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

Кувшинов.Д.В

*(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 ос.  - 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»

**Практическая работа №6. «Управление учетными записями пользователей»**

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

Для перехода в настройки и редактирования учетных записей нужно в панели управления выбрать категорию Учетные записи пользователей, и в ней щелкнуть на ссылке Добавление и изменение учетных записей пользователей. На экране откроется окно, изображенное на рис. 1.

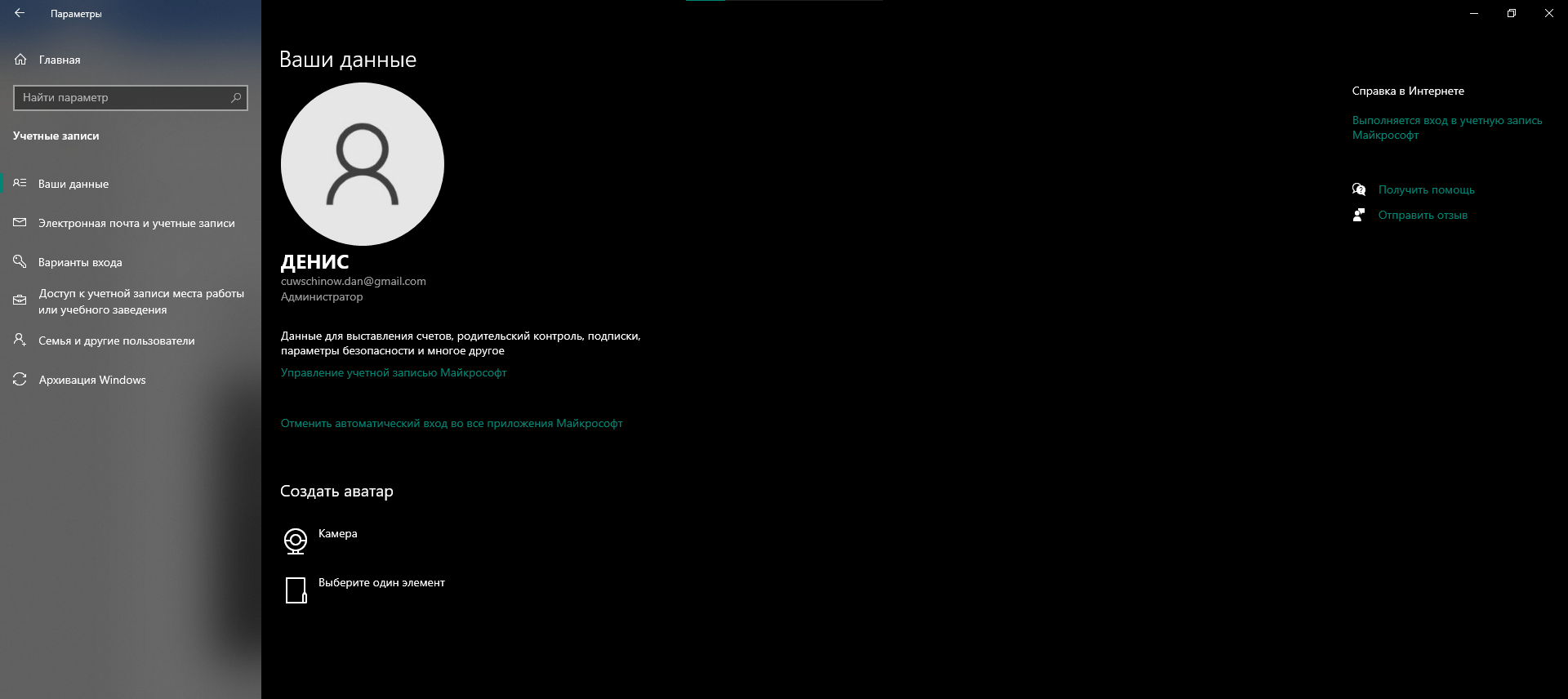


Рисунок 1

В нём содержится перечень созданных ранее учетных записей, а также меню Выберите задание.

**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.

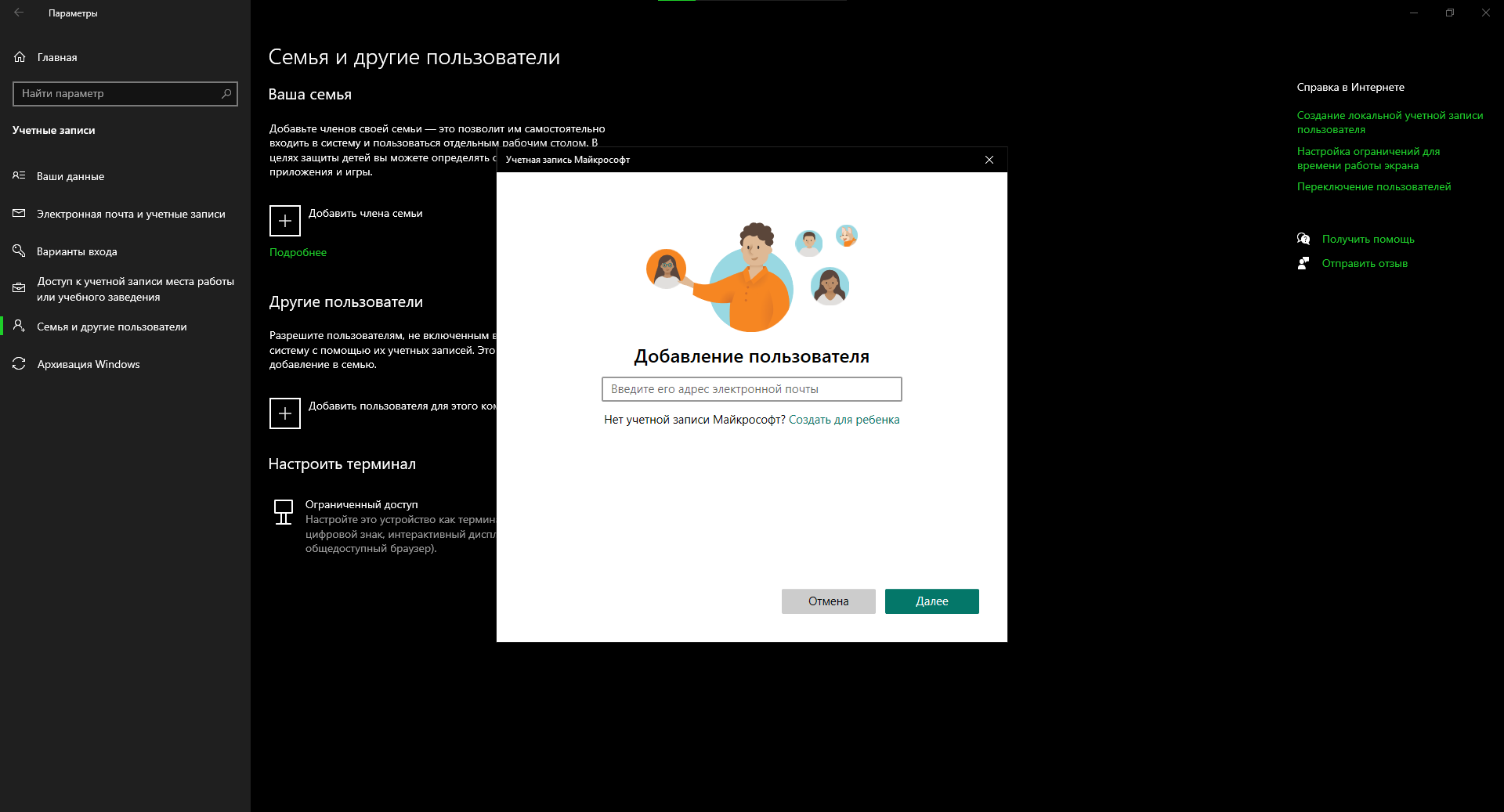
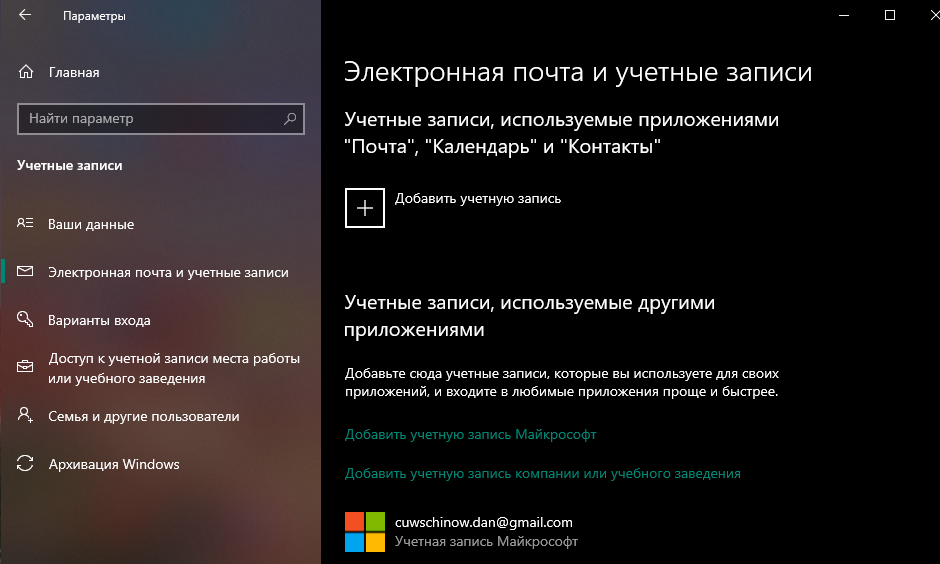


Рисунок 2

В данном окне нужно с клавиатуры ввести имя создаваемой учетной записи. В качестве имени можно использовать любое слово,

После этого с помощью 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 (рис. 3).



**Редактирование и удаление учетных записей**

Для перехода в режим редактирования учетной записи надо 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.

**Родительский контроль**

В любой семье, где есть несовершеннолетние дети, всегда возникает проблема ограничения доступа ребенка к компьютеру

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;

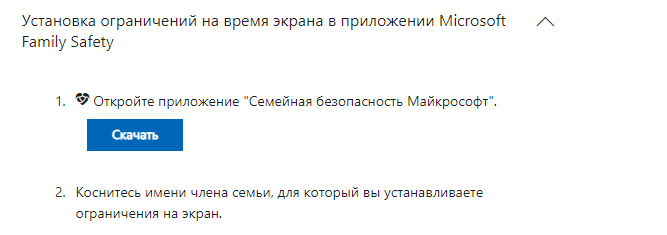
• головные боли;

• 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.

**Настройка ограничения времени работы за компьютером**



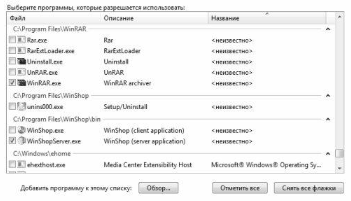
**Настройка ограничения доступа к играм**

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.

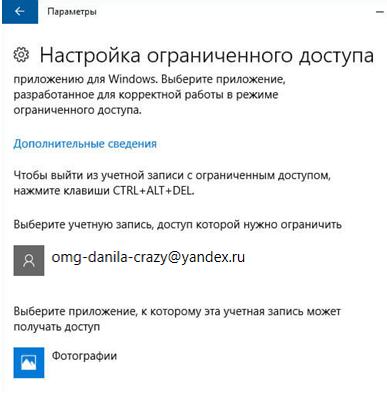
Чтобы ограничить доступ ребенка к установленным на компьютере играм, щелкните на ссылке Игры. В результате на э кране откроется окно, изображенное на рис. 9.

**Настройка ограничения доступа к приложениям**

Как упоминалось ранее, вы можете установить ограничения на доступ вашего ребенка к программам, доступным на вашем компьютере. Это не только запрещает детям использовать подозрительные приложения, но и помогает защитить их данные от повреждения и потери. Например, если у вас много важных данных, хранящихся в различных документах Excel, вы можете безопасно заблокировать запуск дочернего редактора электронных таблиц Excel. Или вы можете установить ограничения на доступ к определенным файлам и папкам, но о том, как это сделать, мы поговорим позже. Чтобы ограничить доступ к установленным на компьютере приложениям, щелкните на ссылке Разрешение и блокировка отдельных программ. В результате на экране откроется окно.



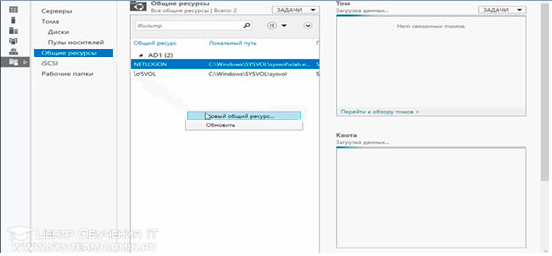
**Настройка ограничения доступа к приложениям**



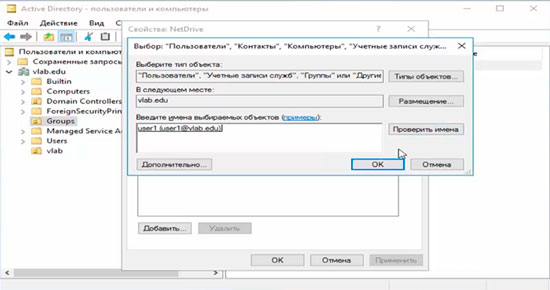
Вывод: мы умеем менять учетные записяи в windows.

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

Создаю общий ресурс на файловом сервере



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



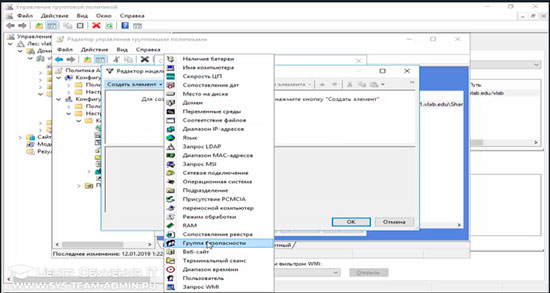
Создаю подразделение, пользователя и группу в Active Directory Windows Server 2016

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



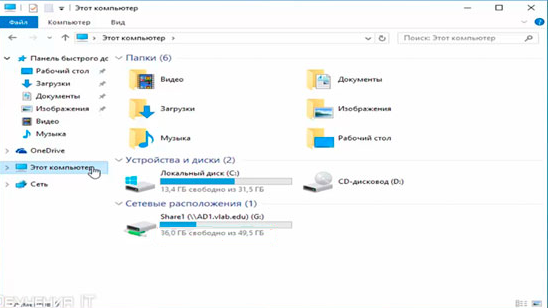
Открываю оснастку "Управление групповой политикой" и в разделе объектов создаю новую групповую политику. Называю ее "AddNetDrive".

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".

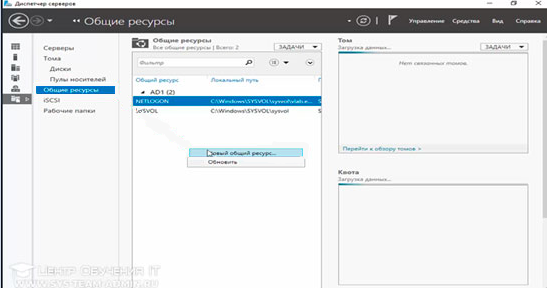
Привязываю объект к подразделению "vlab" и указываю в фильтре безопасности группу "NetDrive".

Вхожу в систему и проверяю подключение сетевого диска

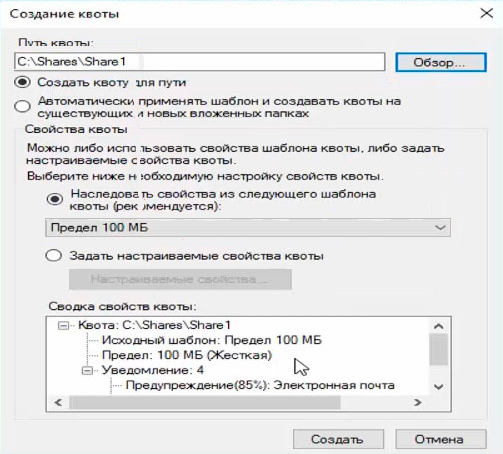


Ввожу учетные данные и вхожу в систему под доменной учетной записью "user1". Проверяю, подключился ли сетевой диск. Диск подключен.

Устанавливаю квоту на дисковое пространство

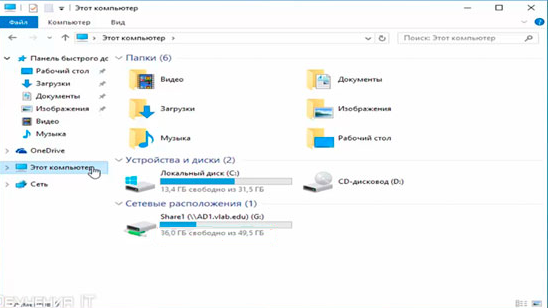


Открываю Диспетчер ресурсов файлового сервера, перехожу в раздел квот и создаю новую квоту. Назначаю ей параметры по умолчанию.



Этого достаточно, чтобы изучить принцип действия квотирования.

Проверяю применение квоты



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

**Третья часть**

**Цель лабораторной работы**

Изучить и освоить администрирование основных параметров мандатного управления доступом в ОССН Astra Linux Special Edition с применением графических утилит и консольных команд.

**Задание на лабораторную работу**

В ходе лабораторной работы необходимо произвести установку и настройку пакетов OpenLDAP, Kerberos, NSS, PAM, NFS, SMB, NMBD.

**Порядок выполнения работы**

Создание учетной записи

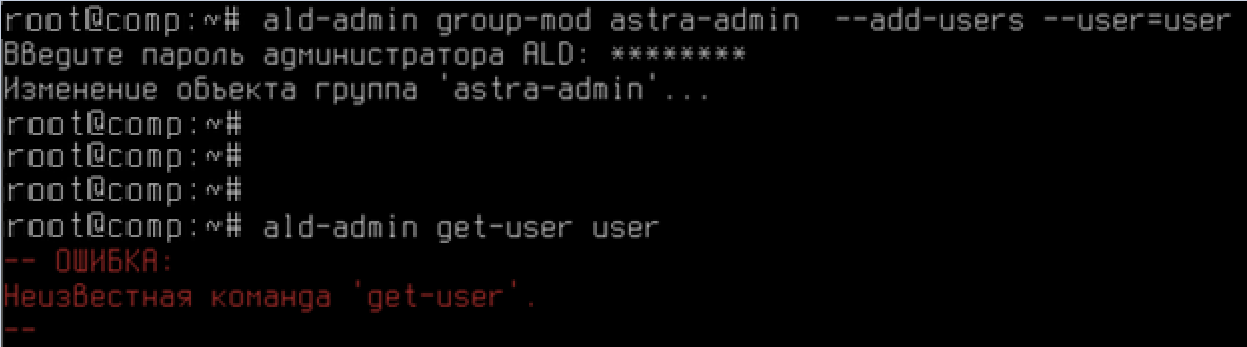


Рис. 1

Вход в учётную запись пользователя «user»



Рис. 2.

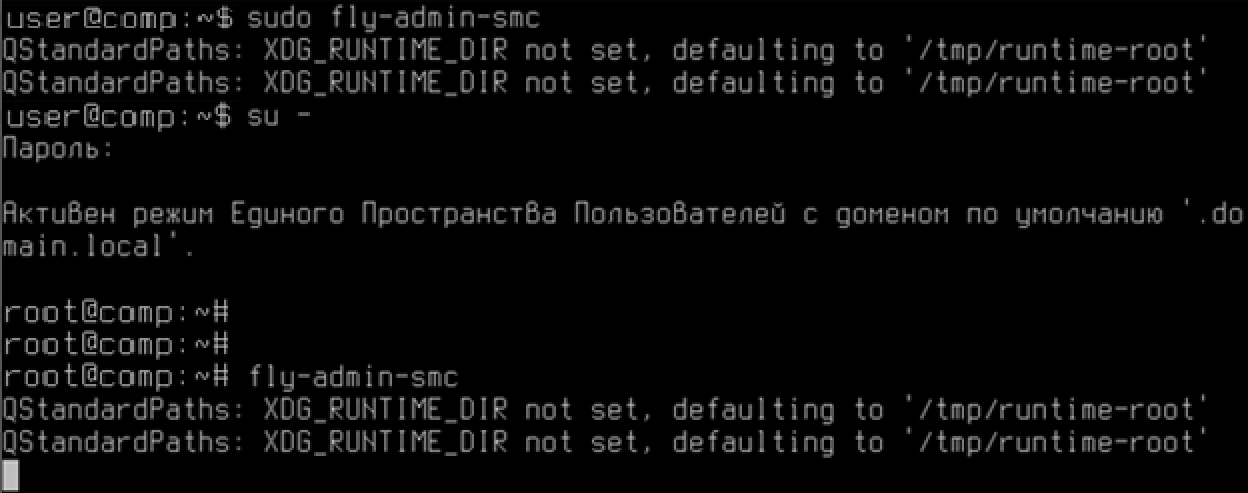
Запуск графической утилиты 

Рис. 3.

Создание уровней доступа 

Рис.4.

Создание пользователя user1 с уровнем доступа 4

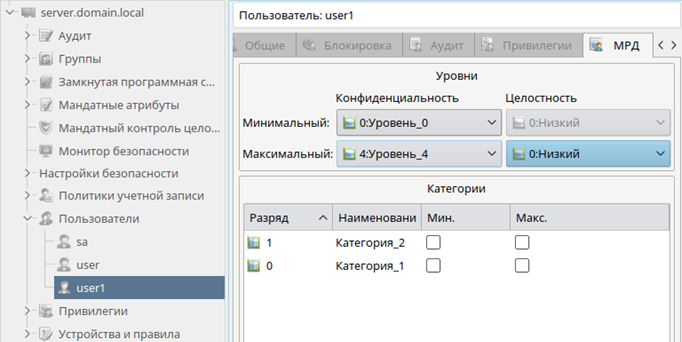


Рис. 5.

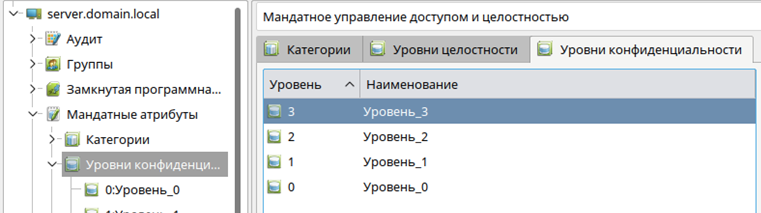
Удаление уровня доступа 

Рис. 6.

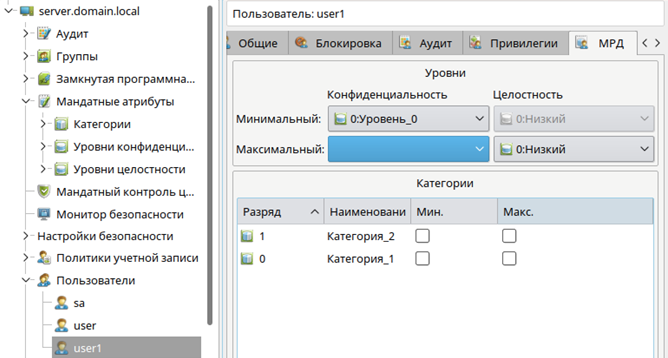
Проверка отсутствия уровня 4

Рис. 7.

Создание новых учётных записей

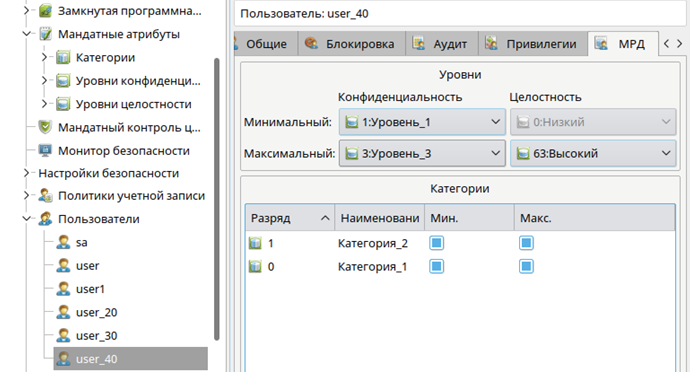


Рис. 8.

* 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».

Пункты a-c

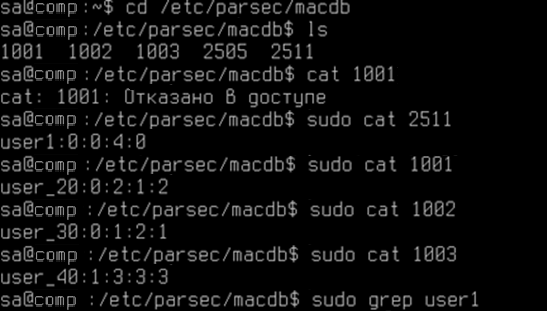


Рис. 9.

Пункты d-f

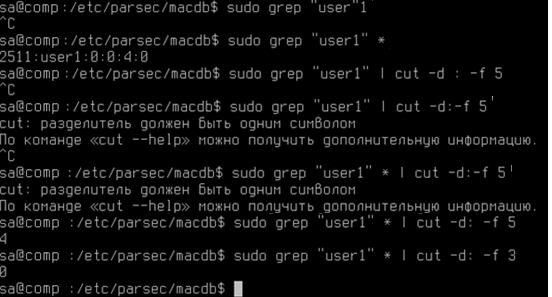


Рис. 10.

Проверка вывода команд на соответствие выводу графической утилиты

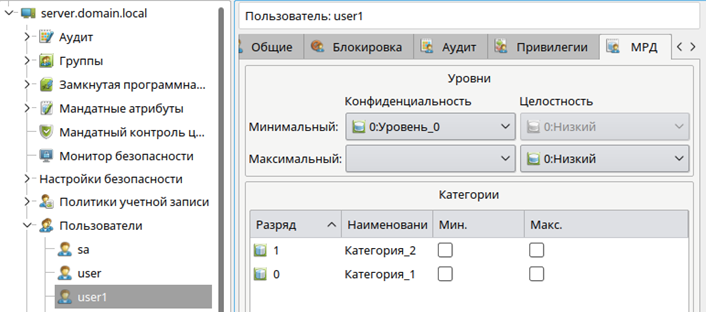


Рис. 11.

Создание новой иерархической категории

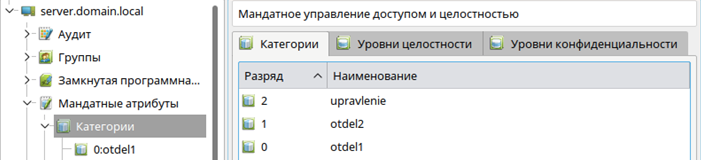


Рис. 12.

Ввод наименований

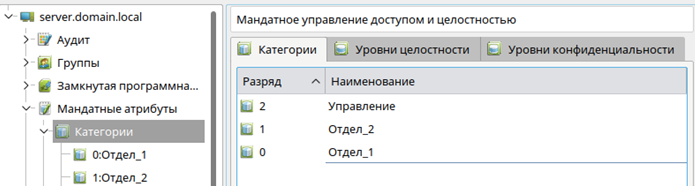


Рис. 13.

Изменить мандатный уровень доступа с использованием графической утилиты «Управление политикой безопасности», для этого выполнить 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».

Создание новой группы

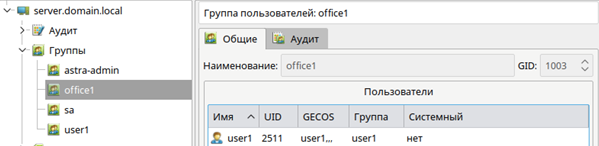


Рис. 14.

Создание новой учётной записи

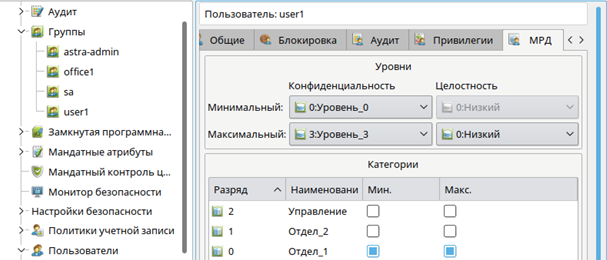


Рис. 15.

Выполнение пункта c

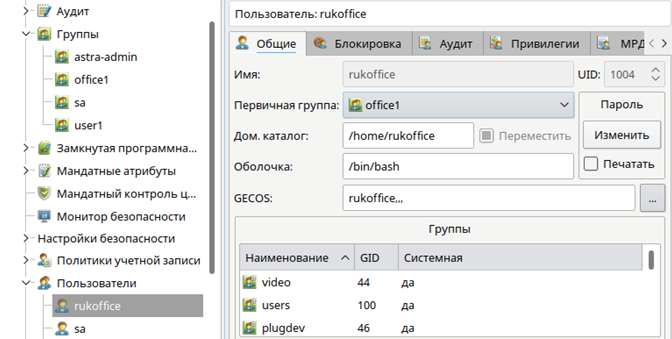


Рис. 16.

Выполнение пункта d

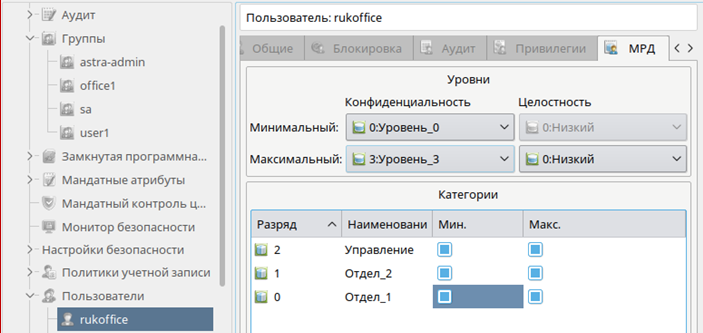


Рис. 17.

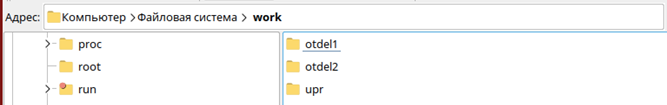
Структура каталогов 

Рис. 18.

1. При этом обеспечить 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*

Задание параметров мандатного и дискреционного управления доступом

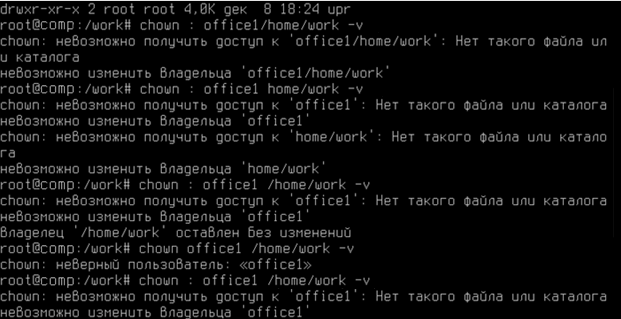


Рис. 19.

Листинг команд 14 пункта

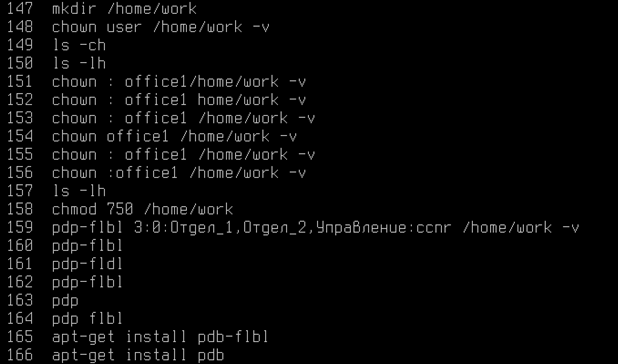


Рис. 20.

Листинг команд 14 пункта (продолжение)

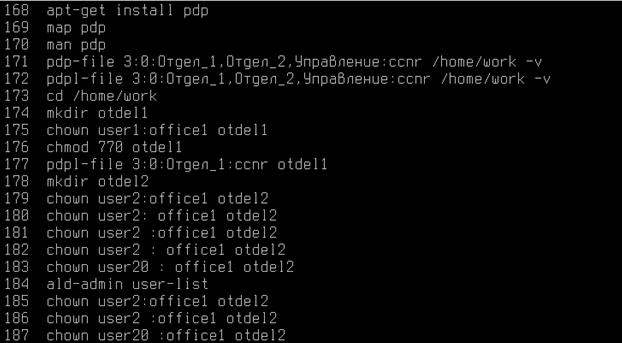


Рис. 21.

Листинг команд 14 пункта (продолжение) (продолжения)



Рис. 22.

Вывод

В ходе выполнения лабораторной работы была изучена мандатная система управления доступом Astra Linux к домену.

Тема 4. Мандатный контроль целостности в Astra Linux 1.6

**Четвертая часть**

**Мандатный контроль целостности в Astra Linux 1.6**

**Введение**

Мандатный контроль целостности (МКЦ) - это мощный механизм безопасности, который защищает систему от несанкционированных изменений и эксплуатации уязвимостей.

МКЦ реализован в Astra Linux 1.6 с помощью подсистемы безопасности Parsec.

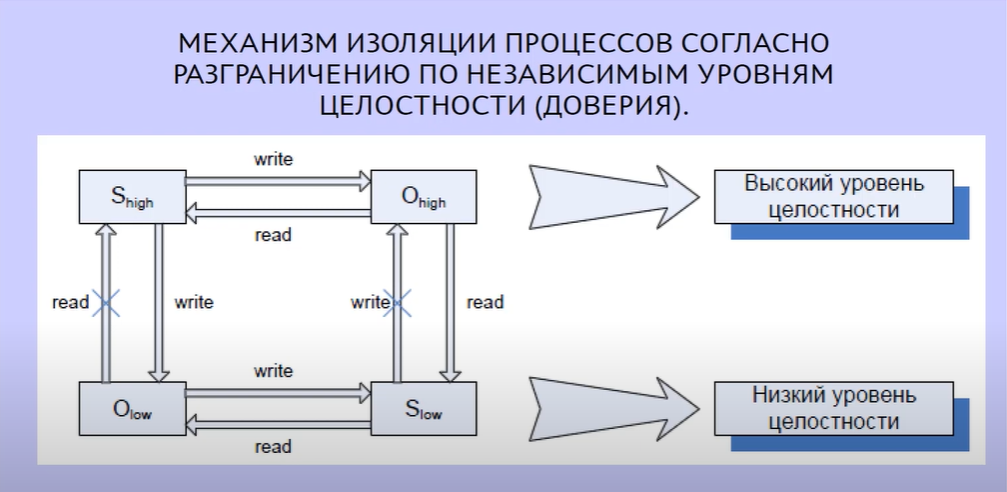
**Теоретическое обоснование**

Дополнительное ограничение доступа (DOS)\*\* Контролирует доступ пользователей к файлам и другим системным ресурсам. Однако DOS не управляет потоком информации и не предотвращает утечку данных.

Обязательное ограничение доступа (Court)\*\* Обеспечивает более детальный уровень контроля, основанный на уровнях конфиденциальности и категориях. MCC является частью этого парня и дополняет его.Как работает МКЦ



МКЦ использует концепцию уровней целостности. Объектам в системе (файлам, процессам и т.д.) присваиваются уровни целостности, которые определяют их важность для функционирования системы.

MCC не позволяет процессам с низким уровнем целостности изменять объекты с высоким уровнем целостности. Это предотвращает использование уязвимостей в приложениях с более высоким уровнем целостности.

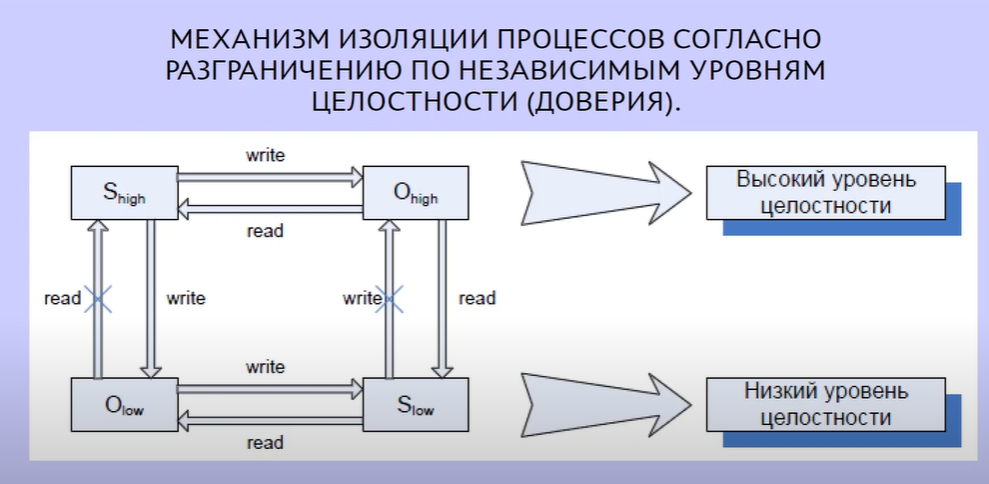
**Реализация в Astra Linux 1.6**

****

В Astra Linux 1.6 МКЦ используется для защиты приложений и их конфигурационных файлов.

Файлы изначально имеют максимальный уровень целостности.

Для включения МКЦ необходимо активировать защиту файловой системы в панели управления.



**Преимущества МКЦ**

Усложняет эксплуатацию уязвимостей нулевого дня.

Повышает безопасность системы путем управления информационными потоками.

Усложняет проведение атак через взлом приложений.

**Мониторинг и защита от эксплоитов**



Монитор Parsec отслеживает действия процессов с низким уровнем целостности. Если обнаруживается попытка создания или запуска процесса с высоким уровнем целостности, Parsec прибивает такой процесс.

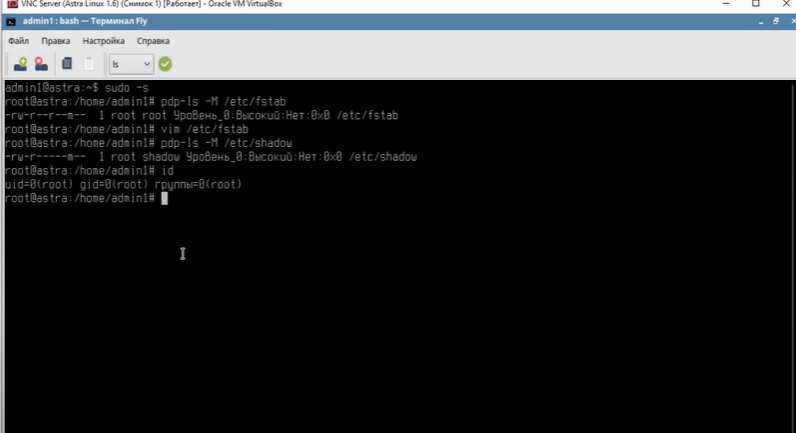
**Примеры работы МКЦ**



В Windows процессы с низким уровнем целостности не могут влиять на процессы с высоким уровнем, даже если они получают привилегии администратора.

В Astra Linux МКЦ защищает системные файлы и приложения от модификации неавторизованными пользователями или вредоносным ПО.

**Активация МКЦ**

****

Чтобы включить MCC, перейдите в Панель управления и включите защиту файловой системы.

После этого все файлы получат максимальный уровень контроля целостности.

**Ограничения МКЦ**

МКЦ не применяется к памяти и оперативной памяти.

Для внесения изменений в файлы с высоким уровнем целостности необходимо войти под соответствующим уровнем.

**Настройка МКЦ**

Уровни целостности и политики МКЦ можно настроить с помощью специальных утилит.

Рекомендации по настройке зависят от конкретной системы и приложений.

**Заключение**

MCC является важным инструментом для защиты Astra Linux1.6 от злоупотреблений и несанкционированных изменений. Его использование значительно повышает уровень безопасности системы и делает ее устойчивой к различным атакам.

Тема 5. Настройка механизма замкнутой программной среды

**Лабораторная работа №8 «Настройка механизма замкнутой программной среды»**

В лабораторной работе продемонстрирована организация замкнутой программной среды для пользователей на примере "user1" и "user2". Пользователям на компьютере организуется запуск ограниченного набора программ:

1. Проводник;
2. LibreOffice Writer;
3. LibreOffice Calc; 4) Internet Explorer; 5) Корзина.

Система Secret Net Studio позволяет сформировать модель данных для механизма замкнутой программной среды на основе сведений о запускавшихся программах из своего журнала безопасности. На основании этих данных формируются задания замкнутой программной среды для субъектов.

# ХОД РАБОТЫ

Я открыл меню настроек «Замкнутая программная среда» («Пуск → Все программы → Код безопасности → Secret Net Studio → Локальный центр управления») и открыл раздел «НАСТРОЙКИ → Замкнутая программная среда». Добавил себя в группу привилегированных пользователей.

Рис. 1. Окно «Локальный центр управления».

Я нажал кнопку «Применить»

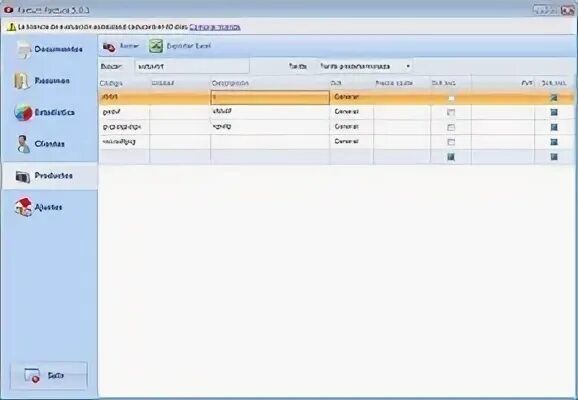


Рис. 2. Окно «Контроль программ и данных».

Я выбрал пункт «Новая модель данных» в меню «Файл». В появившемся диалоге «Настройка контроля по умолчанию» добавил выполнение «Предварительной очистки модели данных» и нажал «ОК».

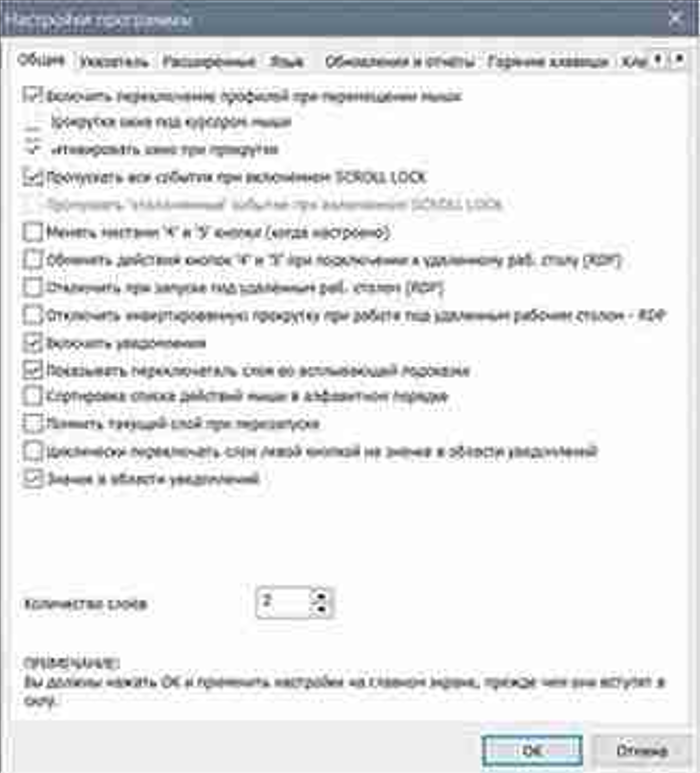


Рис. 3. Окно «Настройка контроля по умолчанию».

Программа начала подготовку ресурсов для использования с ZPS. После завершения подготовки автоматически запускается расчет критериев для ресурса. Я ждал окончания процедуры расчета. Я создал новое задание, выбрав в контекстном меню поля «Субъекты управления» пункт «Добавить задание → Новое».

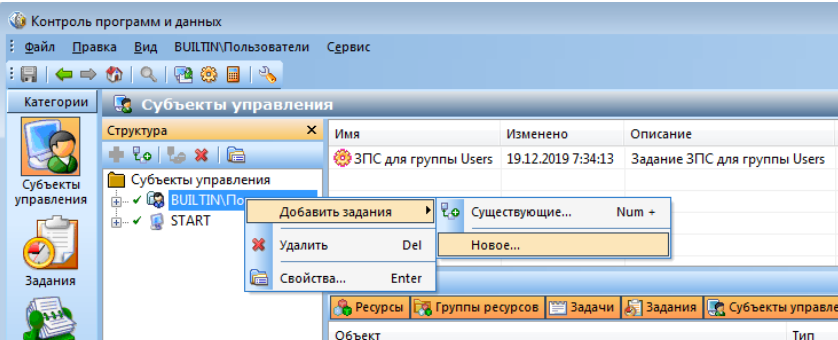


Рис. 4. Создание нового задания.

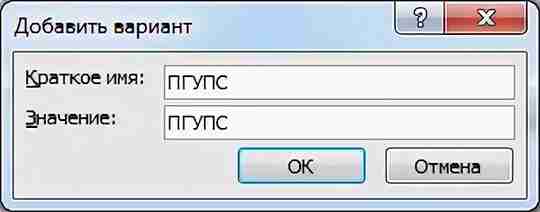
Я ввёл название ЗПС для пользователей и нажал кнопку «ОК».

Рис. 5. Окно «Создание нового задания на ЗПС».

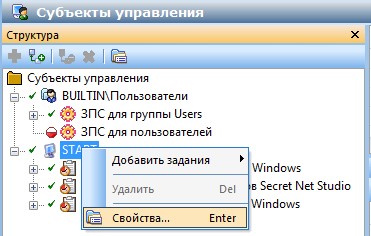
Я выбрал субъект управления «START» и в контекстном меню перешёл в «Свойства».

Рис. 6. Открытие свойств субъекта управления "START".

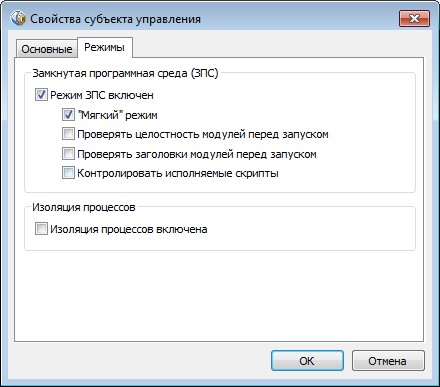
Я включил «Мягкий режим» ЗПС и нажал кнопку «ОК»

Рис. 7. Настройка режима ЗПС для субъекта управления "START".

Я сохранил модель и перезагрузил компьютер. Я вошел в систему как администратор и открыл журнал Secret Net Studio. Экспортируйте журнал во внешний файл и удалите его после экспорта. Я перезагрузил компьютер и вошел в систему под учетной записью "user1". Я запустил все программы, которые будут разрешены пользователю в будущем. Закройте сеанс и снова войдите в систему как администратор. Я открыл программу "Управление программами и данными". Чтобы настроить управление доступом пользователей, в контекстном меню выберите "Добавить задачу/группу" → "Создать группу регистрации".

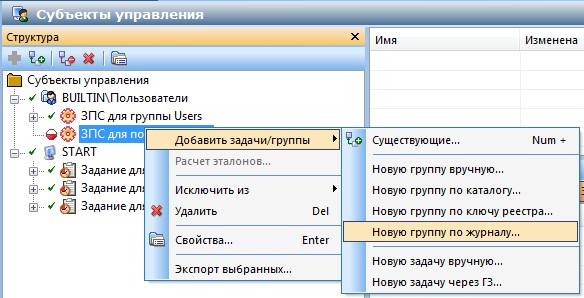


Рис. 8. Создание новой группы по журналу.

Я выбрал загружаемые модули и нажал кнопку «ОК».

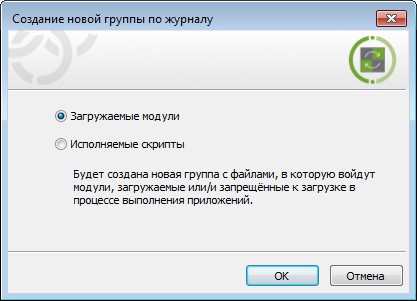


Рис. 9. Использование загружаемых модулей.

Я выполнил необходимые настройки в окне «Создание группы по журналу». В поле «Способ» указал «Из журнала Secret Net Studio», в поле «Пользователь» нажал «Найти» и выбрал «user1», в поле «Отчетный период» указал период запуска разрешённых программ для «user1».

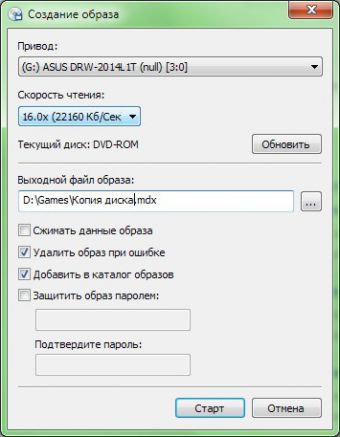


Рис. 10. Окно «Создание группы по журналу».

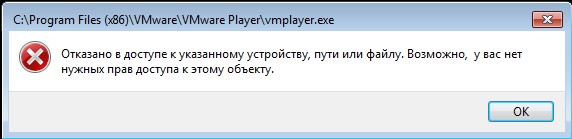
Я нажал кнопку «ОК» и сохранил модель данных. Вошёл в систему под учетной записью пользователя «user1» и убедился, что он может запускать только ограниченный набор программ: проводник, LibreOffice Writer, LibreOffice Calc, Internet Explorer, корзина.

Рис. 11. Сообщение об ошибки при попытке доступа к запрещенным программам.

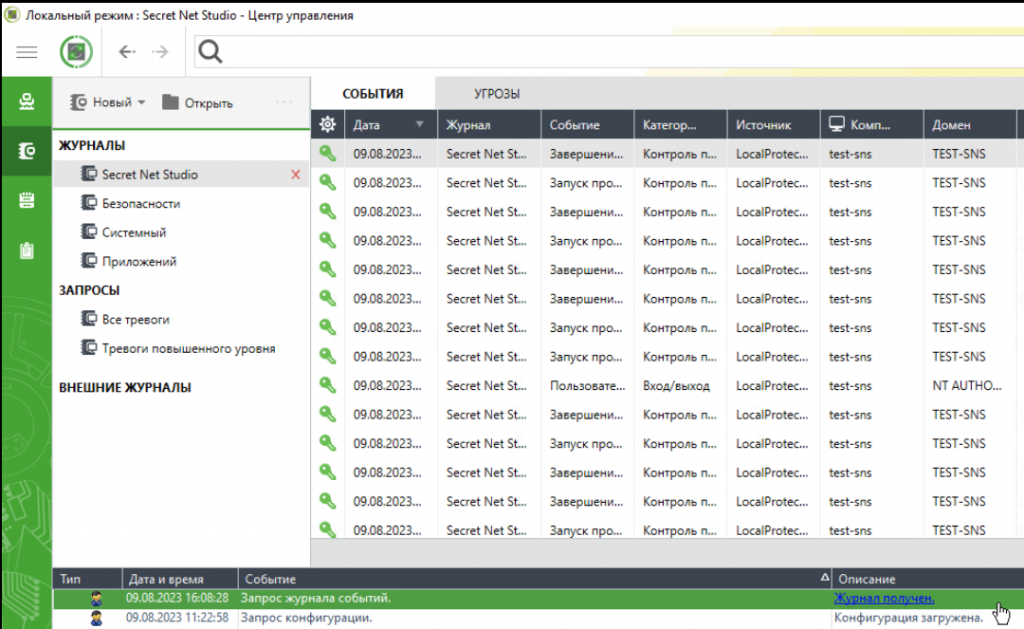
Я вошел в систему под учетной записью пользователя "user2" и подтвердил, что замкнутая программная среда работает и у него. Затем я вошел в систему как администратор и открыл секретный журнал Net Studio. Я ознакомился с записью в журнале с категорией "Закрытая программная среда".

Рис. 12. Журнал с фильтром по категории «Замкнутая программная среда».

Отключил механизм PPS. Я открыл программу "Управление программами и данными" и снял флажок "Включен режим GPS". Я закрыл окно программы и перезагрузил компьютер.

Тема 6. Установка и настройка сервера DNS

**Задание 6 Развертывание стенда. Настройка dns сервера**

**Цель:**научиться устанавливать сервер имён, добавлять зоны расширения имён, включать автоматическое обновление зон.

**Средства для выполнения работы:**

*∙***аппаратные**: компьютер с установленной ОС ***Windows XP***;

*∙***программные**: приложение ВМ: ***VirtualBox***; виртуальные машины: ***VM-1, VM-2***; установочные образы ОС: ***win98.iso.***

***Теоретические сведения***

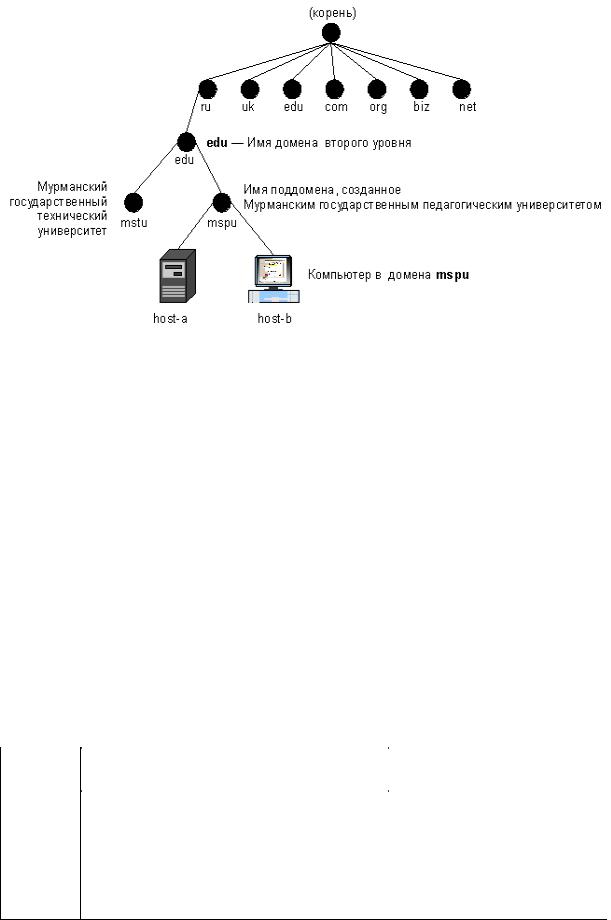
Система доменных имен (DNS) была первоначально определена в RFC (Request for Comment) 1034 и 1035. В этих документах определены следующие элементы, общие для всех программных реализаций DNS:

Пространство доменных имен DNS, которое определяет структурированную иерархию доменов, используемых для организации имен.;

Запись ресурса, которая сопоставляет доменное имя DNS с определенным типом информации о ресурсах, используемой для регистрации и разрешения имен в пространствах имен;

\* DNS-серверы, которые хранят записи ресурсов и отвечают на запросы клиентов;

DNS-клиент, также известный как система разрешения имен, запрашивает у сервера поиск и разрешение имени по типу записи ресурса, указанному в запросе.

40

**Рисунок 3. Пространство доменных имен**

Как показано на рисунке 3, доменное пространство имен DNS основано на концепции именованного доменного дерева. Каждый уровень дерева может представлять собой ветвь или лист дерева. Ветвь представляет собой уровень, на котором для определения семейства именованных ресурсов используется несколько имен. Таблица представляет собой единственное имя, используемое для указания конкретного ресурса на этом уровне.

В процессе разрешения имен важно, чтобы DNS-сервер действовал как DNS-клиент и запрашивал у другого сервера полное разрешение имени в запросе. Доменное имя DNS в дереве технически представляет собой домен. Однако обычно предполагается, что имя будет идентифицировано одним из 5 способов, в зависимости от уровня имени и способа его использования.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Например, доменное имя ***DNS***, зарегистрированное для образовательных учреждений (***edu.ru***), представляет домен второго уровня. Это имя состоит из двух частей (называемых метками), показывающих, что

42

оно находится на втором уровне сверху от корня или вершины дерева. Большинство доменных имен ***DNS***содержат две или большее число меток, каждая из которых задает новый уровень в дереве. Точки используются в именах для разделения меток.

*DNS предоставляет возможность интерпретировать полный путь к доменному имени DNS таким же образом, как вы интерпретируете полный путь к файлу или каталогу в окне командной строки. Например, путь к дереву каталогов может помочь вам указать точное местоположение файлов, которые хранятся на вашем компьютере. На компьютерах с Windows обратная косая черта (\) указывает на новый каталог, который ведет к точному местоположению файла. Эквивалентным символом в DNS является точка (. Указывает на новый уровень домена для каждого из имен.*

*Для DNS следующее полное доменное имя для узла может использоваться в качестве примера имени с несколькими levels:host-a.mspu.edu.ru*

*В отличие от имен файлов, при чтении полного доменного имени DNS-узла слева направо наиболее конкретная информация (DNS-имя хост-компьютера) выделяется из наиболее общей информации (конец - это указывает на корень дерева DNS-имен). В этом примере показаны четыре уровня доменов DNS, которые ведут от определенного местоположения host-a:*

*Домен mspu, для использования которого зарегистрировано имя компьютера host a;*

*Домен edu, соответствующий родительскому домену, который является корневым для поддомена Mspu;*

*Домен Ru соответствует домену верхнего уровня, используемому российской организацией, который является корневым для домена edu;*

*Конечная точка (.DNS) представляет собой стандартный разделитель, используемый для завершения доменного имени в дереве пространства имен DNS.*Работа запросов *DNS*

Если DNS-клиенту необходимо найти имя, используемое программой, он запрашивает у DNS-сервера соответствие этому имени. Каждое сообщение с запросом, отправляемое клиентом, содержит 3 типа информации, которые определяют вопрос, на который отвечает сервер:

43

Доменное имя DNS, указанное в виде полного доменного имени узла (FQDN);

Указанный тип запроса, который определяет либо тип записи ресурса, либо тип операции запроса;

Указанный класс доменного имени DNS.

Для DNS-серверов Windows этот класс всегда должен быть указан как Интернет-класс (IN).Например указанное имя может быть задано так host-a.mspu.edu.ru Адрес этого имени (A) - Тип запроса для поиска записей ресурсов. Запрос DNS может быть представлен в виде вопроса клиента, который состоит из следующих 2 пунктов parts:hostname.mspu.edu.ru ?"Когда клиент получает ответ от сервера, он считывает и интерпретирует запись ресурса A, содержащуюся в ответе, и распознает IP-адрес запрашиваемого компьютера по имени".

DNS-запросы используют несколько методов для сопоставления имен. Клиент может ответить на запрос, используя локально кэшированную информацию, полученную в предыдущем запросе. DNS-серверы могут отвечать на запросы, используя свой собственный кэш информации о записях ресурсов. Кроме того, DNS-сервер запрашивает другой DNS-сервер или связывается с ним в интересах запрашивающего клиента, точно соответствует имени и затем отправляет ответ клиенту. Этот процесс называется рекурсией.

В дополнение к этому клиент может самостоятельно попытаться установить контакт с дополнительными DNS-серверами для сопоставления имен. В этом случае клиент использует отдельный дополнительный запрос, основанный на ответе сервера на запрос. Этот процесс называется итерацией. Процесс запроса DNS выполняется в 2 этапа:

1.Запрос имени инициируется на клиентском компьютере и отправляется в систему сопоставления имен клиентов DNS;

2.Если вы не можете ответить на запросы на локальном уровне, вы можете при необходимости запросить совпадения имен у DNS-сервера.

Ниже более подробно описаны оба этапа процесса.**Локальная система разрешения имен**

На ранних этапах процесса доменные имена DNS используются программами на локальном компьютере. Затем запрос передается по следующему адресу

С помощью、

Клиентская служба DNS, которая сопоставляет данные с использованием локально кэшированной информации. Если запрошенное имя может быть разрешено, процесс завершается в ответ на запрос. Локальный кэш сопоставления имен может содержать информацию об именах из следующих 2 источников:

Если у вас есть локальный файл Hosts, все сопоставления имен и адресов из этого файла сохраняются в кэше при запуске службы DNS-клиента.;

Записи о ресурсах, полученные в ответ на запросы от

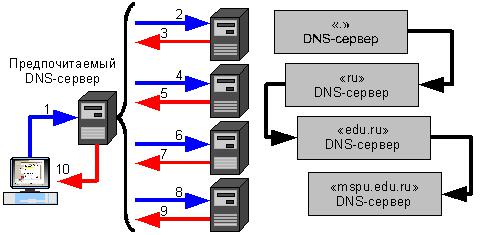
Предыдущих DNS-запросов, добавляются в кэш и сохраняются в нем в течение определенного периода времени.

Если клиенту не удается найти соответствие в кэше, процесс продолжается с помощью запроса разрешения имен от клиента к DNS-серверу.

Запросы к DNS-серверу

Клиент запрашивает основной DNS-сервер. Сервер, используемый на ранних этапах запроса от клиента к серверу, выбирается из глобального списка. Когда DNS-сервер принимает запрос, он сначала проверяет, может ли он выдать ответ для проверки подлинности на основе записей ресурсов, содержащихся в локальной зоне конфигурации сервера. Если запрошенное имя соответствует информации в записи ресурса локальной зоны, сервер использует эту информацию для предоставления ответа на проверку подлинности, который разрешает имя. Если запрошенная информация об имени отсутствует в зоне, сервер проверяет, можно ли разрешить имя, используя информацию из предыдущих запросов в локальном кэше. Если здесь найдено совпадение, сервер будет использовать эту информацию для ответа. В этом случае, если главный сервер может отправить запрашивающему клиенту подтверждение сопоставления из своего собственного кэша, запрос завершается. Если запрошенное имя не найдено на основном сервере

– Ни в кэше, ни в зоне - процесс выполнения запроса может использовать рекурсию для полного разрешения имени. В то же время другие DNS-серверы могут помочь с разрешением имени. По умолчанию служба DNS-клиента предлагает серверу использовать рекурсивный процесс для полного определения имени клиента перед отправкой ответа. В большинстве случаев dns-сервер настроен на поддержку рекурсивного процесса по умолчанию, как показано на рисунке 4.

45

**Рисунок 4. Процесс рекурсии при разрешении имени**

Для корректного выполнения рекурсии DNS-сервером требуется информация о контактах с другими DNS-серверами в пространстве доменных имен DNS. Такая информация может использоваться службой DNS для обнаружения других DNS-серверов, которые аутентифицируют корень дерева пространства доменных имен dns.Сервер перенаправления в записи резервного ресурса удостоверяет корневой домен и домен верхнего уровня домена в дереве пространства доменных имен DNS.

Этот процесс завершается возвращением клиенту положительного ответа. Однако запрос может возвращать и другие ответы, в частности ответы на проверку подлинности, ссылки и отрицательные ответы.

Подтверждение содержит список записей ресурсов, которые соответствуют запрошенной записи ресурса или запрошенному доменному имени DNS, а также типу записи, указанному в сообщении запроса.

Ответ для проверки подлинности возвращается клиенту с битом разрешения, указанным в сообщении dns, что указывает на то, что ответ был получен от сервера с прямыми разрешениями для запрашиваемого имени.

Ответ для проверки подлинности содержит дополнительные записи ресурсов, которые не указаны в имени или типе запроса. Если рекурсивный процесс, не поддерживается, это типа ответ возвращается клиенту. Эти записи должны быть в качестве исходных записей, которые могут быть использованы

Клиентом.

Используйте итерацию для продолжения запроса. Если клиент может использовать итерацию, вы можете запустить дополнительные запросы, чтобы попытаться полностью разрешить имя.

Отрицательный ответ сервера может указывать на один из двух возможных результатов, которые сервер обработал с помощью имен в запросе и попытался рекурсивно подтвердить полностью.:

Сервер аутентификации ответил, что запрошенное имя не существует в пространстве имен DNS;

Сервер аутентификации ответил запрошенным именем

Он существует, но нет записи типа, указанного для этого имени.Система сопоставления имен передает результаты запроса в виде утвердительного или отрицательного ответа в запрашивающую программу и кэширует ответ. Итерации представляют тип сопоставления имен, используемый ***DNS***-клиентами и серверами при выполнении следующих условий:

∙клиент запрашивает использование рекурсии, но рекурсия отключена на ***DNS***-сервере.

∙клиент не запрашивает использование рекурсии при запросе к

***DNS***-серверу.

Итерационный запрос от клиента сообщает DNS-серверу, что клиент ожидает от DNS-сервера наиболее точный ответ немедленно без обращения к другим DNS-серверам. Когда используются итерации, DNS- сервер отвечает клиенту о запрошенных именах на основании собственной информации о пространстве имен. Например, если DNS-сервер в интрасети получает запрос от локального клиента для имени www. ru, он может возвратить ответ из кэша имен. Если в данный момент запрошенное имя не сохраняется в кэше сервера, то сервер может ответить предоставлением ссылки – т. списка записей ресурсов других DNS- серверов, которые ближе к имени, запрошенному клиентом. Когда предоставляется ссылка, DNS-клиент принимает на себя ответственность за продолжение итерационных запросов на сопоставление имени к другим указанным в конфигурации DNS-серверам.Например, в наиболее общем случае ***DNS***-клиент может расширить область поиска до серверов корневого домена в Интернете в попытках обнаружить удостоверяющие ***DNS***-серверы для домена ***ru***. После установления контакта с корневыми серверами Интернета клиент может получить от них дальнейшие итерационные ответы, указывающие на фактические ***DNS***-серверы Интернета для домена ***edu.ru***. Когда клиенту предоставляются записи для этих ***DNS***-серверов, он может отправить дальнейший итерационный запрос внешним ***DNS***-серверам ***edu***в Интернете, которые могут дать определенный и удостоверяющий ответ. При использовании итераций ***DNS***-сервер может также содействовать в запросе на сопоставление имени, предоставив клиенту собственный наиболее точный ответ. Для большинства итерационных запросов клиент использует локальный список ***DNS***-серверов для обращения к другим серверам имен в пространстве имен ***DNS***, если его собственный основной ***DNS***-сервер не может сопоставить имя в запросе.

DNS-серверы используют рекурсивные и итеративные методы обработки для сбора значительных объемов информации о названиях DNS. Эти приобретенные знания впоследствии скрываются на сервере. Механизм caching позволяет ускорить сравнение часто доступных имен DNS в последующих запросах, тем самым существенно уменьшая трафик запросов DNS в сети. Во время рецидивирующих запросов DNS, инициированных клиентами, серверы временно хранят записи ресурсов в своих кешах. Эти кеш-ресурсные записи включают информацию, полученную с аутентифицирующих серверов DNS, относящуюся к конкретным названиям домена DNS. Такое накопление происходит во время итериального поискового процесса.

После завершения повторного запроса на хранение потребностей клиента, DNS-серверы могут использовать скриншоты ресурсов для предоставления ответов, когда последующие клиенты подают новые запросы, связанные с этими скриншотами.При кэшировании информации значение срока жизни применяется ко всем кэшированным записям ресурсов. Пока не истек срок жизни кэшированной записи ресурса, ***DNS***-сервер может продолжать кэшировать и снова использовать запись ресурса при ответах на соответствующие запросы клиентов. Значения срока жизни кэширования, используемые записями ресурсов в большинстве конфигураций зон, назначаются в параметре ***Мин. срок жизни TTL (по умолчанию)***, который задается в начальной записи зоны. По умолчанию задается значение минимального срока жизни 3600 секунд (1 час), но это значение может быть изменено, но могут также задаваться и отдельные значения срока жизни для каждой записи ресурса.

48

**Обратный просмотр**

В большинстве операций просмотра ***DNS***-клиенты обычно выполняют *прямой просмотр*, т. е. поиск, основанный на имени ***DNS***другого компьютера, сохраненного в записи ресурса адреса (A). В этом типе запроса в качестве данных для ответа на запрос ожидается ***IP***-адрес. ***DNS***также обеспечивает возможность *обратного просмотра*, в котором клиенты используют известный ***IP***-адрес для поиска имени компьютера по этому адресу. Обратный просмотр фактически является формой вопроса типа:*«Можете ли вы сказать мне имя****DNS****компьютера, который использует IP-адрес 192.168.1.20?».*

Система доменных имен (DNS) изначально не была разработана для удовлетворения запросов такого характера. Значительный вызов возникает при попытке поддерживать запросы обратной связи из-за различий в организации и индексировании DNS и IP-адресов. Если бы поиск потребовал проходить через любое доменное пространство DNS, обработка такого запроса оказалась бы непрактически медленной, что сделало бы его неэффективным.Чтобы разрешить эту проблему, в стандартах ***DNS***был определен и зарезервирован специальный домен в пространстве имен ***DNS***Интернета, ***in-addr.arpa***, обеспечивающий практичный и надежный способ выполнения обратных запросов. Чтобы создать обратное пространство имен, поддомены в домене ***in-addr.arpa***формируются с помощью обратного упорядочения чисел в точечно-десятичной нотации ***IP***-адресов. Такое обратное упорядочение доменов для каждого октета необходимо, поскольку в отличие от имен ***DNS***, для которых ***IP***-адреса читаются слева направо, здесь интерпретация выполняется в обратном порядке. Когда ***IP***- адрес читается слева направо, информация анализируется от наиболее общей (***IP***-адрес сети в левой части адреса) до наиболее конкретной (***IP***- адрес узла в последнем октете). По этой причине порядок октетов ***IP***- адреса должен быть обращен при построении дерева домена ***in-addr.arpa***. ***IP***-адреса дерева ***DNSin-addr.arpa***могут делегироваться организациям, которым назначается ограниченный набор ***IP***-адресов в границах определенных для Интернета классов адресов. И, наконец, для дерева домена ***in-addr.arpa***, встроенного в ***DNS***, требуется определение дополнительного типа записей ресурсов – запись ресурса указателя (***PTR***). Такая запись ресурса используется для сопоставления в зоне обратного просмотра, обычно соответствующего записи ресурса именованного узла

49



(A) для имени ***DNS***компьютера в зоне прямого просмотра.

*Рисунок5*иллюстрирует обратный запрос, инициируемый ***DNS***- клиентом (***host-b***), которому требуется узнать имя другого узла (***host-a***) по его ***IP***-адресу 192.168.1.20.

**Рисунок 5. Обратный запрос**

Обратный запрос включает следующие этапы:

1.Клиент ***host-b***запрашивает ***DNS***-сервер о записи ресурса указателя (***PTR***), сопоставляющей IP-адрес 192.168.1.20 для

|  |  |
| --- | --- |
| имени | ***host-a.*** |
| *Поскольку* | *запрос относится к записям****PTR****, система* |

*сопоставления имен обращает адрес и добавляет имя домена****inaddr.arpa****в конец обращенного адреса. В результате образуется полное доменное имя узла (****20.1.168.192.in-addr.arpa.****), для которого будет проводиться поиск в зоне обратного просмотра;*

2.После обнаружения имени удостоверяющий ***DNS***-сервер для имени ***20.1.168.192.in-addr.arpa***может возвратить ответ с информацией записи ***PTR***. В этой информации содержится доменное имя ***DNS***узла ***host-a***, что приводит к завершению процесса обратного просмотра. *Необходимо помнить, что если запрошенное обратное имя не может быть возвращено****DNS****- сервером, можно использовать сопоставление имен****DNS****(либо рекурсию, либо итерации) для обнаружения****DNS****-сервера, который является удостоверяющим для зоны обратного просмотра и содержит запрашиваемое имя. В этом смысле процесс сопоставления имен при обратном просмотре аналогичен процессу прямого просмотра.*

**Инвертированные запросы**

*Обратные запросы, ранее предлагаемые в качестве компонента протокола Domain Name System (DNS), оказались застарелыми. Эти запросы используют нетрадиционные операции по запросу DNS и ограничены ограничениями предыдущих итераций NSLookup, инструмента командной линии, предназначенного для устранения проблем и проверки функциональности DNS.*

Служба ***DNS***распознает и принимает сообщения инвертированных запросов и отвечает на них с имитацией ответа на запрос.

**Динамическое обновление**

Механизм динамического обновления позволяет DNS-клиентам автоматически поддерживать и обновлять свои соответствующие ресурсные записи, синхронизируя с назначенным DNS-сервером, когда происходят изменения. Эта функциональность значительно снижает необходимость вручную управления зонами, особенно для пользователей, которые часто перемещают или используют Динамический протокол конфигурации хоста (DHCP) для получения адресов Интернет-протокола (IP), тем самым обеспечивая беспроводную связь и снижая административные нагрузки.Клиентские и серверные службы ***DNS***поддерживают использование динамических обновлений, как описано в документе ***RFC 2136(Dynamic Updates in the Domain Name System)***. Служба ***DNS***-сервер поддерживает включение и отключение динамических обновлений отдельно для каждой зоны на каждом сервере, настроенном для загрузки либо стандартной основной зоны, либо зоны, интегрированной в каталоги. Служба ***DNS***- клиент будет по умолчанию динамически обновлять свои записи ресурсов узла (A) в ***DNS***, когда была выполнена настройка для ***TCP/IP***.

Динамические обновления обычно запрашиваются, когда изменяется имя ***DNS***или ***IP***-адрес компьютера. Например, для клиента с именем ***oldhost***в окне ***Свойства системы***заданы следующие имена:

|  |  |
| --- | --- |
| **Имя компьютера** | ***oldhost*** |
| **Доменное DNS-имя компьютера** | ***mspu.edu.ru*** |
| **Полное имя компьютера** | ***oldhost. mspu.edu.ru*** |

В этом примере в конфигурации компьютера нет доменных имен ***DNS***, специфических для подключения. В дальнейшем компьютер переименовывается из ***oldhost***в ***newhost***, в результате имена изменяются следующим образом:

|  |  |
| --- | --- |
| **Имя компьютера** | ***newhost*** |
| **Доменное DNS-имя компьютера** | ***mspu.edu.ru*** |
| **Полное имя компьютера** | ***newhost.mspu.edu.ru*** |

После изменения имени в окне ***Свойства системы***отображается

51

приглашение перезагрузить компьютер. Когда при перезагрузке компьютер запускает ОС, служба ***DHCP***-клиент выполняет следующие действия для обновления ***DNS***:

1.Служба ***DHCP***-клиент отправляет запрос для типа начальной записи зоны (**SOA**) с использованием доменного имени ***DNS***компьютера. Клиентский компьютер использует текущее полное доменное имя узла компьютера (в данном случае ***newhost.mspu.edu.ru***) как имя, указанное в этом запросе;

2.Удостоверяющий ***DNS***-сервер зоны, содержащей полное доменное имя узла клиента, отвечает на запрос типа ***SOA***;

3.После этого служба ***DHCP***-клиент пытается установить контакт с

основным ***DNS***-сервером:

*Клиент обрабатывает ответ на запрос****SOA****для его имени, чтобы определить****IP****-адрес****DNS****-сервера, удостоверенного как основной сервер, для принятия его имени. Далее он выполняет такую последовательность шагов, необходимых, чтобы установить контакт и динамически обновить его основной сервер.*

−клиент отправляет запрос на динамическое обновление основному серверу, определенному в ответе на запрос **SOA**.

*Если обновление выполняется успешно, другие действия не предпринимаются;*

−при отказе на обновление клиент отправляет запрос типа **NS**(о серверах имен) для зоны, имя которой указано в записи **SOA**;

−когда клиент получает ответ на этот запрос, он отправляет запрос **SOA**на первый ***DNS***-сервер, перечисленный в ответе;

−после разрешения имен в запросе ***SOA***клиент отправляет динамическое обновление серверу, указанному в возвращенной записи ***SOA***. *Если обновление выполняется успешно, другие действия не предпринимаются;*

−при отказе на обновление клиент повторяет запрос ***SOA***, отправляя его к следующему ***DNS***-серверу, перечисленному в ответе;

4.Как только находится основной сервер, который может выполнить обновление, клиент отправляет запрос на обновление, который обрабатывается сервером.

Содержимое запроса на обновление включает инструкции добавить

52

записи ресурсов A (и возможно ***PTR***) для имени ***newhost.mspu.edu.ru***и записи этих типов для ранее зарегистрированного имени ***oldhost.mspu.edu.ru***.

Сервер гарантирует, что обновления допускаются по запросу каждого клиента. Что касается стандартных первичных зон, то динамические обновления считаются неопределенными; поэтому клиентам рекомендуется воздерживаться от попыток обновления этих зон. Напротив, при интеграции зон в каталоги Active Directory обновления защищаются путем внедрения протоколов безопасности, адаптированных к конкретным каталогическим настройкам.

Периодические обновления передаются или выполняются через запланированные интервалы. По умолчанию система начинает обновления каждые семь дней. Тем не менее, если данные в пределах зоны остаются неизменными после обновления, зона останется в своем существующем состоянии без записи каких-либо изменений. Обновления провоцируются только изменением реальных имен и адресов в пределах зоны или результатом дополнительных переносов зоны.**Безопасное динамическое обновление**

Безопасные обновления ***DNS***доступны только для зон, интегрированных в службу каталогов ***Active Directory***. После преобразования зоны в интегрированную становится возможным использование с консоли ***DNS***списков управления доступом. Можно добавлять пользователей и группы в списки или удалять их для указанной зоны или записи ресурса. Параметры безопасного динамического обновления для ***DNS***-серверов и клиентов по умолчанию обрабатываются следующим образом:

∙***DNS***-клиенты сначала предпринимают попытки выполнить небезопасные динамические обновления. При отказе на небезопасные обновления клиенты пытаются выполнить

безопасные обновления;

*Кроме того, клиенты используют политику обновления по умолчанию, которая позволяет им пытаться переписывать ранее зарегистрированную запись ресурса, если она специально не заблокирована условиями безопасности обновления.*

∙ после интегрирования зоны в службу каталогов ***Active Directory DNS***-серверам ***Windows Server 2003***по умолчанию разрешаются только безопасные динамические обновления.

53

*При использовании стандартного сохранения зон настройки по умолчанию службы****DNS****-сервер не разрешают динамические обновления зон. И для зон, интегрированных в каталоги, и для использующих стандартное сохранение в файлах можно изменить параметры зоны и разрешить динамические обновления. Это позволяет принимать любые обновления.*

При развертывании ***DNS***-серверов совместно с ***Active Directory***необходимо иметь в виду следующее:

*∙*служба ***DNS***требуется для обнаружения контроллеров доменов ***Windows Server 2003***. Служба сетевого входа в систему использует новые средства поддержки ***DNS***-серверов для обеспечения регистрации контроллеров доменов в пространстве доменных имен ***DNS***;

*∙****DNS***-серверы ***Windows Server 2003***могут использовать службу

каталогов ***Active Directory***для сохранения и репликации зон.

*При интегрировании зон в службу каталогов пользователи получают возможность использовать дополнительные средства****DNS****, такие как безопасные динамические обновления и средства устаревания и очистки записей.*

Способы интеграции ***DNS***со службой каталогов ***Active Directory***:

*∙*при установке ***Active Directory***на сервер выполняется повышение сервера до роли контроллера указанного домена. Когда данный процесс завершается, пользователю выводится приглашение указать доменное имя ***DNS***для домена ***Active Directory***, для которого выполняется присоединение и повышение сервера;

*∙*если в этом процессе удостоверяющий ***DNS***-сервер для

указанного домена либо не обнаруживается в сети, либо не поддерживает протокол динамического обновления ***DNS***, выводится приглашение установить ***DNS***-сервер. Такая возможность предоставляется, поскольку ***DNS***-серверу необходимо отыскать этот сервер или другие контроллеры домена для рядовых серверов домена ***Active Directory***.

После установки ***Active Directory***имеются две возможности сохранения и репликации зон при работе с ***DNS***-сервером на новом контроллере домена:

*∙*стандартное сохранение зоны с помощью файла в текстовом

54

*формате. Зоны, сохраняемые этим способом, размещаются в файлах с расширением****DNS****, которые сохраняются в папке****systemroot\System32\Dns****на каждом компьютере, на котором выполняется****DNS****-сервер. Имя файла зоны соответствует имени, которое пользователь выбрал для зоны при ее создании, например,****mspu.edu.ru.dns****, если именем зоны является****mspu.edu.ru.dns****;*

∙сохранение зон, интегрированных в службу каталогов, с помощью базы данных ***Active Directory***. *Зоны, сохраняемые таким образом, размещаются в дереве****Active Directory****под разделом каталога домена или приложения. Каждая зона, интегрированная в службу каталогов, сохраняется в контейнере****dnsZone****, который идентифицируется по имени, выбранному пользователем при ее создании.*

**Преимущества интеграции с *Active Directory***

В целях эффективного использования служб директории Active Directory в DNS-базируемых сетях очень целесообразно использовать встроенные функции, предлагающие следующие преимущества:

Бесплатная интеграция с несколькими основными серверами и улучшенные возможности безопасности, заложенные в функциях Active Directory.

В отличие от традиционных стандартных моделей хранения зоны, которые базируются исключительно на одном первичном сервере, наш подход использует мультисерверную архитектуру для динамических обновлений DNS. В рамках этой программы каждый авторитарный DNS-сервер, в том числе доменные контроллеры, предоставляющие DNS-услуги, служит основным источником для своей соответствующей зоны. Основная копия зоны хранится в базе данных Active Directory, обеспечивая непрерывную обработку запросов обновления зоны клиента DNS даже в случае недоступности основного сервера. Принимая этот подход, администраторы сети могут обеспечить оптимальную производительность и надежность своей инфраструктуры сервисов директоров.

***Directory***, которая полностью реплицируется на все контроллеры домена, зона может обновляться любыми ***DNS***-серверами, выполняющимися на любом контроллере домена.При использовании модели ***Active Directory***с несколькими главными серверами любой из основных серверов для зоны, интегрированной в каталоги, может обрабатывать запросы от ***DNS***-клиентов на обновление зоны, пока контроллер домена является доступным по сети. Кроме того, при использовании зон, интегрированных в службу каталогов, можно с помощью списков управления доступом защитить объект-контейнер ***dnsZone***в дереве каталогов. Это средство обеспечивает дифференцированный доступ к зоне или к конкретной записи ресурса в зоне. Например, список управления доступом для записи ресурса в зоне можно ограничить так, чтобы разрешить динамические обновления только указанному компьютеру клиента или группе безопасности, например, группе администраторов домена. Это средство безопасности недоступно для стандартных основных зон. Необходимо отметить, что при преобразовании зоны к типу интегрированной

вслужбу каталогов настройка по умолчанию для обновлений зоны изменяется, и разрешаются только безопасные обновления. Кроме того, при использовании списков управления доступом на объектах ***Active Directory***, относящихся к ***DNS***, списки управления доступом могут применяться только к службе ***DNS***- клиент;

***∙***репликация и синхронизация зон с новыми контроллерами домена выполняется автоматически при каждом добавлении нового контроллера в домен ***Active Directory***. Хотя службу ***DNS***можно выборочно удалять с контроллеров домена, зоны, интегрированные в службу каталогов, всегда сохраняются на каждом контроллере домена. В результате сохранение и управление зонами не является дополнительным ресурсом. Кроме того, способы синхронизации информации, сохраняемой

вслужбе каталогов, обеспечивают повышение быстродействия по сравнению со стандартными способами сохранения обновлений зон, которые могут потенциально потребовать передачи зоны целиком;

56

∙за счет сохранения баз данных зон ***DNS***в ***Active Directory***имеется возможность рационализировать репликацию баз данных в сети. Когда пространство имен ***DNS***и домены ***Active Directory***сохраняются и реплицируются независимо, необходимо обеспечить планирование и администрирование каждого из них в отдельности. Например, при одновременном использовании стандартного сохранения зон ***DNS***и службы каталогов ***Active Directory***необходимо обеспечить структуру, реализацию, тестирование и управление для двух различных топологий репликации баз данных. Одна топология требуется для репликации данных из каталогов между контроллерами домена, а другая топология может потребоваться для репликации баз данных зон между ***DNS***-серверами.Это приведет к дополнительным трудностям при планировании и разработке структуры сети с учетом ее естественного роста. За счет интеграции сохранения информации ***DNS***появляется возможность унифицировать вопросы управления и репликации для ***DNS***и ***Active Directory***, объединяя их в единое административное целое;

∙репликация каталогов выполняется быстрее и эффективнее, чем стандартная репликация ***DNS***. Поскольку репликация ***Active Directory***выполняется на уровне отдельных свойств, распространяются только необходимые изменения. При этом для зон, интегрированных в службу каталогов, используется и отправляется меньший объем данных.

***Выполнение работы***

**Задание 1. Установка сервера *DNS*:**

1.1.Запустил виртуальную машину ВМ ***VM-2***.

1.2.Подключилл к виртуальной машине образ установочного диска ***win2003.iso***.

***1.3.Открыл диалоговое окно Управление данным сервером (Пуск/Администрирование/Управление Данным Сервером).***

1.4.Активизировал установку сервера имен:

−запустил мастер добавления ролей сервера, кнопкой ***Добавить или удалить роль***;

57

−ознакомился с информацией мастера и продолжил установку кнопкой ***Далее***;

−указал тип установки Особая конфигурация и продолжите установку кнопкой ***Далее***;

−выбрал в списке доступных ролей сервера пункт ***DNS***-сервер.

Нажал ***Далее***;

−ознакомился с сводкой выбранных параметров и продолжите

установку кнопкой ***Далее***.

*После завершения установки сервера имен, автоматически запустился****Мастер настройки DNS-сервера****.*

1.5.Выполнил первоначальную настройку ***DNS***-сервера с помощью мастера:

−ознакомился с информацией мастера (***Далее***);

− ознакомился с предлагаемыми вариантами настройки сервера;

−выбрал создание зоны прямого просмотра для небольших сетей, соответствующей радиокнопкой (***Далее***);

−указал свой ***DNS***-сервер в качестве ***DNS***-сервера, который будет обслуживать зону прямого просмотра, радиокнопкой *Управление зоной выполняется этим сервером*. Продолжил установку кнопкой ***Далее;***

−задал имя зоны, например ***example.edu.ru***и продолжил установку кнопкой ***Далее***;

−ввел в поле ***Создать новый файл***имя файла в котором будет храниться конфигурация зоны. Продолжил установку кнопкой ***Далее***;

−запретил динамическое обновление соответствующей радиокнопкой и продолжил настройку кнопкой ***Далее***;

−отказался от пересылки запросов на другие ***DNS***-сервера, выбрав радиокнопку *Нет, не пересылать запросы*(***Далее***);

− ознакомился с информацией о недоступности корневых сертификатов и щелкнул ***ОК***;

−завершил первоначальную настройку ***DNS***-сервера кнопкой

***Готово.***

**Задание 2. Настройка сервера *DNS*:**

2.1.Переключился в диалоговое окно ***Управления данным сервером***.

2.2.Перешел в управление ***DNS***-сервером, кнопкой ***Управление этим***

58

***DNS-сервером.***

*Появилось окно консоли администрирования, с открытой оснасткой управления****DNS****-сервером*

2.3.Настроил зону прямого просмотра:

***−***открыл диалоговое окно свойств созданной ранее зоны  **(*контекстное меню/Свойства*)**;

***−***настроил очистку и обновление содержимого ***DNS***-сервера:

***−***открыл окно очистки, кнопкой ***Очистка***;

***−установил флажок Удалять устаревшие записи ресурсов;***

***−установил интервал блокирования–1 день;***

***−установил интервал обновления–7 дней;***

***−***подтвердил изменения кнопкой ***ОК***;

***−установил срок жизни (TTL) записи–2 часа:***

***−перешел на вкладку Начальная запись зоны (SOA);***

***−ввел в поле Срок жизни (TTL) записи–0: 2: 0: 0;***

***−установил желаемые интервалы для обновления и повтора–не менее 1 и не более 15 минут;***

***−***завершил настройку кнопкой ***ОК***.

2.4.Создал запись в ***DNS***-сервере соответствующую физическому компьютеру:

***−***открыл диалоговое окно **добавления новых узлов (*контекстное меню /Создать узел (А)*)**;

***−****ввел в поле****Имя****–<user228>*

***−***ввел в поле ***IP-адрес***–*192.168.1.1*

***−***завершил добавление кнопкой ***Добавить***.

2.5.Создал новую основную зону обратного просмотра:

***−открыл мастер создания новых зон (контекстное меню Зоны обратного просмотра/Создать новую зону);***

***−***ознакомился с информацией мастера и щелкните ***Далее***;

***−указал тип создаваемой зоны–Основная зона (Далее);***

***− указал код сети–192.168.1 (Далее);***

*Поскольку IP-адреса создаваемой сети к сети класса C, то в IP адресах сети будет меняться только последний разряд адреса.*

***−***указал имя файла для зоны по умолчанию и продолжите установку кнопкой ***Далее***;

***−***установил запрет динамических обновлений (***Далее***);

Тема 7. Служба каталогов Astra Linux Directory

# 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

[https://disk.yandex.ru/d/87pkCdkO...](https://disk.yandex.ru/d/87pkCdkOgI-y5A) - УП Сидлеров

[https://disk.yandex.ru/d/0SV17Kvg...](https://disk.yandex.ru/d/0SV17KvgO9m2cg) - УП Ожигова