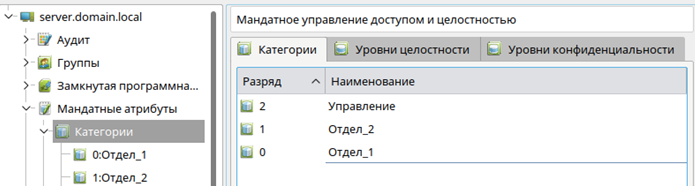


Рис. 13. Ввод наименований

1. Изменил мандатный уровень доступа с использованием графической утилиты «Управление политикой безопасности», для этого выполниk следующие действия:
   1. создать новую группу с именем «office1» и задать первичную группу учётной записи пользователя user1 — «office1»;
   2. создать новую учетную запись пользователя user2 и установить её первичную группу — «officel»;
   3. в закладке «МРД» осуществить попытку выбора минимального набора неиерархических категорий — «Отдел\_2» и проанализировать результат;
   4. в закладке «МРД» выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_2», после чего задать минимальный набор неиерархических категорий — «Отдел\_2»;
   5. 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»;.
   6. создать учётную запись пользователя rukoffice1 и задать первичную группу: «office1» ;
   7. в закладке «МРД» выбрать максимальный уровень: «Уровень\_3», максимальный набор категорий: «Отдел\_1», «Отдел\_2», «Управление».

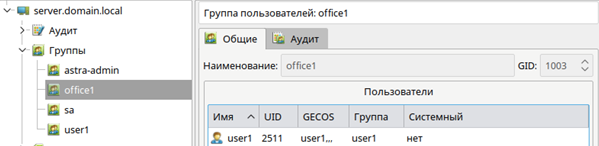


Рис. 14. Создание новой группы

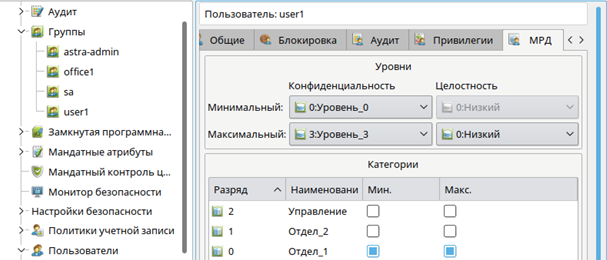


Рис. 15. Создание новой учётной записи

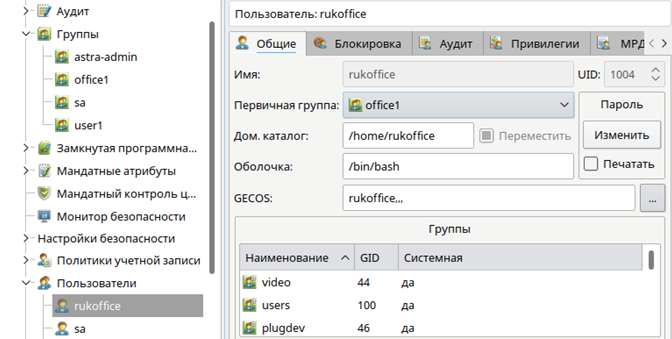


Рис. 16. Выполнение пункта c

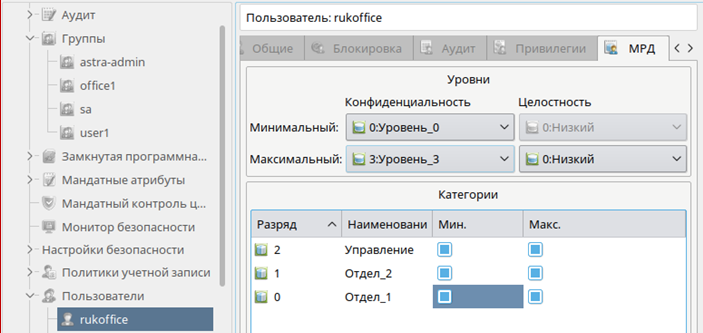


Рис. 17. Выполнение пункта d

1. Созда общий каталог для работы от имени учётных записей пользователей userl, user2, rukoffice1 в каталоге /home/work. Для работы от имени учётных записей пользователей с наборами неиерархическими категорий «Отдел\_1», «Отдел\_2» и «Управление» выделить отдельные каталоги «otdel1», «otdel2» и «upr» соответственно.

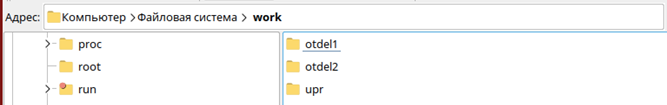


Рис. 18. Структура каталогов

1. При этом обеспечил хранение файлов с различными уровнями конфиденциальности в каталогах с использованием специального атрибута CCNR, для чего осуществить следующие действия:
   1. запустить терминал Fly в «привилегированном» режиме командой sudo fly-term;
   2. Прочесть информацию по командам mkdir, chown и chmode в приложении для практической работы.
   3. создать каталог work и задать параметры мандатного и дискреционного управления доступом командами:

*mkdir /home/work*

*chown user /home/work -v (назначение user владельцем каталога)*

*ls –lh (посмотрите изменения параметра “владелец” для каталога work)*

*chown :office1 /home/work –v (назначение группы)*

*ls –lh (посмотрите изменения параметра “группа” для каталога work)*

*chmod 750 /home/work*

*pdp-flbl 3:0:Отдел\_1,Отдел\_2,Управление:ccnr /home/work –v*

* 1. создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий «Отдел\_1» и задать параметры мандатного и дискреционного управления доступом командами:

*cd /home/work*

*mkdir otdel1*

*chown user1:office1 otdel1*

*chmod 770 otdel1*

*pdp-flbl 3:0:Отдел\_1:ccnr otdel1*

* 1. создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий «Отдел\_2» и задать параметры мандатного и дискреционного управления доступом командами:

*mkdir otdel2*

*chown user2:office1 otdel2*

*chmod 770 otdel2*

*pdp-flbl 3:0:Отдел\_2:ccnr otdel2*

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

*mkdir upr*

*chown rukoffice1:office1 upr*

*chmod 770 upr*

*pdp-flbl 3:0:Управление:ccnr upr*

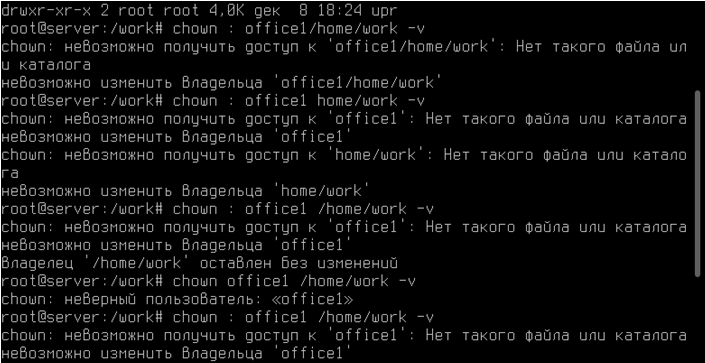


Рис. 19. Задание параметров мандатного и дискреционного управления доступом

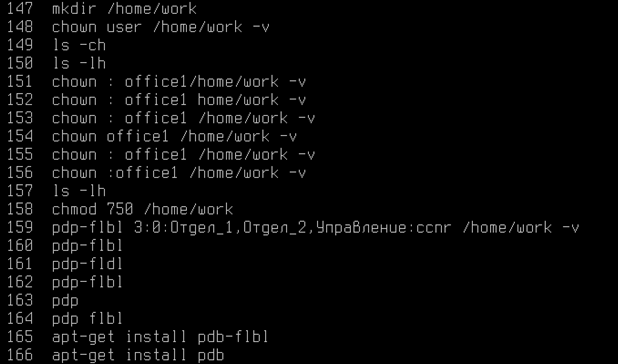


Рис. 20. Листинг команд 14 пункта

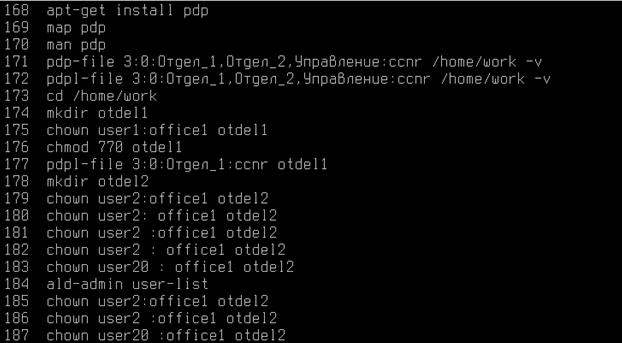


Рис. 21. Листинг команд 14 пункта (продолжение)



Рис. 22. Листинг команд 14 пункта (продолжение) (продолжения)

**Вывод:** я изучил и освоиа администрирование основных параметров мандатного управления доступом в ОССН Astra Linux Special Edition с применением графических утилит и консольных команд.

# Тема 4. Мандатный контроль целостности в Astra Linux 1.6

**Цель работы:** законспектировать видеофайл.

**Мандатный контроль целостности**

Мандатный контроль целостности - это процесс проверки целостности данных, который осуществляется на основе прав доступа и прав пользователей к информационной системе. Этот вид контроля обеспечивает защиту данных от несанкционированных изменений, разрушений или копирования.

В рамках мандатного контроля целостности устанавливаются и проверяются правила и ограничения доступа для пользователей и приложений. Система контроля целостности проверяет, что данные не были изменены или повреждены без разрешения, и что только уполномоченные пользователи имеют доступ к определенным данным.

Этот вид контроля является важной частью обеспечения безопасности данных и обеспечивает сохранность информации от угроз как внутри, так и за пределами организации. Важно поддерживать мандатный контроль целостности в актуальном состоянии и регулярно анализировать его эффективность для обеспечения безопасности информационной системы.

В Astra Linux 1.6 мандатный контроль целостности может быть реализован с помощью механизма SE Linux (Security Enhanced Linux), который позволяет определить правила доступа к ресурсам системы на основе меток безопасности.

**Дискреционное ограничение доступа**

В Astra Linux используется дискреционное ограничение доступа, которое регулирует доступ пользователей к файлам.

Недостатки этого механизма: не позволяет управлять информационными потоками и контролировать утечку данных.

Дискреционное ограничение доступа - это метод управления доступом к ресурсам информационной системы, основанный на предоставлении пользователю контроля над своими собственными данными и ресурсами. Сущность дискреционного ограничения доступа заключается в том, что владелец или создатель данных определяет, кому и какие права доступа предоставляются к собственной информации.

Основные принципы дискреционного ограничения доступа:

1. Владелец информации имеет право определять, кто и как может получить доступ к его данным.

2. Пользователь, который обладает правами доступа, может делиться своими данными или ресурсами с другими пользователями в соответствии с заданными правами.

3. Дискреционное ограничение доступа основывается на концепции "need-to-know" (необходимо знать), что означает, что пользователь получает доступ только к информации, необходимой для выполнения своих обязанностей или задач.

Примером дискреционного ограничения доступа являются системы управления правами доступа (Access Control Lists - ACL), где владелец информации может устанавливать список пользователей или групп пользователей с различными уровнями доступа к файлам или папкам.

Дискреционное ограничение доступа является одним из основных методов обеспечения безопасности данных в информационных системах и позволяет управлять доступом к информации на уровне индивидуальных пользователей.

**Мандатное управление доступом**

Мандатное управление доступом работает по уровням конфиденциальности и категориям.

Реализовано в Astra Linux с помощью подсистемы безопасности Parsec.

В Astra Linux 1.6 мандатное управление доступом реализуется с помощью механизма Security Enhanced Linux (SE Linux). SE Linux предоставляет возможность добавления дополнительного уровня обеспечения безопасности, который работает на основе меток безопасности.

SE Linux позволяет администраторам системы определить политики безопасности для контроля доступа к ресурсам системы, таким как файлы, каталоги, процессы и сетевые соединения. При этом SE Linux дополнительно к основным правам доступа (режим DAC - discretionary access control) использует мандатный контроль доступа (MAC - mandatory access control), который принуждает процессы к выполнению определенных правил безопасности.

Администратор Astra Linux может настроить уровень безопасности SE Linux в соответствии с требованиями безопасности своей системы, определяя разрешенные и запрещенные действия для различных сущностей в системе. SE Linux позволяет усилить защиту от атак, включая привилегированные угрозы, эксплойты и распространение вредоносного программного обеспечения.

Для работы с мандатным управлением доступом в Astra Linux 1.6 необходимо иметь соответствующие знания по настройке SE Linux и опыт в администрировании системы.

**Примеры работы мандатного контроля целостности**

В видео демонстрируется, как работает мандатный контроль целостности на примере процессов с разными уровнями целостности.

В Linux, если взламывают иксорга и получают привилегии рута, то в Windows это не получится, так как процессы с низким уровнем целостности не могут влиять на процессы с высоким уровнем.

**Мандатный контроль целостности**

В системе действует мандатный контроль целостности, но он не применяется к файлам.

Для включения мандатного контроля целостности необходимо зайти в панель управления и включить защиту файловой системы.

**Защита файловой системы**

После включения защиты файловой системы все файлы получают максимальный уровень контроля целостности.

Если пользователь пытается изменить файл с высоким уровнем контроля целостности, ему будет отказано в доступе.

**Мониторинг и защита от эксплоитов**

Монитор Parsec отслеживает действия пользователей с низким уровнем мандатного контроля целостности и при обнаружении создания или запуска процесса с высоким уровнем, он его прибивает.

Это усложняет эксплуатацию уязвимостей и повышает уровень безопасности системы.

# Тема 5. Настройка механизма замкнутой программной среды

# Тема 6. Установка и настройка сервера DNS

# Задание 7 Конфигурирование службы astra linux directory

**Цель:** Создание единого пользовательского пространства ALD.

**Используемое программное обеспечение:**

* **VirtualBox**
* **OC Astra Linux**

**Проверка имени компьютера**

Проверили имя компьютера через свойства. Также можно проверить имя компьютера командой hostname через терминал.

Изображение выглядит как текст, Шрифт, число, снимок экрана

Автоматически созданное описание

Рис. 1. Проверка имени на клиенте

Изображение выглядит как текст, Шрифт, программное обеспечение, число

Автоматически созданное описание

Рис. 2. Проверка имени сервера

**Установка ALD на клиенте**

Перед настройкой необходимо установить пакеты из репозитория, иначе после настройки доступа в интернет не будет.

Установка пакетов осуществляется по средствам менеджера пакетов Synaptic. Установленные пакеты показаны на Рис.3

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 3. Установленные пакеты на клиенте

**Настройка сети**

Настроил сеть на клиенте и сервере:

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рис. 4. Настройка на клиенте

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рис. 5. Настройка на сервере

**Конфигурация файла hosts**

В терминале выполнили следующие команды:

sudo –i

kate /etc/hosts

Команда sudo –i, меняет текущего пользователя на root.

Команда kate /etc/hosts, открывает файл hosts, и позволяет его редактировать.

После выполнения данных команд откроется файла hosts, в котором дописали строки привязки сервера и клиента.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 6. Файл hosts на клиенте

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Автоматически созданное описание

Рис. 7. Файл hosts на сервере

**Проверка работоспособности сети**

Выполним команды:

*ping client.domain.local* – на сервере

*ping server.domain.local* – на клиенте

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рис. 8. Ping с сервера на клиента

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 9. Ping с клиента на сервер

**Установка ALD на сервер**

Запустили Менеджер пакетов Synaptic и установили следующие пакеты:

*ald-server-common*

*ald-admin-common*

*fly-admin-ald-server*

Пакет *ald-server-common* содержит набор программ и утилит для работы службы ALD. Пакет *ald-admin-common* содержит набор программ и утилит для администрирования службы ALD.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 10. Установленные пакеты на сервер

**Настройка службы ALD**

Поле запуска программы в открывшемся окне ввожу пароль *admin*. Дале перешел в раздел Создание ALD сервера.

При создании ALD сервера указал данные как на рисунке 11.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 11. Настройка ALD сервера

После происходит процесс инициализации ALD сервера рис. 12.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рис. 12. Процесс инициализации ALD сервера

Подключаем домен. В левой части программы Доменной политики безопасности отобразилась структура домена рис. 13.

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Автоматически созданное описание

Рис. 13. Дерево домена

**Настройка ALD на клиента и подключение к домену**.

Запустил Настройку ALD клиента Fly и указал настройки, приведенные на рисунке 14.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 14. Настройка ALD клиента Fly

После ввода настроек проверил соединение с сервером службы ALD, кнопкой «Проверить соединение».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 10 Нет соединения

Настройка ALD клиента Fly, сообщает об ошибке, а именно заполните конфигурационный файл /etc/ald/ald.conf. Для заполнения файла ald.conf, запускаю терминал и с помощью графического текстового редактора NotePad++ открываю данный файл.

В данном конфигурационном файле задал значения, соответствующие таблице 1.

Таблица 1. Конфигурационный файл ald.conf

|  |  |  |
| --- | --- | --- |
| № п.п. | Параметр | Значение |
| 1 | DOMAIN | .domain.local |
| 2 | SERVER | server.domain.local |
| 3 | SERVER\_ON | 1 |
| 4 | CLIEBT\_ON | 1 |

После изменения конфигурационного файла выполнил проверку соединения с сервером ALD рис. 15.

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Автоматически созданное описание

Рис. 15. Статус соединения с ALD сервером

После успешной проверки нажал на кнопку «Подключиться» рис. 16.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рис. 16. Настройка ADL клиента

**Создание и настройка пользователя ALD**

Для создания пользователя на сервере ALD запустил «Управления доменной политикой безопасности», в выпадающем списке .domain.local перешел во вкладку Пользователи и нажал на кнопку «+». Далее заполнил поле «Имя» и выбрал Тип ФС local.

После создания пользователя изменил ему пароль рис. 17.

Изображение выглядит как снимок экрана, программное обеспечение, текст, Значок на компьютере

Автоматически созданное описание

Рис. 17. Смена пароля

После успешного создания пароля перешел в раздел Привилегии домена и в блоке компьютеры добавил компьютер *client.domain.local*. Затем проверил наличие созданного пользователя рис. 18.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рис. 18. Привилегии домена

**Проверка работоспособности ALD**

После выхода из системы нажал кнопку Сессия, выбрал новую сессию.

После ввода учетных данных нового пользователя осуществил проверку учетных данных пользователя, для этого зашел в терминал Fly рис. 19.

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, Мультимедийное программное обеспечение

Автоматически созданное описание

Рис. 19. Терминал Fly нового пользователя

**Вывод:** в ходе работы было создано единое пользовательское пространство на основе службы ALD. Была произведена настройка проводного соединения между сервером и клиентом. Установлены пакеты серверной и клиентской части службы ALD и графических утилит администрирования. Была проведена настройка конфигурации службы ALD сервера и клиента. Проверена работоспособность единого пользовательского пространства.

# Проектная работа по созданию баз данных

1. **Предметная область**

В качестве предметной области мы выбрали базу данных автомобилей, с информацией от марки и модели, до адреса и цены продажи автомобиля.

**2.Создание базы данных**

Создаем базу данных с помощью данного запроса:

create database mashinki;

use mashinki

create table manufacturers

(

manufacture\_id int primary key,

manufacture\_name varchar(45),

country varchar(45)

)

create table models

(

model\_id int primary key,

model\_name varchar(45),

manufacture\_id int foreign key references manufacturers(manufacture\_id)

)

create table dealers

(

dealer\_id int primary key,

dealer\_name varchar(45),

country varchar(45),

adress varchar(100)

)

create table price\_list

(

order\_id int IDENTITY(1,1) primary key,

dealer\_id int foreign key references dealers(dealer\_id),

manufacture\_id int foreign key references manufacturers(manufacture\_id),

model\_id int foreign key references models(model\_id),

price int

)

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок

В итоге получаем данную диаграмму таблиц где наглядно показаны все связи в таблице (пункт 3).

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок

**4.Заполнение таблиц данными.**

**Начинаем с таблицы производителей “manufacturers”.**

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

Рисунок

**Затем заполняем таблицу с моделями “models”.**

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок

Записей в таблице больше 100.

**Далее идёт таблица “dealers”.**

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок

**После заполняем таблицу “price\_list” где встречаются все наши данные.**

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок

Во время заполнения данной таблицы забыли, что подключили автоинкремент и пытались внести идентификатор, потратив много времени, а в результате дело было максимально простое.

# Разработка СУБД для базы данных.

На этапе подключения к базе данных у нас возникла проблема, не могли подключиться к БД. Подумав, была выдвинута гипотеза, что возможно порт, через который идёт подключение просто закрыт или вообще не указан. Поискав на просторе интернета, было найдено решение данной проблемы.

Вот сама ошибка:

Traceback (most recent call last):   
  File "C:\Users\viper\Desktop\PyProject\SYBDProject\[test.py](https://test.py/)", line 5, in <module>   
    conn = pyodbc.connect("Driver={SQL Server};"   
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^   
pyodbc.OperationalError: ('08001', '[08001] [Microsoft][ODBC SQL Server Driver][Shared Memory]SQL Server не существует, или доступ запрещен. (17) (SQLDriverConnect); [08001] [Microsoft][ODBC SQL Server Driver][Shared Memory]ConnectionOpen (Connect()). (2); [08001] [Microsoft][ODBC SQL Server Driver]Недопустимый атрибут строки соединения (0)')

Решение было максимально простое, но на его поиски было потрачено несколько дней. Вот решение:

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Рисунок

В данном окне всего на просто нужно было сменить динамические порты на статический порт 1433, после чего подключение появилось.