ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИРКУТСКОЙ ОБЛАСТИ «ЧЕРЕМХОВСКИЙ ГОРНОТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМ. М.И. ЩАДОВА»

РАССМОТРЕНО
на заседании ЦК
«Информатики и ВТ»
«04» февраля 2025 г.
«Протокол № 6
Председатель: Коровина Н.С.

УТВЕРЖДАЮ
Зам. директора
О.В. Папанова
« 26» мая 2025 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по практическим занятиям студентов

учебной дисциплины

ПМ.07 Соадминистрирование баз данных и серверов

09.02.07 Информационные системы и программирование

Разработал:
Плескач Т.А.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 54CE6FF6F2E941EC6571CFEA2EAFB5E4
Владелец: Сычев Сергей Николаевич
Действителен: с 23.08.2024 до 16.11.2025

2025 г.

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по практическим занятиям учебной ПМ.07 **«Соадминистрирование баз данных и серверов»** составлены в соответствии с учебным планом и рабочей программы дисциплины по специальности ***09.02.07 Информационные системы и программирование***

Цель проведения практических занятий: формирование практических умений, необходимых в последующей профессиональной и учебной деятельности.

Методические указания практических занятий являются частью учебно-методического комплекса по учебной дисциплине и содержат:

- тему занятия (согласно тематическому плану учебной дисциплины);
- цель;
- оборудование (материалы, программное обеспечение, оснащение, раздаточный материал и др.);
- методические указания (изучить краткий теоретический материал по теме практического занятия);
- ход выполнения;
- форму отчета.

В результате выполнения полного объема заданий практических занятий студент должен **уметь:**

- проектировать и создавать базы данных;
- выполнять запросы по обработке данных на языке SQL;
- осуществлять основные функции по администрированию баз данных;
- разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных;
- владеть технологиями проведения сертификации программного средства

При проведении практических работ применяются следующие технологии и методы обучения: чтение с маркировкой, «фишбон», информационные технологии, ментальные карты и т.д.

Оценка выполнения практических занятий

«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.

«Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.

«Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.

«Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.

В соответствии с учебным планом и рабочей программы ПМ.07 **«Соадминистрирование баз данных и серверов»** на практические (лабораторные) занятия отводится **54 часа.**

2. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

№ п/п	Тема практических занятий	Количество часов
МДК. 07.01 Управление и автоматизация баз данных		
1	Построение схемы базы данных	2
2	Построение схемы базы данных	2
3	Составление словаря данных	2
4	Составление словаря данных	2
5	Составление словаря данных	2
6	Разработка технических требований к серверу баз данных	2
7	Разработка требований к корпоративной сети	2
8	Разработка требований к корпоративной сети	2
9	Конфигурирование сети	2
10	Конфигурирование сети	2
11	Сравнение технических характеристик серверов	2
12	Формирование аппаратных требований и схемы банка данных	2
13	Установка и настройка сервера MySQL	2
14	Выполнение запросов к базе данных	2
15	Выполнение изменений в базе данных, создание триггеров	2
16	Создание запросов и процедур на изменение структуры базы данных	2
17	Работа с журналом аудита базы данных	2
18	Мониторинг нагрузки сервера	2
МДК.07.02 Сертификация информационных систем		
19	Настройка политики безопасности	2
20	Создание резервных копий базы данных	2
21	Восстановление базы данных	2
22	Восстановление носителей информации. Восстановление удаленных файлов	2
23	Мониторинг активности портов	2
24	Блокирование портов	2
25	Проверка наличия и сроков действия сертификатов	2
26	Разработка политики безопасности корпоративной сети	2
27	Получение сертификата	2

3. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие№1

Тема: Построение схемы базы данных
Цель: отработать навыки по построению схемы базы данных
Оборудование: тетрадь, ручка, ПК
Методические указания: выполните задания
Ход выполнения:
Задание 1.
В соответствии с заданием

1. Обследовать предметную область.
2. Выявить пользователей базы данных.

3. Определить информационные потребности пользователей, сформулировать функции приложения.

4. Описать входную и выходную информацию.

5. Определить ограничения на предметную область.

ГИБДД города производит регистрацию автомобилей. Инспектора дорожно-патрульной службы следят за безопасностью дорожного движения. В случае нарушения правил дорожного движения к водителям применяются меры взысканий. Виды нарушений и меры взысканий определяются Кодексом об административных правонарушениях.

Необходимо спроектировать базу данных ГИБДД, информация которой будет использоваться для подведения статистики совершаемых водителями нарушений правил дорожного движения; выявления водителей, многократно совершающих нарушения правил дорожного движения; определения наиболее аварийных районов города, размера штрафа за совершенное нарушение и др.

В БД должна храниться информация:

– о водителях: номер водительского удостоверения, Ф.И.О., адрес, телефон;

– автомобилях: номер автомобиля, марка, модель, цвет, год выпуска, дата регистрации в ГИБДД;

– нарушениях правил дорожного движения: код нарушения, вид нарушения (превышение скорости, управление автомобилем в состоянии алкогольного опьянения и др.), штраф за нарушение, предупреждение сделать или не сделать (Да/Нет), срок лишения права управления автомобилем (диапазон месяцев. Например, срок за управление автомобилем в состоянии алкогольного опьянения составляет 12 – 36 месяцев);

– взысканиях с водителей-нарушителей: код нарушения, дата и время нарушения, номер водительского удостоверения, район совершения нарушения, размер штрафа, оплачен штраф или не оплачен (Да/Нет), срок лишения права управления автомобилем (количество месяцев, определяемое инспектором по Кодексу об административных правонарушениях), личный номер инспектора ДПС, установившего нарушение.

При проектировании БД необходимо учитывать следующее:

– водитель может иметь несколько автомобилей. Автомобиль принадлежит одному водителю;

– водитель может получить несколько взысканий (он может совершить несколько нарушений). Взыскание применяется к одному водителю;

– одному и тому же нарушению могут соответствовать несколько взысканий (взыскания к водителям могут применяться за один и тот же вид нарушения). Взысканию соответствует единственное нарушение.

Кроме того следует учесть:

– каждый водитель обязательно имеет автомобиль (ГИБДД хранит сведения только о тех водителях, которые зарегистрировали автомобиль). Каждый автомобиль обязательно принадлежит водителю (ГИБДД хранит сведения только о зарегистрированных автомобилях);

– водитель не обязательно получает взыскания (водитель может не совершить ни одного нарушения). Каждое взыскание обязательно применяется к водителю;

– нарушению не обязательно соответствует взыскание (нарушение может ни разу никем не совершаться). Каждому взысканию обязательно соответствует нарушение.

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№2

Тема: Построение схемы базы данных

Цель: научиться создавать концептуальную схему базы данных для решения конкретной экономической индивидуальным вариантом.
Оборудование: тетрадь, ручка, ПК
Методические указания: выполните задания
Ход выполнения:
Задание 1.

1. Создать файл БД, присвоить имя БД в соответствии с предметной областью индивидуального варианта.
2. Установить пароль на БД.
3. Создать структуры таблиц БД.
4. Просмотреть видео-урок «Создание схемы данных в Microsoft Access».
5. Создать схему данных БД.
6. Заполнить таблицы данными.
7. Подготовиться к контрольным вопросам.
8. Продемонстрировать результат работы.

Контрольные вопросы:

1. Перечислить объекты Microsoft Access.
2. Что такое объект БД таблиц?
3. Какие существуют способы создания таблиц?
4. Как создается таблица в режиме Конструктора?
5. Назовите типы данных в Microsoft Access.
6. Какие могут быть заданы свойства для полей таблицы?
7. Что называют схемой данных?
8. Какие существуют типы связей между таблицами? Какие типы связи в вашей БД?

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

6. Дату проведения работы;
7. Цель работы;
8. Тему (название);
9. Ход работы, выполненный в тетради;
10. Файл выполненной работы.

Практическое занятие№3

Тема: Составление словаря данных
Цель: отработать навыки по составлению словаря данных
Оборудование: тетрадь, ручка, ПК
Методические указания: выполните задания
Ход выполнения:
Задание 1.

Для создания словаря данных с помощью Архивариуса (Documentor):

1. Откройте требуемую базу данных и выберите команду "Сервис, Анализ, Архивариус" (Tools, Analyze, Documentor).

2. Выберите вкладку с требуемым типом объектов, которые необходимо описать. Если выбрать вкладку "Все типы объектов" (All Object Types) и нажать кнопку "Выбрать все" (Select All), то можно создать описание для всех объектов базы данных.

3. Нажмите кнопку "Параметры" (Options) для вывода диалогового окна "Печать описания таблицы" (Print Table Definition). По умолчанию печатается наиболее подробное описание таблиц и индексов. Если база данных не имеет системы защиты, то можно сбросить флажок "Разрешения для пользователей и групп" (Permissions By User and Group), чтобы не выводить в отчете данные о правах доступа. Нажмите кнопку ОК для возврата в первое диалоговое окно Архивариуса (Documentor).

4. Выберите требуемые таблицы, нажимая кнопку "Выделить" (Select). При этом будет установлен флажок напротив имени указанной таблицы. Кроме того, можно выделить

объект, дважды щелкнув по его названию. Если необходимо документировать все таблицы базы данных, нажмите кнопку "Выбрать все" (Select All).

5. Выберите вкладку "Запросы" (Queries) для вывода запросов базы данных. Нажмите кнопку "Параметры" (Options) для вывода диалогового окна "Печать описания запроса" (Print Table Definition). Сбросьте флажок "Разрешения для пользователей и групп" (Permissions By Group and Group), чтобы не выводить в отчете данные о правах доступа, и задайте нужные параметры, чтобы не выводить данные, дублирующие информацию о полях таблиц. Нажмите кнопку" ОК.

6. Выберите запрос "Сведения о заказах", дважды щелкнув по его имени, и нажмите кнопку ОК для создания отчета длиной 13 страниц

7. Вскоре появляется окно предварительного просмотра "Описание объекта" (Object Definition). Обратите внимание на то, что отчет о трех объектах занимает одну страницу.

8. Нажмите на панели инструментов кнопку "Печать" (Print) для печати отчета либо щелкните по кнопке "Связи с Office" (Office Links) для создания файла в формате .RTF или .XLS

9. Нажмите на панели инструментов кнопку "Закрыть" (Close) либо дважды щелкните по кнопке системного меню для закрытия окна предварительного просмотра.

Документирование других объектов базы данных выполняется аналогичным образом. Можно вывести данные о самой базе данных, выбрав вкладку "Текущая база данных" (Current Database), или распечатать данные из выбранных форм, отчетов, макросов и модулей.

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№4

Тема: Составление словаря данных

Цель: Изучение стандарта IDEF1X, CASE-средства ERWin и получение практических навыков создания ER-модели и генерации базы данных

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1.

Построить ER-модель предметной области для выбранного варианта курсовой работы.

Создать логический уровень модели (режим отображения сущностей Display/Entity Level). Создать сущности при помощи линейки инструментов. Выбрав каждую сущность, задать для нее подробное описание на русском языке в редакторе "Entity Definition". Это описание появится в отчетах ERwin и может быть отображено на диаграмме.

Указать связи между сущностями. Описание связи вводится в редакторе "Editor/Relationship".

Перейти в режим задания атрибутов (Display/Atribute Level). В редакторе "Entity/Attribute" задать на русском языке имена ключевых и неключевых атрибутов. Для дочерних сущностей ключевые атрибуты, мигрирующие из родительской сущности, не указываются вручную.

Для атрибута "имя" сущности "служащий" укажем, что он является альтернативным ключом (будем считать, что у всех служащих уникальные имена/фамилии). После имен атрибутов, образующих альтернативный ключ, поместить указатель (AK1).

Для перехода к физическому уровню модели следует поставить в соответствие именам атрибутов идентификаторы таблиц, колонок и ограничений, удовлетворяющие правилам

целевой СУБД (обычно это означает использование латинских букв, цифр и некоторых специальных символов).

В редакторе "Database Schema" указать для каждой сущности соответствующее имя таблицы. Затем в редакторе "Attribute Definition" задать имена колонок таблиц, соответствующие атрибутам сущностей. ERwin и здесь обеспечивает миграцию имен колонок в подчиненные таблицы.

В редакторе "Relationship Definitions" указать физическое имя связи, которое соответствует имени ограничения (constraint), создаваемого ERwin в базе данных.

Выбрать целевую СУБД Access 97.

В редакторе Access Database Schema задать типы данных для колонок таблиц.

Перейти к созданию базы данных. Для этого выполнить команду “Access schema generation”. ERwin построит пакет SQL-предложений генерации базы данных.

Пакет SQL-предложений можно просмотреть (preview), распечатать, сохранить в файл (report), выполнить генерацию (generate).

Получить описание построенной модели в виде отчетов ERWin.

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№5

Тема: Составление словаря данных

Цель: отработать навыки по составлению словаря данных

Оборудование: тетрадь, ручка, ПК

Методические указания: ознакомьтесь с теоретической частью, выполните задания

Ход выполнения:

Теоретические сведения

Разработанная для предприятий среднего и большого бизнеса операционная система Windows Server 2003 Enterprise Edition позволяет развертывать легкодоступные и масштабируемые приложения на стандартном оборудовании. В результате пользователь получает высокопродуктивную инфраструктуру, оптимизированную для запуска ответственных бизнесприложений и служб. Общими приме-рами приложений, которые могут выполняться в ОС Windows Server 2003 Enterprise Edition, являются приложения для работы в сети и обмена сообщениями, системы инвентаризации и клиентских служб, системы баз данных, узлы электронной коммерции, файловые серверы и серверы печати. Данная операционная система обеспечивает высокую надежность, производительность и экономическую эффективность.

Все операционные системы семейства Windows Server 2003, включая Windows Server 2003 Enterprise Edition, являются многозадачными операционными системами, способными централизовано или распределено управлять различными наборами ролей, в зависимости от потребностей пользователей.

В операционных системах семейства Windows Server 2003 доступны следующие роли сервера:

- файловый сервер;
- сервер печати;
- сервер приложений;
- почтовый сервер;
- сервер терминалов;
- сервер удаленного доступа и VPN-сервера;
- контроллер домена;
- DNS-сервер (система доменных имен);

- DHCP-сервер (сервер протокола динамической настройки узлов);
- сервер потоков мультимедиа;
- WINS-сервер.

Файловый сервер предназначен для предоставления доступа к файлам и управления ими. Если планируется использовать дисковое пространство данного компьютера для хранения, управления и общего доступа к данным в виде файлов и доступных в сети приложений, то данный компьютер следует настроить как файловый сервер.

Настройка роли файлового сервера позволяет отслеживать и ограничивать дисковое пространство, доступное отдельным пользователям. Также можно задать, что необходимо регистрировать в журнале - превышение пользователем заданного дискового пространства или превышение пользователем указанного порога предупреждения (то есть отметки, при прохождении которой пользователь приближается к заданному для него или нее пределу использования дискового пространства). Для быстрого и безопасного поиска информации (как локального, так и в сети) можно использовать Службу индексирования. Настройка роли файлового сервера позволяет производить поиск в файлах различных форматов и на разных языках либо при помощи команды "Найти" в меню Пуск, либо при помощи страниц HTML, отображаемых обозревателем.

Сервер печати предоставляет доступ к принтерам и управляет им. Если планируется удаленное управление принтерами, управление принтерами при помощи Инструментария управления Windows (WMI) или печать с сервера или компьютера клиента на сервер печати, используя URL-адрес, то данный компьютер следует настроить как сервер печати.

После того как задана роль сервера печати, появляется возможность использования обозревателя для управления принтерами. Можно приостанавливать, возобновлять и удалять задания на печать, а также просматривать состояние принтера и заданий на печать. Также можно использовать созданный корпорацией Майкрософт инструментарий управления Windows (WMI), являющийся интерфейсом управления API, что позволяет отслеживать и контролировать все компоненты системы, как локальные, так и удаленные. Служба доступа к принтерам WMI позволяет управлять серверами печати, устройствами печати и прочими связанными с печатью объектами из командной строки. Служба доступа к принтерам WMI допускает использование сценариев Visual Basic (VB) для администрирования принтеров. Настройка роли серверами печати позволяет осуществлять печать с клиентов Windows XP на сервере печати под управлением Windows Server 2003, используя URL-адрес. Можно подключаться к общим принтерам сети путем установки их одним щелчком через Интернет. Имеется возможность установки драйверов с веб-узла

Сервер приложений представляет собой базовую технологию, обеспечивающую инфраструктуру ключа и службы, для приложений, находящихся в системе. Обычно серверы приложений содержат перечисленные ниже службы.

1. группировка ресурсов в пул (например, группировка в пул соединения базы данных и объекта);
2. управление распределенными транзакциями;
3. асинхронная связь программ, в основном при помощи очереди сообщений;
4. модель оперативной активации объекта;
5. интерфейсы автоматических веб-служб XML для доступа к рабочим объектам;
6. службы перемещения при сбое и определения работоспособности приложений;
7. интегрированная безопасность.

Операционные системы семейства Windows Server 2003 включают сервер приложений, содержащий все эти и другие службы для разработки, развертывания и рабочего цикла управления веб-службами XML, веб-приложениями и распределенными приложениями.

При настройке сервера приложений производится установка информационных служб Интернета (IIS) и других необязательных технологий и служб, таких как COM+ и ASP.NET. Работая вместе с информационными службами Интернета, операционные системы семейства Windows Server 2003 обеспечивают интегрированные, надежные, масштабируемые, безопасные и управляемые возможности веб-серверов для использования как в интрасети и в

Интернете, так и во внешних сетях. IIS является средством создания усиленной платформы соединений для динамических сетевых приложений

Почтовый сервер. Для предоставления пользователям служб электронной почты могут быть использованы Протокол Post-Office Protocol, версия 3 (POP3) и Протокол SMTP, являющиеся входящими в состав семейства операционных систем Windows Server 2003 компонентами. Служба POP3 использует стандартный протокол POP3 для извлечения почты и может быть использована вместе со службой SMTP для передачи почты. Если планируется поддерживать клиентские соединения с данным сервером POP3 и получать электронную почту на локаль-ный компьютер при помощи почтового клиента, поддерживающего POP3, то сле-дует настроить данный сервер как почтовый сервер.

После того как задана роль почтового сервера, появляется возможность выполнять следующие действия:

1. использовать службу POP3 для хранения учетных записей электронной почты и управления ими на почтовом сервере;

2. включить доступ пользователя к почтовому серверу, чтобы он мог получать электронную почту со своего локального компьютера при помощи поддерживающего протокол POP3 клиента электронной почты (например, Microsoft Outlook).

При помощи сервера терминалов можно предоставить одну точку установки, позволяющую нескольким пользователям получить доступ к любому компьютеру под управлением операционной системы Windows Server 2003. Пользователи могут запускать программы, сохранять файлы и использовать ресурсы сети с удаленного компьютера так, как если бы эти ресурсы были установлены на их компьютере.

После того как задана роль сервера терминалов, появляется возможность выполнять следующие действия:

1. проверять параметры расширенной настройки безопасности Internet Explorer;

2. централизованно разворачивать программы на одном компьютере;

3. обеспечить использование клиентами одной и той же версии программы.

Сервер удаленного доступа и VPN-сервера. Маршрутизация и удаленный доступ обеспечивают полнофункциональный программный маршрутизатор, удаленное соединение и соединение виртуальных частных сетей (VPN) для удаленных компьютеров. Также предлагаются службы маршрутизатора для локальной сети (LAN) и глобальной сети (WAN). Такой сервер позволяет удаленным или мобильным сотрудникам получить доступ к корпоративным сетям при подключении напрямую, либо через службы удаленного соединения, либо через Интернет при помощи VPN-соединения. Если планируется подключать удаленных сотрудников к офисной сети, сервер следует настроить как сервер удаленного доступа или VPN-сервер. Соединения удаленного доступа включают все обычно доступные пользователям локальной сети службы, включая службы совместного использования файлов и принтеров, доступ к веб-серверу и службу сообщений.

После того как задана роль сервера удаленного доступа или VPN-сервера, появляется возможность выполнять следующие действия:

1. контролировать время и место доступа пользователей в сеть;

2. использовать службы преобразования сетевых адресов (NAT) для компьютеров в сети;

3. создавать собственные сетевые решения, используя интерфейсы программирования приложений (API).

Контроллеры домена хранят данные каталога и управляют взаимодействием между пользователями и доменом, а именно: процессом входа в домен, проверкой подлинности и поиском в каталоге. Если планируется позволить службе каталогов Active Directory управлять пользователями и компьютерами, следует настроить данный сервер как контроллер домена.

После того как задана роль контроллера домена, появляется возможность выполнять следующие действия:

1. Сохранять данные каталога и делать их доступными для пользователей сети и администраторов. Служба каталога Active Directory, хранящая сведения об объектах сети, предоставляет возможность пользователям и администраторам легко находить эти данные,

обеспечивая логическую иерархическую организацию данных. Служба каталога Active Directory хранит сведения об объектах сети, например, имена, пароли, номера телефонов и тому подобные сведения и предоставляет возможность пользователям и администраторам той же сети, прошедшим проверку, получать доступ к этим сведениям.
2. Создавать дополнительные контроллеры домена в существующем домене для повышения доступности и надежности сетевых служб.
3. Повысить производительность сети между сайтами путем размещения контроллера домена на каждом сайте. Размещение контроллера домена в каждом сайте позволяет выполнять процесс входа в сеть внутри сайта без использования медленных подключений между сайтами.
4. DNS представляет собой службу разрешения имен TCP/IP, используемую в Интернете. Служба DNS позволяет компьютерам клиентов в сети регистрировать и сопоставлять понятные имена DNS. Если планируется сделать ресурсы сети доступными в Интернете, сервер следует настроить как DNS-сервер.
5. После того как задана роль сервера DNS, появляется возможность выполнять следующие действия:
6. Поддерживать записи в распределенной базе данных DNS и использовать эти записи для обработки DNS-запросов, созданных DNS-клиентами, таких как запросы имен веб-сайтов или компьютеров в сети или в Интернете.
7. Именовать и располагать сетевые ресурсы, используя понятные имена.
8. Контролировать разрешение имен для каждого сегмента сети и реплицировать изменения или внутри всей сети, или глобально в Интернете.
9. Уменьшить администрирование DNS за счет динамического обновления DNS-сведений.

DHCP-сервер. Протокол DHCP (Dynamic Host Configuration Protocol) - это стандарт протокола IP, разработанный для уменьшения сложности администрирования настроек адресов, используя компьютер сервера для централизованного управления IP-адресами и другими связанными подробностями настройки, используемыми в сети. Если планируется выполнять распределение адресов многоадресной рассылки и получать клиентские IP-адреса и связанные динамически параметры конфигурации, следует настроить сервер как DHCP-сервер.

После того как задана роль сервера DHCP, появляется возможность выполнять следующие действия.
1. Централизованно управлять IP-адресами и связанной с ними информацией. 2. Использовать DHCP для предотвращения конфликтов адресов, вызываемых использованием ранее назначенного IP-адреса при настройке нового компьютера в сети.
3. Настраивать серверы таким образом, чтобы поддерживать полный диапазон дополнительных значений настройки при назначении аренды адреса. Это позволит значительно снизить время, затрачиваемое на настройку и перенастройку компьютеров в сети.
4. Использовать при частом обновлении конфигурации клиентов (например, для пользователей с переносными компьютерами, часто меняющими расположение) процесс обновления аренды DHCP с целью гарантировать эффективное и автоматическое внесение нужных изменений клиентами за счет обращения непосредственно к DHCP-серверам.

Серверы потоков мультимедиа позволяют организации использовать службы Windows Media. С помощью служб Windows Media можно управлять содержимым этих служб, включая потоковые аудио- и видеоданные, архивировать его и доставлять через интрасеть или Интернет. Если планируется использовать цифровое мультимедиа в режиме реального времени через удаленное Интернет соединение или через локальную сеть, следует настроить сервер как сервер потоков мультимедиа.

После того как задана роль сервера потокового мультимедиа, появляется возможность выполнять следующие действия:
1. Транслировать цифровое видео в режиме реального времени посредст-вом сетей с низкой пропускной способностью, при удаленном соединении через Интернет с высокой пропускной способностью, а также через локальную сеть.

2. Транслировать потоковое цифровое аудио клиентам и другим серверам через Интернет или Интранет.

Серверы Windows Internet Name Service (WINS) отображают IP-адреса в NetBIOS имена компьютеров и NetBIOS-имена компьютеров обратно в IP-адреса. Используя серверы WINS в организации, можно осуществлять поиск ресурсов по имени компьютера, которое проще запомнить, вместо его IP-адреса. Если планируется отображать NetBIOS-имена в IP-адреса или централизованно управлять базой данных, сопоставляющей имена и адреса, следует настроить сервер как WINS-сервер.

После того как задана роль сервера WINS, появляется возможность выпол-нять следующие действия:

1. Уменьшить широковещательный трафик в подсетях, связанный с NetBIOS, разрешением клиентам, запрашивающим WINS-серверы, непосредст-венно искать удаленные системы.
2. Поддерживать клиентов, использующих ранние версии Windows и NetBIOS, в сети. Этим типам клиентов разрешается просматривать списки уда-ленных доменов Windows без необходимости наличия локальных контроллеров доменов в каждой подсети.
3. Поддерживать DNS-клиентов. Этим клиентам позволено искать ресурсы NetBIOS, если внедрено объединение просмотра WINS.

Сразу после первого входа в систему будет запущена утилита Управление данным сервером для настройки Windows Server 2003.

Она предназначена для быстрого запуска утилит, отвечающих за конфигурирование определенных служб. Чтобы данное окно не появлялось при каждом запуске Windows, установите флажок **Не показывать эту страницу при входе в систему** в нижней часть окна. Для дальнейшей настройки сервера вы всегда можете вызвать это окно из меню**Администрирование**.

Задание: ознакомиться и изучить роли серверов и их назначение. Представить отчет по проделанной работе.

Контрольные вопросы:

1. Какие роли доступны серверу Windows Server 2007?
2. Какие службы обычно содержат серверы?
3. Что такое Windows Server 2007?
4. Укажите основные этапы установки Windows Server 2007

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№6

Тема: Разработка технических требований к серверу баз данных

Цель: приобретение студентами практических навыков настройки управляющего, информационного сервера и сервера приложений.

Оборудование: тетрадь, ручка, ПК

Методические указания: ознакомиться с теоретическими сведениями**,** выполните задания

Ход выполнения:

Теоретические сведения

Каталог представляет собой иерархическую структуру, которая хранит сведения об объектах в сети. Служба каталогов, такая как Active Directory, обеспечивает возможность хранения данных каталога и доступа к этим данным сетевых пользователей и администраторов. Например, в Active Directory хранятся сведения об учетных записях пользователей, такие как имена, пароли, номера телефонов и тому подобные, к которым могут получать доступ другие пользователи той же сети, прошедшие проверку. Служба каталогов - одна из наиболее важных составных частей развитой компьютерной системы. Пользователи и

администраторы зачастую не знают точ-ных имен нужных им объектов, которые им в данный момент требуются. Они могут знать один или несколько их признаков или атрибутов (attributes) и могут послать запрос (query) к каталогу, получив в ответ список тех объектов, атрибуты которых совпадают с указанными в запросе. Служба каталогов позволяет найти любой объект по одному из его атрибутов. Служба каталогов Active Directory может быть установлена на серверах, работающих под управлением операционных систем Microsoft Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition и Windows Server 2003, Datacenter Edition. Она хранит сведения об объектах сети и упрощает поиск и использование этих сведений пользователям и администраторами. В Active Directory основой для логической, иерархической организации сведений каталога служит структурированное хранилище данных. Это хранилище данных, называемое также каталогом, содержит сведения об объектах Active Directory. В число этих объектов обычно входят общие ресурсы, такие как серверы, тома, принтеры, а также учетные записи сетевых пользователей и компьютеров.

Служба каталогов позволяет обеспечивать защиту информации от вмешательства посторонних лиц в рамках, установленных администратором системы. Группа безопасности интегрирована с Active Directory посредством проверки подлинности при входе в сеть и управления доступом к объектам в каталоге. В рамках одного входа в сеть администраторы могут управлять данными каталога и организацией через их сеть, а прошедшие проверку сетевые пользователи могут иметь доступ к ресурсам во всей сети. Администрирование, основанное на политике, облегчает управление даже самой сложной сетью.

В состав службы Active Directory входят также следующие элементы: Набор правил - схему, определяющую классы объектов и атрибуты, содержащиеся в каталоге, а также пределы и ограничения на экземпляры этих объек-тов, и формат их имен.

Глобальный каталог, содержащий сведения о каждом объекте в каталоге. Это позволяет пользователям и администраторам находить сведения каталога независимо от того, в каком из доменов каталог в действительности содержатся эти данные.

Механизм запросов и индексации, позволяющий опубликовывать и находить объекты и их свойства сетевым пользователям или приложениям. Службу репликации (тиражирования), распространяющую данные каталога по сети. Все контроллеры домена в домене участвуют в репликации и содержат полную копию всех сведений каталога для своего домена. Любое изменение данных каталога реплицируется во все контроллеры домена в домене.

Определим основные понятия, используемые для описания Active Directory.

Область действия (scope) Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать не-сколько объединенных сетей.

Active Directory, как и любая другая служба каталогов, является, прежде всего, пространством имен. Пространство имен - это такая ограниченная область, в которой может быть распознано данное имя.

Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует. Файловая система Windows образует пространство имен, в котором имя файла может быть поставлено в соответствие конкретному файлу. Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

Объект - это непустой, именованный набор атрибутов, обозначающий нечто конкретное, например, пользователя, принтер или приложение. Атрибуты содержат информацию, однозначно описывающую данный объект. Атрибуты пользователя могут включать имя пользователя, его фамилию и адрес электронной почты.

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имен. Однако, в отличие от объекта, контейнер не обозначает ничего конкретного - он может содержать группу объектов или другие контейнеры.

Термин дерево используется для описания иерархии объектов и контейнеров. Как правило, конечными элементами дерева являются объекты. В узлах (точках ветвления) дерева

располагаются контейнеры. Дерево отражает взаимосвязь между объектами или указывает путь от одного объекта к другому. Простой каталог представляет собой контейнер. Компьютерная сеть или домен тоже являются контейнерами.

Домен - это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows Server 2003. Active Directory состоит из одного или нескольких доменов. Применительно к отдельной рабочей станции доменом является сама рабочая станция. Границы одного домена могут охватывать более чем одно физическое устройство. Каждый домен может иметь свои правила защиты информации и правила взаимодействия с другими доменами. Если несколько доменов связаны друг с другом доверительными отношениями и имеют единую логическую структуру, конфигурацию и глобальный каталог, то говорят о дереве доменов. Несколько доменных деревьев могут быть объединены в лес.

Дерево доменов (дерево) состоит из нескольких доменов, которые имеют общую логическую структуру и конфигурацию и образуют непрерывное пространство имен. Домены в дереве связаны между собой доверительными отношениями. Active Directory является множеством, которому принадлежат одно или несколько деревьев.

Лесом называется одно или несколько деревьев, которые не образуют непрерывного пространства имен. Все деревья одного леса имеют общие логическую структуру, конфигурацию и глобальный каталог. В отличие от дерева, лес может не иметь какого-то определенного имени.

Узлом называется такой элемент сети, который содержит серверы Active Directory. Узел обычно определяется как одна или несколько подсетей, поддерживающих протокол TCP/IP и характеризующихся хорошим качеством связи. "Хорошее" качество связи в данном случае подразумевает высокую надежность и скорость передачи данных. Определение узла как совокупности подсетей позволяет администратору быстро и без больших затрат настроить топологию доступа и репликации в Active Directory и полнее использовать достоинства физического расположения устройств в сети. Когда пользователь входит в систему, клиент Active Directory ищет серверы Active Directory, расположенные в узле пользователя. Поскольку компьютеры, принадлежащие к одному узлу, в масштабах сети можно считать расположенными близко друг к другу, связь между ними должна быть быстрой, надежной и эффективной. Распознавание локального узла в момент входа в систему не составляет труда, так как рабочая станция пользователя уже знает, в какой из подсетей TCP/IP она находится, а подсети напрямую соответствуют узлам Active Directory.

В Windows Server 2003 Active Directory может быть интегрирована с DNS воедино. DNS представляет собой распределенное пространство имен, которое используется в Интернет и в котором именам отдельных компьютеров и служб ставятся в соответствие адреса, формируемые по правилам протокола TCP/IP. При создании контроллера домена, то есть сервера, управляющего работой Active Directory, мастер предлагает создать и настроить DNS-сервер. В этом случае запускается DNS-сервер и создается зона (контейнер, объединяющий несколько доменов в структуру с общими разрешениями на управление), одноименная с доменом.

Контроллеры домена хранят данные и управляют взаимодействием пользователей с доменом, включая процесс входа в домен, проверку подлинности и поиск в каталогах. Чтобы предоставить сетевым пользователям и компьютерам службу каталогов Active Directory, нужно настроить данный сервер как контроллер домена.

Для настройки сервера в качестве контроллера домена необходимо установить на данный сервер Active Directory. В мастере установки Active Directory доступны четыре параметра: можно создать дополнительный контроллер домена в существующем домене, контроллер домена для нового дочернего домена, контроллер домена для нового доменного дерева или новый контроллер домена для нового леса. Рассмотрим создание контроллера домена для нового леса.

Операционная система Windows Server 2003 позволяет настроить данный сервер как контроллер домена. Для этого нам необходимо выполнить следующие действия: открыть

оснастку "Управление данным сервером"; выбрать ссылку "Добавить или удалить роль"; на странице "Предварительные шаги" прочитать информацию о сетевых соединениях и подтвердить, что все они доступны; на странице "Параметры настройки" выбрать вариант "Особая конфигурация".

На экран будет выведена новая страница, представленная на рис. 20 - Роль сервера.

На этой странице мы выбираем из приведённого списка "Контроллер домена (Active Directory)" и нажимаем кнопку "Далее".

Появится страница "Сводка выбранных параметров" , в которой можно просмотреть и подтвердить выбранные параметры:

Для применения параметров, выбранных на странице "Сводка выбранных параметров", нажимаем кнопку "Далее".

Появится страница "Применение выбранных параметров", которая будет находиться на экране всё время до окончания установки и настройки Active Directory.

Автоматически запустится мастер установки Active Directory. Нажимаем кнопку "Далее" для продолжения. К этой странице можно вернуться из любого места мастера, пока не нажата кнопка "Готово" на последней странице.

Мастер установки выведет на экран страницу "Совместимость операционных систем", в которой приводится информация о влиянии усовершенствованных параметров безопасности в Windows Server 2003 на совместимость с предыдущими версиями Windows.

Прочитав сведения, приведённые на этой странице, нажимаем кнопку "Далее".

На странице "Тип контроллера домена" выбираем вариант "Контроллер домена в новом домене"

Для продолжения нажимаем кнопку "Далее".

На появившейся странице "Создать новый домен" выбираем вариант "Новый домен в новом лесу".

Для продолжения нажимаем кнопку "Далее". На странице "Новое имя домена" вводим полное DNS-имя нового домена.

Полное DNS-имя также называют полным доменным именем (FQDN). Домены Active Directory обозначаются с помощью DNS-имен и повторяют иерархическую структуру DNS. DNS-имена для леса Active Directory должны начинаться с зарегистрированного суффикса домена DNS, который зарезервирован организацией для использования в Интернете, например microsoft.com. Для продолжения нажимаем кнопку "Далее".

На странице NetBIOS-имя домена проверяем NetBIOS-имя, которое будет использоваться пользователями предыдущих версий Windows для идентификации домена

Домены Active Directory обозначаются в соответствии со стандартами именования DNS, однако при создании доменов Active Directory необходимо задать также NetBIOS-имя. NetBIOS-имена по возможности должны совпадать с первой меткой DNS-имени домена. Если первая метка DNS-имени домена Active Directory отличается от его NetBIOS-имени, в качестве полного доменного имени используется DNS-имя, а не NetBIOS-имя. Например, если первая метка полного DNS-имени домена - child (child.microsoft.com), а NetBIOS-имя домена - sales, полным доменным именем будет child.microsoft.com. Для продолжения нажимаем кнопку "Далее". На странице "Папки базы данных и журналов, вводим расположение, в которое нужно установить папки базы данных и журналов (или нажимаем кнопку Обзор, чтобы указать расположение).

При этом нужно убедиться, что на диске достаточно места для размещения базы данных каталога и файлов журналов, чтобы избежать проблем при установке или удалении Active Directory. Мастеру установки Active Directory необходимо 250 МБ дискового пространства для установки базы данных Active Directory и 50 МБ для файлов журналов. Рекомендуется размещать данные файлы в разделе NTFS. Для продолжения нажимаем кнопку "Далее".

На странице "Общий доступ к системному тому" указываем расположение, в которое следует установить папку Sysvol (или нажимаем кнопку Обзор, чтобы указать расположение).

Папка Sysvol должна находиться в томе NTFS, так как в ней находятся файлы, реплицируемые между контроллерами домена в домене или лесу. Эти файлы содержат

сценарии, системные политики для Windows NT 4.0 и более ранних версий, общие папки NETLOGON и SYSVOL и параметры групповой политики. Для продолжения нажимаем кнопку "Далее". На странице "Диагностика регистрации DNS" проверяем правильность установки параметров.

Если в окне "Результаты диагностики" отображается сообщение об ошибках диагностики, можно нажать кнопку "Справка" для получения дополнительных инструкций по устранению ошибки. Для продолжения нажимаем кнопку "Далее".

На странице "Разрешения" выбираем требуемый уровень совместимости приложений с операционными системами пред-Windows 2000, Windows 2000 или Windows Server 2003.

После выбора одного из вариантов можно вручную переключаться между обратной совместимостью и высоким уровнем безопасности объектов Active Directory. Для этого нужно открыть компонент "Active Directory - пользователи и компьютеры" и добавить группу безопасности "Анонимный вход" в группу безопасности "Пред-Windows 2000 доступ". Для продолжения нажимаем кнопку "Далее".

На странице "Пароль администратора для режима восстановления" нужно ввести и подтвердить пароль для учетной записи администратора режима восстановления для данного сервера.

В качестве паролей режима восстановления каталогов необходимо использовать надежные пароли. Этот пароль необходимо знать для восстановления резервной копии состояния системы данного контроллера домена. Данный пароль нужно также использовать при запуске контроллера домена в режиме восстановления служб каталогов. Для продолжения нажимаем кнопку "Далее".

После этого просматриваем сведения на странице "Сводка" и нажимаем кнопку "Далее".

Мастер установки настроит Active Directory: После завершения установки нажимаем кнопку "Готово". Для перезагрузки компьютера нажимаем кнопку "Перезагрузить сейчас", чтобы изменения вступили в силу. После перезагрузки сервера "Мастер настройки сервера" отобразит страницу "Этот сервер теперь является контроллером домена".

Задание: на практике осуществить настройку Active Directory. Представить отчет по проделанной работе.

Контрольные вопросы:

1. Что такое каталог?
2. Что такое служба каталогов?
3. Какие элементы входят в состав службы Active Directory?
4. Охарактеризуйте понятия «дерево» и «лес». Чем они отличаются?

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№7,8

Тема: Разработка требований к корпоративной сети

Цель: изучить основные принципы организации и построения консоли администрирования, а также базовые возможности некоторых инструментов системного администратора ОС Windows 10.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Перед началом выполнения практической работы в среде ОС Windows 10 необходимо выполнить следующее:

1) загрузить ОС Windows 10 и активировать справочное меню (**Пуск** | **Справка и поддержка**);

2) ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;

3) ознакомиться с возможностью получения сведений пункта 2 из альтернативного источника информации, доступного непосредственно в справке консоли администрирования MMC (**Справка** | **Вызов справки**);

4) ознакомиться с описанием и возможностями оснасток "Локальные пользователи и группы" и "Редактор объекта групповой политики" ("Групповая политика").

Задание 1. Создание консоли администрирования MMC в авторском режиме. Для выполнения задания проделайте следующие действия:

– нажмите **Пуск** | **Выполнить**,
– наберите в появившемся окне **MMC.exe** (или просто **mmc**),
– нажмите **Enter** для ввода.

Возможны следующие альтернативные варианты авторского запуска созданной ранее консоли администрирования:

А. запуск из командной строки, используя синтаксис:

Mmc *путь\имя_файла.msc* /**a**,

где параметр:

путь\имя_файла.msc – запускает консоль MMC с одновременным открытием файла сохраненной консоли с именем имя_файла.msc (**Приложение 1**). Если файл консоли не указан, будет открыта новая консоль MMC.

/**a** — открывает консоль MMC в авторском режиме.

Дополнительными параметрами команды могут быть:

/**64** — открывает 64-разрядную версию консоли MMC (MMC64). Этот параметр используется только при работе в ОС Windows XP 64-Bit Edition.

/**3**2 — открывает 32-разрядную версию консоли MMC (MMC32). При работе в ОС Windows XP 64-Bit Edition в окне консоли MMC, запущенной с этим параметром, открываются 32-разрядные оснастки.

Дополнительная информация по данной команде доступна одноименном разделе справки ОС Windows XP (**Пуск** | **Справка и поддержка**). Справку также можно получить, набрав в окне командной оболочки строку **Mmc /?** и нажав **Enter** для ввода.

В. Запуск из файлового менеджера Проводник ОС Windows XP:

– наведите манипулятор мышь на файл с расширением .msc, находящийся в системной папке ОС (%systemroot%\system32\),
– кликните правой кнопкой мыши на файле и из контекстного меню выберите **Автор**.

Задание 2. Изучение возможности изменения параметров, настройки и сохранения консоли администрирования MMC.

Для придания уникального вида сохраненной (новой) консоли администрирования MMC в авторском режиме выполните следующие действия:

1. В меню **Консоль** выберите команду **Параметры**.
2. На вкладке **Консоль** в поле названия введите новый заголовок.
3. На вкладке **Консоль** выполните следующие действия:
– нажмите кнопку **Сменить значок**,
– в поле **Имя файла** введите путь к файлу, содержащему значки (например, %systemroot%\system32\shell32.dll),
– в поле **Текущий значок** выберите необходимый значок,
– кликните **Применить** для подтверждения.
4. Сохраните окончательно сконфигурированную консоль администрирования MMC, выбрав самостоятельно ее имя и путь к месту расположения в меню **Консоль** | **Сохранить как...** При сохранении обратите внимание на то, что файлы консоли по умолчанию размещаются в папке «Администрирование», имеющей полный путь C:\Documents and Settings*Имя_пользователя*\Главное меню\Программы\Администрирование\.

Задание 3. Добавление различных элементов и компонентов к дереву консоли администрирования MMC.

Основным, интегрируемым на консоль компонентом, как уже упоминалось, является оснастка. Оснастки существуют двух видов: **изолированные** и **расширения**. Изолированная оснастка (или просто оснастка) добавляется к дереву консоли MMC без предварительного добавления других элементов, то есть непосредственно в корень дерева консоли. Оснастка расширения (или просто расширение) всегда добавляется к другой изолированной оснастке или расширению, которые уже имеются в дереве консоли MMC. Если для определенной оснастки разрешены расширения, то, как правило, они работают с объектами, управляемыми непосредственно этой оснасткой, например с компьютером, принтером, модемом или другим внешним устройством.

В дереве консоли оснастки и расширения располагаются для удобства иерархически или по группам. При добавлении новой оснастки или расширения, они появляются в виде нового элемента в дереве консоли MMC или в виде нового пункта контекстного меню, дополнительной панели инструментов, страницы свойств, а также возможно мастера, организующего определенную последовательность действий, к уже установленной оснастке.

Другими элементами, по необходимости применимыми для интеграции на консоль администрирования MMC, являются виды панели задач и собственно задачи, которые могут включать в себя команды меню для элементов консоли и команды, запускаемые из командной строки. Кроме того, могут быть созданы команды, действующие как часть дерева консоли или открывающие другой компонент.

Прежде всего, перед добавлением указанных элементов к консоли MMC, необходимо определить их число. Если, в частности, требуется добавить несколько видов панели задач, то наряду с этим необходимо определить тип каждой панели (для отображения списка и задач или только задач), а также разделить задачи по интегрированным видам панели. Добавление видов панели задач и собственно задач осуществляется посредством работы мастера создания этих элементов. При этом важно помнить, что консоль MMC должна содержать, по крайней мере, одну оснастку, чтобы возможность интеграции появилась в принципе.

Отдельной возможностью, иногда необходимой при администрировании сетей, является добавление элементов и компонентов дерева консоли администрирования MMC в виде списка ярлыков в меню "Избранное".

Дополнительные сведения о добавлении различных элементов в дерево консоли администрирования MMC можно получить, воспользовавшись справкой ОС Windows XP (**Пуск | Справка и поддержка**) в разделе **Общее представление о MMC \ Консоль MMC в авторском режиме \ Оснастки \ Создание консолей**.

Первым необходимым компонентом, добавляемым к дереву консоли администрирования MMC при ее организации и построении, является оснастка. Для добавления оснастки в авторском режиме выполните следующие действия:

1. Откройте **Консоль** управления MMC, созданную ранее.
2. В меню **Консоль** выберите команду **Добавить или удалить оснастку**.
3. В диалоговом окне **Добавить/удалить оснастку** нажмите кнопку **Добавить** вкладки **Изолированная оснастка**. Список **Оснастки** в диалоговом окне **Добавить/удалить оснастку** определяет элемент дерева консоли, к которому выполняется добавление элементов. В этом списке можно найти любой элемент дерева консоли. Обратите внимание на то, что по умолчанию это **Корень консоли**.
4. В диалоговом окне **Добавить изолированную оснастку**, выберите оснастки **Службы** из списка доступных в системе, кликнув на ней манипулятором мышь и нажав кнопку **Добавить**. Для добавления другой оснастки из списка, повторите указанные действия настоящего пункта повторно.
5. Для некоторых оснасток в процессе их инсталляции выводится диалоговое окно **Выбор целевого компьютера**, определяющее, чем, устанавливаемая оснастка будет управлять в дальнейшем – локальным или сетевым компьютером. Выберите **Локальный компьютер**, установив переключатель в соответствующее положение.

6. Нажмите **Готово**, **Закрыть** и затем кликните **OK** для подтверждения ввода.

7. Скройте меню и панель инструментов оснастки **Службы**, выполнив действия указанные ниже:

– В меню **Вид** выберите команду **Настроить**,
– В группе **Оснастка** снимите флажок **Меню**,
– В группе **Оснастка** снимите флажок **Панели инструментов**,
– Нажмите **OK**.

При устанавливании или снятии флажков, соответствующие им меню и панели инструментов отображаются или скрываются, причем, для всех оснасток консоли, включая текущую. Если переключение флажков не приводит к изменению вида консоли, тогда текущая оснастка не имеет специальных меню или панелей инструментов.

8. Не закрывая консоль администрирования MMC, сохраните ее, выбрав команду **Сохранить** в меню **Консоль**.

Для добавления расширений к уже установленной в предыдущем задании оснастке **Службы** выполните следующее:

9. В меню **Консоль** выберите команду **Добавить или удалить оснастку**.

10. В диалоговом окне **Добавить/удалить оснастку** выберите вкладку **Расширение**. На этой вкладке можно выбрать любой элемент дерева консоли из списка **Оснастки**, которые могут быть расширены, и просмотреть **Доступные расширения**, которые могут быть включены или отключены. После подключения расширение автоматически размещается в дереве консоли под оснасткой, к которой оно относится. Если дерево консоли содержит больше одного экземпляра оснастки, к которой подключено расширение, все остальные экземпляры автоматически получают это расширение.

11. Среди **Доступных расширений** оснастки **Службы** удалите флажок с расширения **Расширенный вид** (предварительно сняв флажок **Добавить все разрешения**) и отметьте, к чему привело это действие. Повторите аналогичные действия с другими расширениями данной оснастки и изучите получаемый результат.

12. Не закрывая консоль администрирования MMC, сохраните ее.

Следующим элементом, необходимым в ряде случаев администрирования и предназначенным, в том числе, для удобства отображения информации, является новый вид панели задач. Для добавления видов панелей задач и собственно задач в авторском режиме выполните следующее:

1. Откройте **Консоль** управления MMC, созданную ранее.
2. Добавьте оснастку **Службы** в корень консоли MMC.
3. В дереве консоли кликните манипулятором мышь на этой оснастке.
4. В меню **Действие** или кликнув правой кнопкой манипулятора на оснастке, выберите команду **Новый вид панели задач**.
5. Следуйте инструкциям **"Мастера создания вида панели задач"**, чтобы добавить на консоль новую панель вида.
6. Если сразу после создания вида панели задач необходимо создать задачи, установите флажок **"Запустить мастер создания новой задачи"** на последнем экране **"Мастера создания вида панели задач"**.
7. Следуйте инструкциям "**Мастера создания новой задачи"**, чтобы добавить на консоль новую задачу к существующей панели вида.
8. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), связанный с видом панели задач, затем в меню **Действие** выберите команду **Правка вида панели задач**.
9. На вкладке **Задачи** нажмите кнопку **Создать**.
10. Повторите инструкции пункта 7 настоящего задания.
11. Не закрывая консоль администрирования MMC, сохраните ее.

Измените вид панели задач сохраненной консоли администрирования MMC, выполнив следующие действия:

– введите новое имя,

– введите новое описание,

– установите переключатель **Стиль для области сведений** в положение, соответствующее новому формату списка,

– удалите соответствующий флажок, чтобы отобразить стандартную вкладку,

– установите переключатель **Стиль для описания задачи** в положение, соответствующее новому стилю задачи,

– выберите новое значение ширины для вертикального списка или высоты для горизонтального списка,

– нажмите кнопку **Параметры** и установите переключатель в одно из необходимых положений,

– нажмите **OK** для подтверждения ввода,

– изучите полученный результат.

Важной особенностью при построении и организации консоли администрирования MMC является возможность добавления элементов и компонентов дерева консоли в виде списка ярлыков в меню **"Избранное"**. Для добавления элемента или компонента в авторском режиме выполните следующее:

1. Откройте **Консоль** управления MMC, созданную ранее.

2. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), который нужно добавить в список "Избранное".

3. В области сведений выберите вкладку вида панели задач, которую нужно добавить, в случае, если для элемента или компонента, указанного в дереве консоли, настроен вид панели задач. В противном случае в области сведений вкладки не видны.

4. Выберите в меню **Избранное** команду **Добавить в избранное**.

5. В поле **Создать в:** диалогового окна **Добавление в папку "Избранное"** выполните указанные ниже действия:

– создайте новую папку с названием, выбранным самостоятельно, кликнув папку, которая будет выступать в качестве родительской для создаваемой папки и нажав кнопку **Создать папку**,

– нажмите кнопку **OK** для ввода,

– в поле **Имя папки** введите имя, под которым будет добавлен элемент,

– кликните **OK** для подтверждения ввода.

6. Не закрывая консоль администрирования MMC, сохраните ее.

Упорядочите "Избранное" сохраненной консоли администрирования MMC, выполнив следующие действия:

– добавьте новую папку, введя ее имя в соответствующее поле и кликнув **OK** для подтверждения ввода,

– переместите элемент, созданный в **пункте 5** настоящего задания, в новую, только что созданную, папку и кликните **OK** для ввода,

– переименуйте выбранный элемент и нажмите клавишу **Enter** для подтверждения ввода,

– удалите все элементы, расположенные ниже папки "Избранное",

– нажмите **Закрыть** для завершения задания,

– изучите полученный результат.

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№9,10

Тема: Конфигурирование сети

Цель: получить практические навыки установки и настройки файлового и web-серверов.
Оборудование: тетрадь, ручка, ПК
Методические указания: выполните задания
Ход выполнения:
Задание 1. Подготовьте файловый сервер.

1. Запустите ОС Windows.
2. Добавьте новую **роль** серверу – *Файл-сервер*:

- откройте диалоговое окно **Управление данным сервером (*Пуск/дминистрирование/Управление Данным Сервером*)**;
- активизируйте добавление ролей кнопкой ***Добавить или удалить роль***;
- выберите **Файловый сервер** и щелкните ***Далее***

3. установите параметры файлового сервера:

- Предоставить доступ UNIX-системам к файлам;
- Предоставить доступ Apple--системам к файлам;
- подтвердите введенные параметры кнопкой ***Далее***;
- запустите установку роли сервера кнопкой ***Далее***.

4. Перезагрузите виртуальный компьютер кнопкой ***Перезегрузить***.
5. Откройте диалоговое окно **Настройки файлового сервера (*Пуск/дминистрирование/Управление Данным Сервером/Управление этим файловым сервером*)**.
6. Установите стандартные квоты использования места на диске:

- установите флажок *Установить дисковые квоты по умолчанию для новых пользователей данного сервера*;
- укажите **размер квот** - *50Мб*;
- установите **предупреждение о квоте** - *40Мб*;
- установите флажок *Не выделять место на диске при превышении дискового пространства*;
- завершите ввод стандартных квот кнопкой ***Далее***.

8. Откажитесь от включения службы индексирования.
9. Укажите папку на сервере, для хранения файлов, например ***C:\Documents and settings\Администратор\Рабочий стол\PUB***.
10. Далее мастер установки завершит свою работу. Попробуйте теперь зайти на созданную вами сетевую папку с другого компьютера сети. Обратите внимание на способ подключения. Попробуйте заполнить папку для превышения квоты.

Задание 2. Настройте Web-сервер.

1. Установите **Internet Information Service (IIS) (*Пуск/администрирование/Управление Данным Сервером/Сервер приложений IIS*)**:

о Подготовьте тестовую страницу: создайте временную страницу, вызываемую по умолчанию: наберите в **Блокноте** и сохраните в файле с именем ***Default.html*** в каталоге ***\Inetpub\wwwroot***.

2. Настройте **Web-сервер**:

откройте консоль управления сервером **IIS (*Пуск/администрирование/Управление Данным Сервером/Управление этим сервером приложений*)**;

перейдите к web-узлу, заданному по умолчанию (***Диспетчер служб IIS/Веб-узлы/Веб-узел по умолчанию***);

- откройте диалоговое окно **Свойства узла по умолчанию (*контекстное меню/Свойства*)**;
- добавьте страницу по умолчанию:
- перейдите на вкладку **Документы**;
- установите флажок *Задать страницу содержания по умолчанию*;
- откройте окно добавления кнопкой ***Добавить***;

- введите в поле ***Default.html***;
- подтвердите добавление кнопкой ***ОК***. закройте окно свойств кнопкой ***ОК***.

3. Проверьте настройку **Web-сервера**:

- на вашем компьютере откройте **Internet Explorer (*Пуск/Программы/Internet Explorer*)**;
- наберите в адресной строке **http://127.0.0.1/**;
- сделайте скриншот происходящего на экране и сохраните его в своей папке.

Задание 3. Установите и настройте сервер FTP

1. Установите сервер **FTP - FileZilla**.
2. Запустите **FileZilla Server Interface**.
3. Ограничьте количество одновременных подключений к серверу:

- откройте окно настройки сервера (***Edit/Settings***);
- перейдите в раздел **General Settings** (общие настройки);
- введите в поле **Max.number of users** – *2*;

4. Установите текст приветствия:

перейдите в раздел **Welcome message**;

введите в поле **Custom welcome message** – *Добро пожаловать на мой сервер*;

Установите ограничения по скорости:

- перейдите в раздел **Speed Limits** (ограничения скорости);
- включите использование правил ограничения скорости радио-
- кнопкой *Use Speed Limit rules*;
- добавьте ограничение по скорости не более 3 Кб/с в понедельник:
- откройте окно задания параметров ограничений кнопкой ***Add*** (Добавить);
- сбросьте все флажки кроме *Monday* (Понедельник);
- введите в поле **Speed** – *3*;
- подтвердите ввод данных кнопкой ***ОК***; примените параметры кнопкой ***ОК***.

Создайте группы пользователей **FTP-сервера**:

- откройте диалоговое окно **добавления групп** кнопкой на панели инструментов;
- активируйте добавление групп кнопкой ***Add*** (Добавить);
- введите **имя группы**, например *Students* (***ОК***);
- задайте общую папку для созданной группы:
- перейдите в раздел **Shared Folders** (Общие папки);
- активируйте добавление папок кнопкой ***Add*** (Добавить);
- укажите общую папку, например ***C:\Documents and settings\Администратор\Рабочий стол*** и подтвердите выбор кнопкой ***ОК***;
- разрешите чтение и удаление содержимого общей папки – установите флажок*Write и Delete*;
- завершите добавление групп пользователей кнопкой ***ОК***.
- Добавьте нового пользователя:
- откройте диалоговое окно добавления пользователей кнопкой на панели инструментов;
- активируйте добавление пользователей кнопкой ***Add*** (Добавить);
- введите **имя группы**, например *justuser*;
- выберите в списке **User should be member of the following group** созданную ранее группу и подтвердите создание пользователя кнопкой ***ОК***;
- установите пароль для созданного пользователя:
- перейдите на вкладку **General** (Общие);
- введите в поле **Password** новый пароль, например *123*;
- завершите добавление групп пользователей кнопкой ***ОК***.
- Проверьте работу сервер:
- запустите командную строку (***Пуск/Программы/Стандартные/Командная строка***);
- введите команду для подключения к FTP-серверу на текущем компьютере: **FTP 127.0.0.1**

- введите имя пользователя - *justuser* (***ENTER***);
- введите пароль - *123* (***ENTER***);
- просмотрите содержимое домашней папки: **DIR**
- отключитесь от сервера: **QUIT**
- закройте командную строку.
- Закройте интерфейс управления **FTP-сервером**.

Контрольные вопросы

1.Где располагается файл журнала FTP-сервера?

2. Какие варианты ограничения доступа по IP-адресу существуют?

3. В чем отличие виртуального каталога от обычного?

4. Для чего необходимо создавать виртуальный каталог upload, если можно было сделать обычный каталог upload?

5. Можно ли средствами IIS и FTP-сервера ограничить доступ к данным определенному пользователю (по его имени)?

6. Шифруются ли имя пользователя и пароль при аутентификации пользователя на FTP-сервере?

7. В чем преимущество использования FTP-сервера перед использованием обычным папок, к которым предоставлен общий доступ?

Если разрешены анонимные подключения к FTP-серверу, то от имени какой учетной записи будет происходить доступ к различным папкам на сервере? Можно управлять данным параметром?

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№11

Тема: Сравнение технических характеристик серверов

Цель: узнать параметры настройки стандартного брандмауэра, научиться создавать различные типы исключений

Оборудование: тетрадь, ручка, ПК

Методические указания: ознакомиться с теоретическими сведениями**,** выполните задания

Ход выполнения:

Теоретические сведения

Брандмауэр позволяет обеспечить безопасность системы путем ограничения трафика, который поступает от других компьютеров, и предоставления пользователю возможности контролировать локальные данные. (запишите в отчет)

Кроме того, брандмауэр защищает систему от несанкционированного подключения других пользователей и программ (в т.ч. вирусов и компьютерных червей).

Брандмауэр можно представить себе в виде защитного барьера, на котором осуществляется проверка поступающих из Интернета или другой сети данных. В зависимости от настроенных параметров брандмауэр блокирует трафик или пропускает его на компьютер.

В Windows XP с пакетом обновления 2 (SP2) пользователь может включать и выключать брандмауэр. Несмотря на то, что брандмауэр Windows включен по умолчанию, он может быть отключен производителем компьютера или сетевым администратором. Вы не обязаны использовать на своем компьютере брандмауэр Windows, а можете установить брандмауэр любого стороннего производителя, предварительно взвесив преимущества каждого из них и выбрав наиболее подходящий. В случае использования брандмауэра стороннего производителя брандмауэр Windows следует отключить.

Чтобы настроить параметры брандмауэра Windows, выполните следующие действия.

1. Выберите в меню **Пуск** пункт **Выполнить**, введите команду **wscui.cpl** и

нажмите
кнопку **ОК**.

2. В диалоговом окне **Центр обеспечения безопасности Windows** щелкните ссылку
Брандмауэр Windows.

Запишите в отчет способы запуска брандмауэра.

Диалоговое окно **Брандмауэр Windows** содержит следующие вкладки.

Общие Исключения Дополнительно

На вкладке **Общие** расположены ледующие элементы управления.

Включить (рекомендуется)

Не разрешать исключения

Выключить (не рекомендуется)

Запишите в отчет, какие вкладки и элементы управления находятся в настройках брандмауэра.

Если установлен флажок **Не разрешать исключения**, брандмауэр Windows блокирует все запросы на подключение к компьютеру, включая запросы от программ и служб, перечисленных на вкладке **Исключения**. Кроме того, брандмауэр блокирует совместный доступ к файлам и принтерам, а также обнаружение сетевых устройств.

Использовать брандмауэр Windows в этом режиме целесообразно при подключении к сетям общего пользования, например сетям в гостиницах и аэропортах. Защита компьютера обеспечивается путем блокирования всех попыток установить к нему подключение.

Брандмауэр Windows в режиме «Не разрешать исключения» позволяет просматривать веб-страницы, обмениваться сообщениями электронной почты или немедленными сообщениями.

На вкладке **Исключения** можно создать исключение ***для порта или программы***, чтобы разрешить получение определенных видов входящего трафика. Каждому исключению можно назначить область.

Для домашних и небольших офисных сетей рекомендуется ограничивать такую область пределами локальной сети. В этом случае установленные на компьютере программы доступны другим компьютерам в составе той же подсети, а трафик из удаленных сетей блокируется.

Вкладка **Дополнительно** служит для выполнения следующих действий:

настройка правил для подключений, которые применяются к каждому сетевому интерфейсу;

настройка параметров ведения журнала безопасности;

настройка глобальных правил для трафика по протоколу ICMP (Internet Control Message Protocol), который служит для передачи сведений об ошибках и состоянии;

восстановление параметров по умолчанию.

Настройка исключений

Брандмауэр Windows содержит несколько предопределенных исключений, которые разрешают сетевой доступ для некоторых общих системных задач***, таких как удаленное управление и совместное использование файлов и принтеров.*** В таблице перечислены включенные по умолчанию исключения брандмауэра Windows, а также открытые порты и использующие их программы.

Запишите в отчет, что такое исключение и какие исключения заданы в работе брандмауэра по умолчанию. Проверьте настройки на соответствующей вкладке. Запишите таблицу в отчет.

Администратор может также задать собственный набор исключений локально через приложение "Брандмауэр Windows" в панели управления или удаленно с использованием механизма групповых политик. Для этого достаточно просто указать имя программы, которая генерирует трафик или сетевые параметры (номер порта TCP или UDP) и адрес источника, а затем разрешить сформированное исключение в брандмауэре Windows.

Предопределенные исключения предоставляют более гибкие возможности настройки, чем пользовательские, поскольку в них допускается задание нескольких портов в одном правиле. Например, исключение для совместного доступа к файлам и принтерам разрешает использование портов TCP 139, TCP 445, UDP 137 и UDP

138.

При создании пользовательского исключения система позволяет указать только один порт, так что для открытия диапазона портов необходимо создать набор исключений для каждого порта. При этом допускается создание пользовательских областей, т.е. адресов IP или диапазонов адресов IP, для которых разрешен обмен. Это позволяет задавать наборы портов для предопределенных и для пользовательских исключений.

Администраторы корпоративных сетей для настройки брандмауэра Windows могут использовать групповые политики. При этом необходимо указать порт (например, 80), транспорт (TCP или UDP), область, статус (разрешен или запрещен), и имя соединения. Конструкция имеет вид Порт:Транспорт:Область:Статус:Имя (Port:Transport:Scope:Status:Name).

Ведение журнала

Можно настроить брандмауэр Windows для ведения журнала в виде текстового файла на локальном компьютере или сетевом диске. Брандмауэр Windows может записывать события блокирования пакетов и успешных подключений. Журнал содержит необходимые сведения для устранения неисправностей и ошибок при невозможности подключиться к необходимым ресурсам или просмотре разрешенных соединений.

По умолчанию брандмауэр Windows выдает пользователю предупреждение о том, что некоторая программа пытается использовать указанный порт. При централизованной настройке брандмауэра Windows через групповые политики администратор может по своему желанию отключить выдачу предупреждений пользователям.

Запишите в отчет, как создать файл журнала и указать путь для его хранения. После его создания, просмотрите его содержимое, предварительно осуществив какое-либо сетевое подключение.

Управление брандмауэром Windows из командной строки

Программа Netsh позволяет выполнять настройку клиентов брандмауэра Windows из командной строки напрямую или через пакетный файл. Например, команда ***netsh firewall show config*** показывает текущее состояние брандмауэра Windows на компьютере клиента.

Выполните команду, запишите команду и ее назначение в отчет.

Netsh позволяет управлять почти всеми параметрами брандмауэра Windows, так что администраторы, активно использующие в работе сценарии, могут использовать сценарии подключения к домену для настройки и проверки работы брандмауэра Windows.

Например, приведенная ниже команда Netsh создает локальное правило брандмауэра, разрешающее доступ по Telnet к компьютеру, защищенному брандмауэром Windows, с указанных адресов.

netsh firewall add portopening protocol = TCP port = 23
name = Telnet mode = ENABLE scope = CUSTOM addresses = 192.168.0.0/255.255.255.0, 10.0.0.0/255.255.240.0

Эту команду можно было сократить, исключив имена атрибутов: netsh firewall add portopening TCP 23 Telnet ENABLE CUSTOM 192.168.0.0/255.255.255.0, 10.0.0.0/255.255.240.0

Результат исполнения приведенных выше команд можно проверить с помощью команды netsh firewall show portopening

Как работает брандмауэр Windows в режиме повышенной безопасности

Появился, только начиная с Windows Vista.

Брандмауэр Windows в режиме повышенной безопасности – это брандмауэр, регистрирующий состояние сети, для рабочих станций. В отличие от брандмауэров для маршрутизаторов, которые развертывают на шлюзе между локальной сетью и Интернетом, брандмауэр Windows создан для работы на отдельных компьютерах. Он отслеживает только трафик рабочей станции: трафик, приходящий на IP-адрес данного компьютера, и исходящий трафик самого компьютера. Брандмауэр Windows в режиме повышенной безопасности выполняет следующие основные операции:

Входящий пакет проверяется и сравнивается со списком разрешенного трафика. Если пакет соответствует одному из значений списка, брандмауэр Windows передает пакет протоколу TCP/IP для дальнейшей обработки. Если пакет не соответствует ни одному из

значений списка, брандмауэр Windows блокирует пакет, и в том случае, если включено протоколирование, создает запись в файле журнала.

Список разрешенного трафика формируется двумя путями:

Когда подключение, контролируемое брандмауэром Windows в режиме повышенной безопасности, отправляет пакет, брандмауэр создает значение в списке разрешающее прием ответного трафика. Для соответствующего входящего трафика потребуется дополнительное разрешение.

Когда Вы создаете разрешающее правило брандмауэра Windows в режиме повышенной безопасности, трафик, для которого создано соответствующее правило, будет разрешен на компьютере с работающим брандмауэром Windows. Этот компьютер будет принимать явно разрешенный входящий трафик в режимах работы в качестве сервера, клиентского компьютера или узла однораноговой сети.

Первым шагом по решению проблем, связанных с Брандмауэром Windows, является проверка того, какой профиль является активным. Брандмауэр Windows в режиме повышенной безопасности является приложением, отслеживающим сетевое окружение. Профиль брандмауэра Windows меняется при изменении сетевого окружения. Профиль представляет собой набор настроек и правил, который применяется в зависимости от сетевого окружения и действующих сетевых подключений.

Брандмауэр различает три типа сетевого окружения: домен, публичная и частная сети. Доменом является сетевое окружение, в котором подключения проходят аутентификацию на контроллере домена. По умолчанию все другие типы сетевых подключений рассматриваются как публичные сети. При обнаружении нового подключения Windows Vista предлагает пользователю указать, является ли данная сеть частной или публичной. Общий профиль предназначен для использования в общественных местах, например, в аэропортах или кафе. Частный профиль предназначен для использования дома или в офисе, а также в защищенной сети. Чтобы определить сеть как частную, пользователь должен обладать соответствующими административными полномочиями.

Хотя компьютер может быть подключен одновременно к сетям разного типа, активным может быть только один профиль.

Форма отчета:

1. Запишите в отчет все, что указано по тексту работы.
2. Ответьте на контрольные вопросы

Контрольные вопросы:

1. Зачем на вкладке «Дополнительно» используется настройка протокола ICMP?
2. В каком случае исключения создаются автоматически (то есть мы не заносим программу вручную в список запрещенных)?
3. Какая информация сохраняется в файле журнала брандмауэра. Чем она может помочь?
4. Какие типы сетевого окружения поддерживает брандмауэр в режиме повышенной безопасности.

Практическое занятие№12

Тема: Формирование аппаратных требований и схемы банка данных

Цель: изучить этапы установки прикладного программного обеспечения, научиться настраивать и работать с прикладным программным обеспечением.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1. Напишите этапы установки программного обеспечения. Для выполнения задания можете воспользоваться ссылкой http://www.oszone.net/4186_2

Задание 2. Напишите клиентские компоненты установки ПО для Windows Professional. Для выполнения задания можете воспользоваться ссылкой http://www.oszone.net/4186_2

Задание 3. Напишите этапы настройки программного обеспечения. Для выполнения задания можете воспользоваться ссылкой http://www.oszone.net/4186_2

Задание 4. Сравни, чего больше:

А) Графических редакторов или прикладных программ?

Б) Антивирусных программ или системных программ?

В) Отладчиков или языков программирования?

Задание 5. Укажите, какое ПО необходимо людям в следующих ситуациях:

Ситуация	Системное ПО	Прикладное ПО	Инструментальное ПО
Ландшафтные дизайнеры создают проект нового городского ландшафта			
Профессиональный программист пишет компьютерную программу по заказу крупной фирмы			
Ученые научно-исследовательского института расшифровывают записи, переданные марсходом			
Выпускной 11 класс готовит фотоальбом и собирает воспоминания о своей школьной жизни			
Web-дизайнер создает сайт известной фирмы			
Школьник играет в компьютерную игру			
Создатели нового мобильного телефона пробуют различные варианты дизайна			
Учитель пишет компьютерный тест по своему предмету			
Конструкторы исследуют модель новой подводной лодки			

Задание 6. Напишите в чем принципиальное отличие прикладного программного обеспечения общего назначения от иных видов прикладного программного обеспечения?

Задание 7. Напишите в чем заключается принцип организации диалога «компьютер—пользователь» с помощью меню?

Задание 8. Ваша работа будет состоять в следующем. У вас в задании приведен алгоритм выполнения практической. Ваша задача, выполняя его, справиться с максимальным количеством заданий.

Алгоритм работы

1. Запустите *с Рабочего стола* презентацию *Прикладные программы* (двойной щелчок ЛКМ по ярлыку).
2. Нажмите клавишу F5 для начала показа слайдов.
3. Откройте прикладную программу Текстовый редактор.
4. Выполните задания, закройте Приложение, сохранив результат.
5. Откройте прикладную программу Графический редактор.
6. Выполните задание, закройте Приложение, сохранив результат.
7. Откройте прикладную программу Электронные таблицы.
8. Выполните задание, закройте Приложение, предварительно сохранив результат.

9. Откройте игровую программу.

Из среды Power Point с помощью гиперссылок на соответствующие файлы осуществляются переходы в среды Microsoft Word (Приложение№1), Paint (Приложение№2) Microsoft Excel (Приложение№3), любую игровую или развивающую среду, имеющуюся в распоряжении учителя (Приложение№4), в которых учащиеся выполняют работу.

Форма отчета:

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.
4. Вывод по работе.

6. Контрольные вопросы

1. Что принято понимать под термином 'software'?
2. На какие уровни делится программное обеспечение?
3. Совокупность программ какого уровня образовывают ядро операционной системы?
4. Какие функции выполняет ядро операционной системы?
5. Для чего предназначены программы базового уровня?
6. Какие классы программ служебного уровня вы знаете?
7. С помощью программ какого класса можно осуществлять ввод, редактирование и оформление текстовых данных?
8. Какие вы знаете категории графических редакторов?
9. В каких случаях целесообразно использовать системы автоматизированного перевода?
10. Что такое интерпретатор и компилятор? Какая между ними разница?

Практическое занятие№13

Тема: Установка и настройка сервера MySQL

Цель: изучить этапы установки прикладного программного обеспечения, научиться настраивать и работать с прикладным программным обеспечением.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание № 1. Напишите этапы установки программного обеспечения.

Для выполнения задания можете воспользоваться ссылкой http://www.oszone.net/4186_2

Задание № 2. Напишите клиентские компоненты установки ПО для Windows Professional.

Для выполнения задания можете воспользоваться ссылкой http://www.oszone.net/4186_2

Задание № 3. Напишите этапы настройки программного обеспечения.

Для выполнения задания можете воспользоваться ссылкой http://www.oszone.net/4186_2

Задание № 4. Сравни, чего больше:

А) Графических редакторов или прикладных программ?_____

Б) Антивирусных программ или системных программ?_____

В) Отладчиков или языков программирования?_____

Задание № 5. Укажите, какое ПО необходимо людям в следующих ситуациях:

Ситуация	Системное ПО	Прикладное ПО	Инструментальное ПО
Ландшафтные дизайнеры создают проект нового городского ландшафта			
Профессиональный программист пишет компьютерную программу по заказу крупной фирмы			
Ученые научно-исследовательского института расшифровывают записи, переданные марсходом			
Выпускной 11 класс готовит фотоальбом и собирает воспоминания о своей школьной жизни			
Web-дизайнер создает сайт известной фирмы			

Школьник играет в компьютерную игру			
Создатели нового мобильного телефона пробуют различные варианты дизайна			
Учитель пишет компьютерный тест по своему предмету			
Конструкторы исследуют модель новой подводной лодки			

Задание № 6. Напишите в чем принципиальное отличие прикладного программного обеспечения общего назначения от иных видов прикладного программного обеспечения?

Задание № 7. Напишите в чем заключается принцип организации диалога «компьютер—пользователь» с помощью меню?

Ответы на контрольные вопросы

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№14

Тема: Выполнение запросов к базе данных

Цель: научиться создавать запросы простые и сложные к готовой базе данных.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1. Создание базы данных

1. Любым, изученным, способом создайте в новой базе данных 2 таблицы **Студент** и **Работник** и заполните их данными по образцу.

Студент

Код Студент	Фамилия	Имя	Отчество	Адрес	Номер телефона	Специализация
1	Иванов	Иван	Иванович	г. Тула	457896	администратор
2	Петров	Сергей	Петрович	г. Москва	7458962	технолог
3	Голубева	Ольга	Ивановна	г. Белев	3698521	бухгалтер
4	Соколова	Инна	Олеговна	г. Тула	852967	бухгалтер
5	Мухина	Олеся	Петровна	г. Москва	8625471	технолог
6	Андреева	Анна	Романовна	г. Люберцы	748596	повар
7	Галкина	Дина	Евгеньевна	г. Люберцы	919597	технолог
8	Сорина	Ольга	Сергеевна	г. Москва	9191954	бухгалтер
9	Сидоров	Илья	Владимирович	г. Волгоград	126578	слесарь

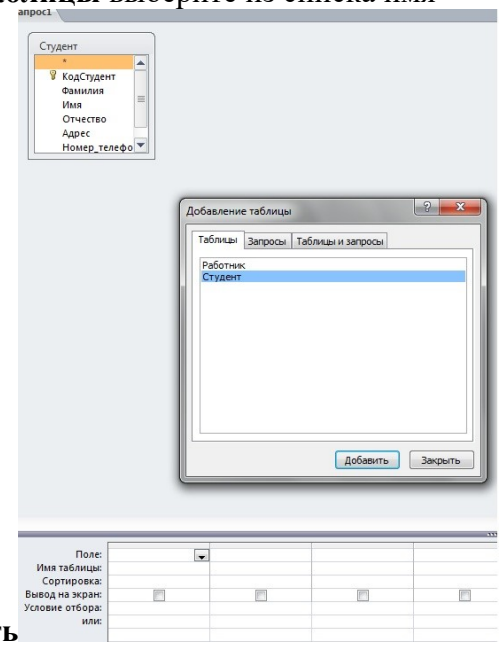
Работник

Код работника	Фамилия	Имя	Отчество	Адрес	Организация	должность	телефон
1	Бубнов	Олег	Петрович	Г.Москва	РотФронт	директор	785456
2	Фролова	Ольга	Ивановна	Г. Люберцы	Гранд	бухгалтер	213568
3	Сорян	Виктория	Викторовна	Г.Тула	Рубин	бухгалтер	526598
4	Фельдман	Генрих	Вениаминович	Г.Москва	Растр	инженер	569726
5	Ильичева	Татьяна	Федоровна	Г. Воронеж	Симка	секретарь	569875
6	Тимофеева	Инна	Вячеславовна	Г.Елец	Магнит	продавец	687459

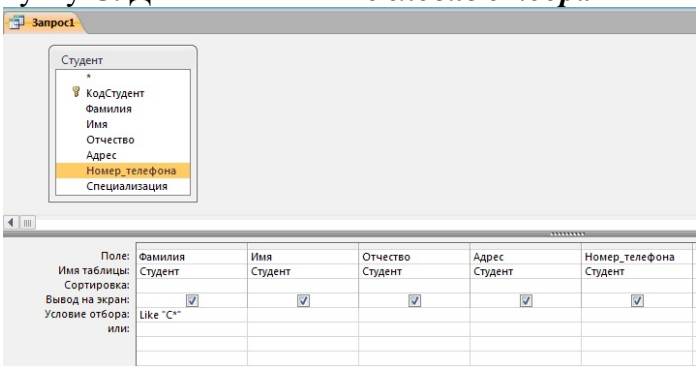
Задание 2. Создание запроса на выборку.

1. Выполните команду **Создание – Конструктор запросов.**

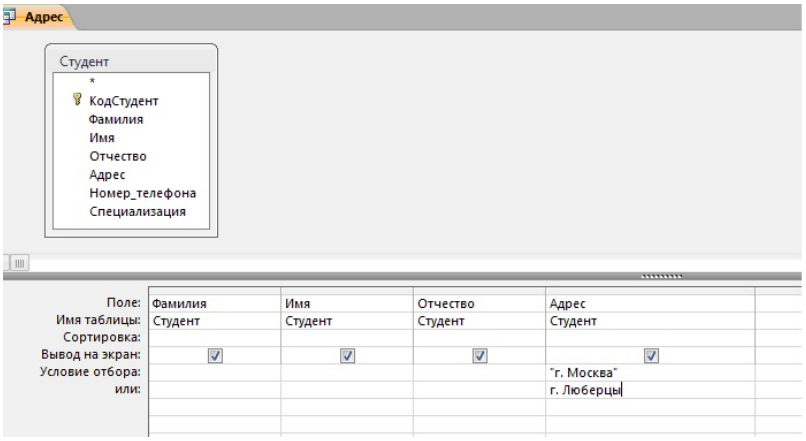
2. В появившемся диалоговом окне **Добавление таблицы** выберите из списка имя таблицы **Студент**, щелкните по кнопке **Добавить**



3. Закончите выбор, щелкнув по кнопке **Закрыть.** Появится возможность выбора полей из таблицы “Студент”. Для этого достаточно дважды щелкнуть по именам полей или перетащить мышью названия полей в клетку запроса.
4. Создайте телефонную книгу для всех студентов, фамилии которых начинаются на букву **С.** Для этого в поле ***Условие отбора*** напишите условие **Like “С*”**



5. Сохраните запрос, щелкнув по кнопке **Сохранить**. Введите имя запроса **Телефонная книга** и щелкните по кнопке **ОК.**
6. Щелкните по кнопке **Выполнить** для представления запроса. Закройте запрос.
7. Убедитесь в правильности полученного запроса, щелкнув по имени запроса **Телефонная книга** слева в окне **Все объекты Access.** Закройте таблицу.
8. Создайте запрос на выборку тех студентов, которые приехали из Москвы или Люберцы.
9. Для этого выполите команду **Создание – Конструктор запросов.**
10. В появившемся диалоговом окне **Добавление таблицы** выберите из списка имя таблицы **Студент**, щелкните по кнопке **Добавить**
11. Закончите выбор, щелкнув по кнопке **Закрыть.** Появится возможность выбора полей из таблицы “Студент”. Для этого достаточно дважды щелкнуть по именам полей или перетащить мышью названия полей в клетку запроса.
12. В поле ***Условие отбора*** напишите условия для поля **Адрес** так, как показано на рисунке



13. Сохраните запрос, щелкнув по кнопке **Сохранить**. Введите имя запроса **Адрес** и щелкните по кнопке**ОК.**
14. Щелкните по кнопке **Выполнить** для представления запроса. Закройте запрос.

Самостоятельное задание.

1. Составьте запрос на выборку тех студенток, имя которых – Ольга.
2. Составьте запрос на выборку работников организаций, названия которых начинаются на букву **Р,** используя таблицу **Работник.**
3. Составьте запрос на выборку всех студентов, которые обучаются по специальности технолога.
4. Составьте запрос на выборку работников организаций, которые работают по должности **инженер** или **бухгалтер**.
5. Результаты предъявите учителю.

Задание 3. Завершение работы с программой Access.

1. Выполните команду *Файл – Выход.*
2. Если вы производили редактирование в базе данных, появится вопрос о сохранении изменений. Ответьте утвердительно.

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№15

Тема: Выполнение изменений в базе данных, создание триггеров

Цель: сформировать знания о создании и изменении триггера; привести примеры практического использования триггера; повторить знания о создании хранимых процедур; провести контроль операторов хранимых процедур.

Оборудование: тетрадь, ручка, ПК

Методические указания: ознакомьтесь с теоретическими сведениями, выполните задания

Ход выполнения:

1 Написать триггер, настроенный на операцию добавления записей в таблицу сотрудников, с фиксацией идентификатора строки и даты выполненного обновления во вспомогательной таблице базы данных.

2 Создать строчный триггер, активизирующийся при каждый раз для удаляемых строк таблицы с фиксацией пользователя, выполнившего данные удаления и старых данных о имени, фамилии, дне рождения, адреса и телефона удаленных строк с информацией о сотрудниках предприятия.

3 Создать триггер, который бы фиксировал во вспомогательной таблице изменения, произведенные над столбцом рентной стоимости для таблицы с описанием объектов

недвижимости с сохранением значений до и после изменения, а также имя пользователя, от лица которого данные изменения производились.

4 Создать триггер, настроенный на ввод новых строк в таблицу с описанием сотрудников. Реакцией на добавление должна быть проверка количества работающих сотрудников в заданном отделении и занесение (путем разового обновления данных соответствующего столбца) этого количества с учетом нового сотрудника во вспомогательную таблицу. В случае превышения вычисленного значения 5 в строку с данным отделением во вспомогательной таблице следует добавить некоторое информирующее сообщение.

5 Создать триггер, фиксирующий ежеквартальное увеличение заработной платы для сотрудников предприятия. Данные о предварительных изменениях фиксировать во вспомогательной таблице с указанием даты сделанных изменений. Перед обновлением триггер считывает информацию из вспомогательной таблицы, сравнивая текущую дату с датой последней прибавки, в случае если со времени последнего пересчета прошло более 3-х месяцев во вспомогательной таблице фиксируется дата текущего пересчета и значения средних зарплат сотрудников до и после изменения в зависимости от занимаемых должностей.

Контрольные вопросы

1 Что такое триггер?

2 Чем отличаются триггеры от хранимых процедур и функций

3 Какие типы триггеров вы знаете?

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№16

Тема: Создание запросов и процедур на изменение структуры базы данных

Цель: создать SQL-запросы на создание таблицы, на выборку с параметрами, на обновление записей, на удаление записей, на добавление данных, на удаление таблицы, на создание индексов.

Оборудование: тетрадь, ручка, ПК

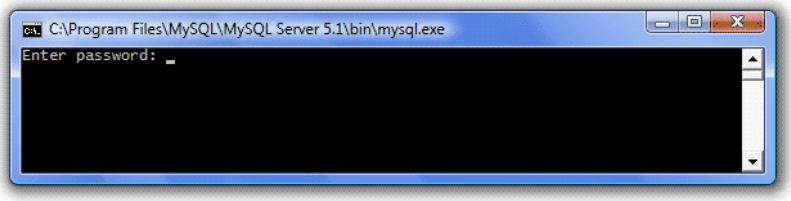
Методические указания: выполните задания

Ход выполнения:

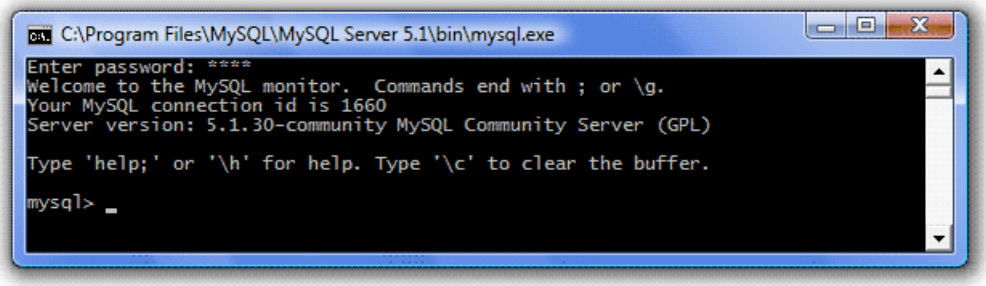
Задание 1.

Итак, вы установили MySQL, и мы начинаем осваивать язык SQL. В уроке 3 по основам баз данных, мы создали концептуальную модель маленькой БД для форума. Пришло время реализовать ее в СУБД MySQL.

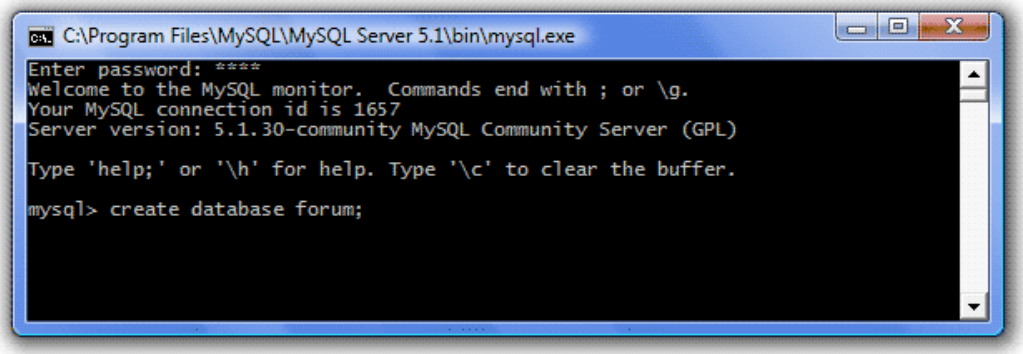
Для этого прежде всего надо запустить сервер MySQL. Идем в системное меню Пуск — Программы — MySQL — MySQL Server 5.1 — MySQL Command Line Client. Откроется окно, предлагающее ввести пароль.



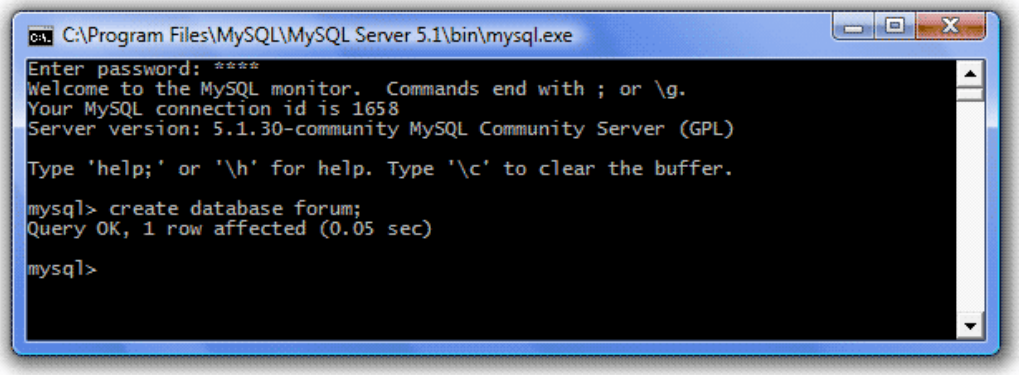
Нажимаем Enter на клавиатуре, если вы не указывали пароль при настройке сервера или указываем пароль, если вы его задавали. Ждем приглашения mysql>.



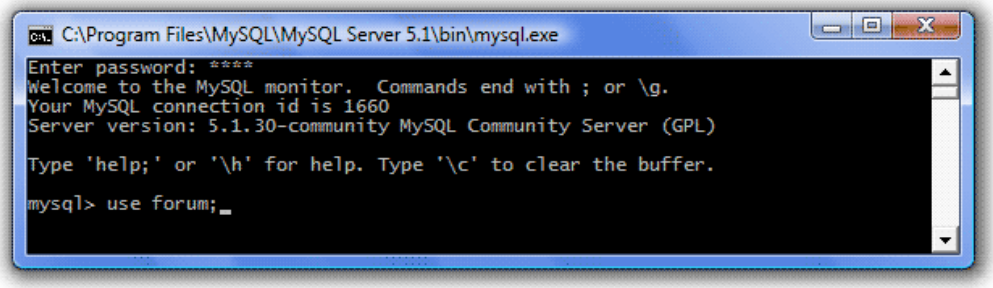
Нам надо создать базу данных, которую мы назовем forum. Для этого в SQL существует оператор *create database*. Создание базы данных имеет следующий синтаксис:
create database имя_базы_данных;
Максимальная длина имени БД составляет 64 знака и может включать буквы, цифры, символ «_» и символ «$». Имя может начинаться с цифры, но не должно полностью состоять из цифр. Любой запрос к БД заканчивается точкой с запятой (этот символ называется разделителем — delimiter). Получив запрос, сервер выполняет его и в случае успеха выдает сообщение «Query OK …»
Итак, создадим БД forum:



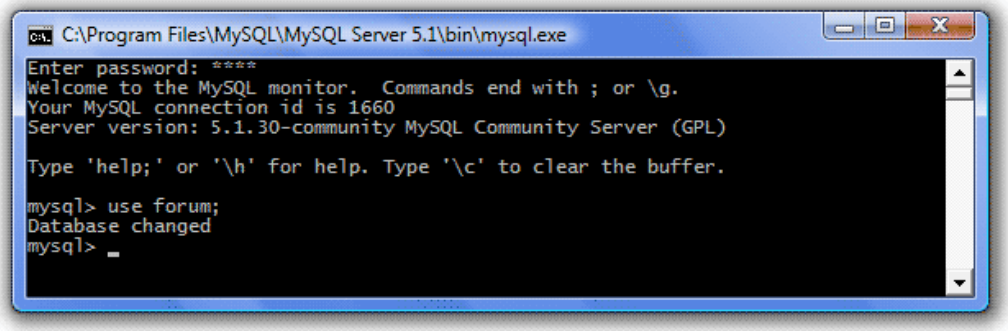
Нажимаем Enter и видим ответ «Query OK …», означающий, что БД была создана:



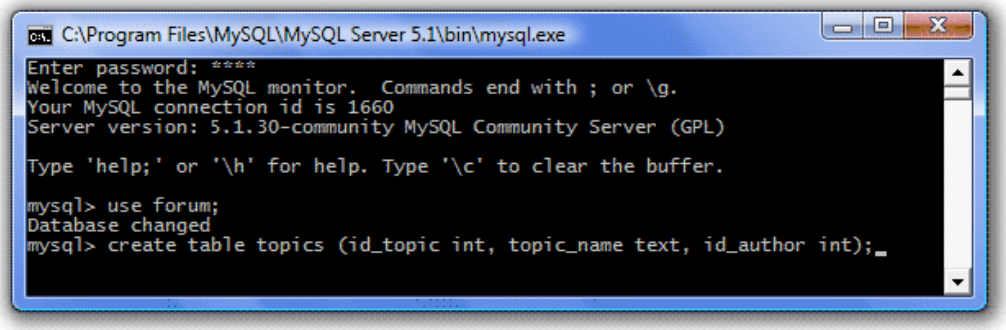
Вот так все просто. Теперь в этой базе данных нам надо создать 3 таблицы: темы, пользователи и сообщения. Но перед тем, как это делать, нам надо указать серверу в какую именно БД мы создаем таблицы, т.е. надо выбрать БД для работы. Для этого используется оператор *use*. Синтаксис выбора БД для работы следующий:
use имя_базы_данных;
Итак, выберем для работы нашу БД forum:



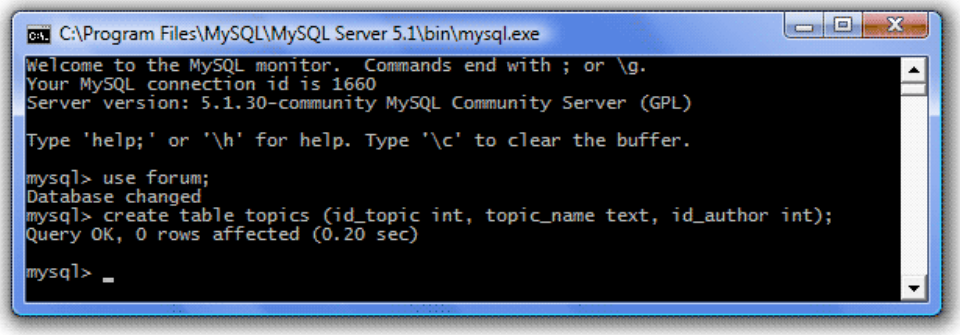
Нажимаем Enter и видим ответ «Database changed» — база данных выбрана.



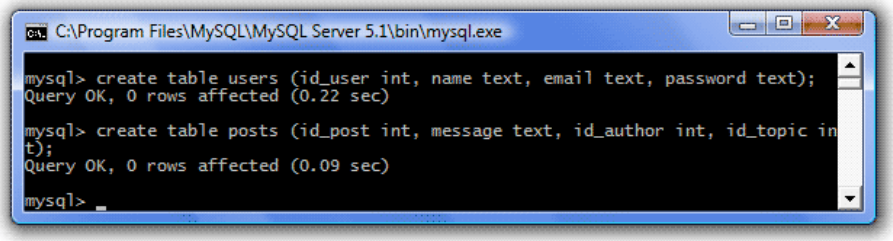
Выбирать БД необходимо в каждом сеансе работы с MySQL.
Для создания таблиц в SQL существует оператор *create table*. Создание базы данных имеет следующий синтаксис:
create table имя_таблицы (имя_первого_столбца тип, имя_второго_столбца тип, ..., имя_последнего_столбца тип);
Требования к именам таблиц и столбцов такие же, как и для имен БД. К каждому столбцу привязан определенный тип данных, который ограничивает характер информации, которую можно хранить в столбце (например, предотвращает ввод букв в числовое поле). MySQL поддерживает несколько типов данных: числовые, строковые, календарные и специальный тип NULL, обозначающий отсутствие информации. Подробно о типах данных мы будем говорить в следующем уроке, а пока вернемся к нашим таблицам. В них у нас всего два типа данных — целочисленные значения (int) и строки (text). Итак, создадим первую таблицу — Темы:



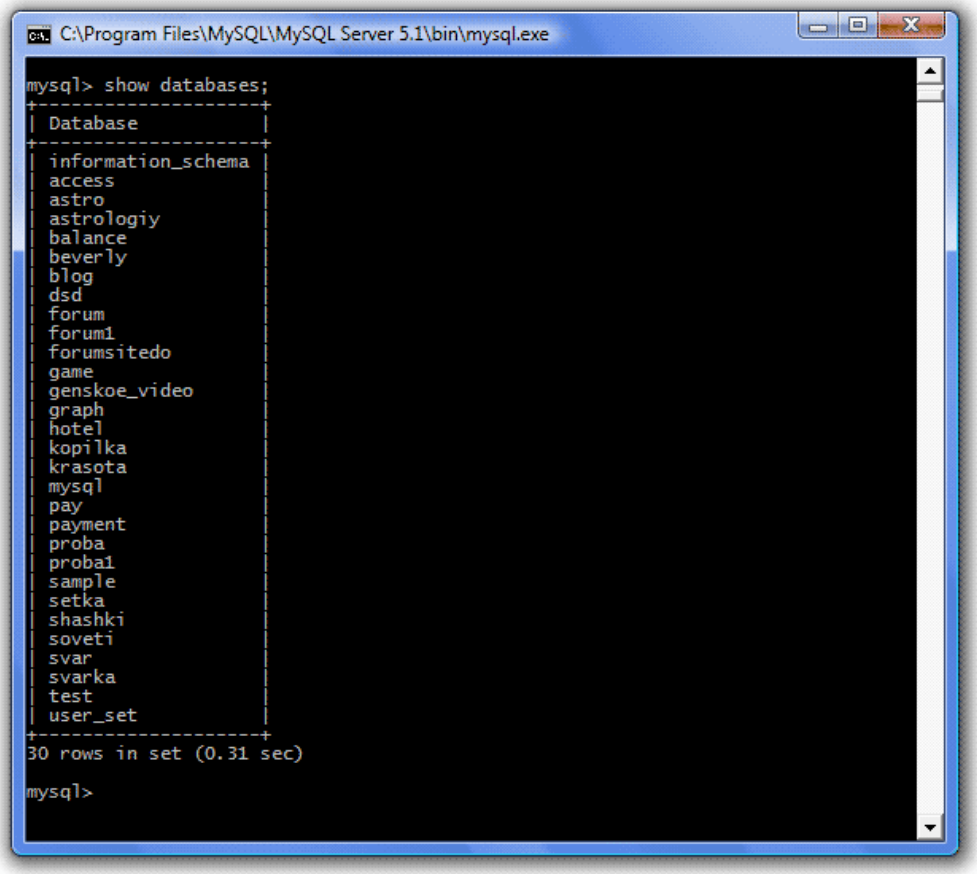
Нажимаем Enter — таблица создана:



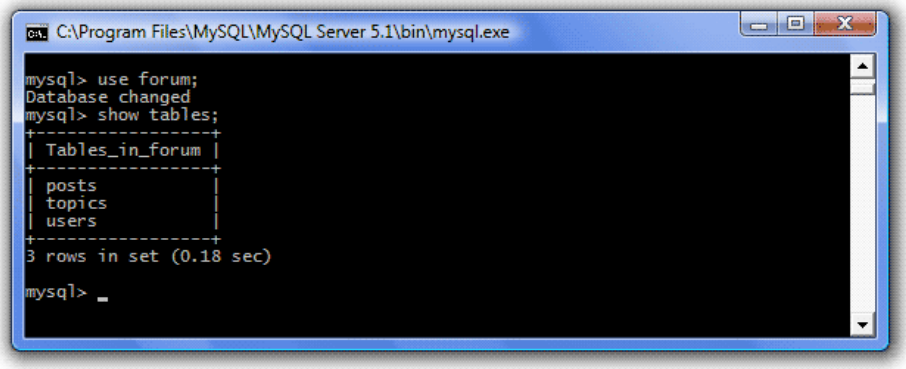
Итак, мы создали таблицу topics (темы) с тремя столбцами:
id_topic int — id темы (целочисленное значение),
topic_name text — имя темы (строка),
id_author int — id автора (целочисленное значение).
Аналогичным образом создадим оставшиеся две таблицы — users (пользователи) и posts (сообщения):



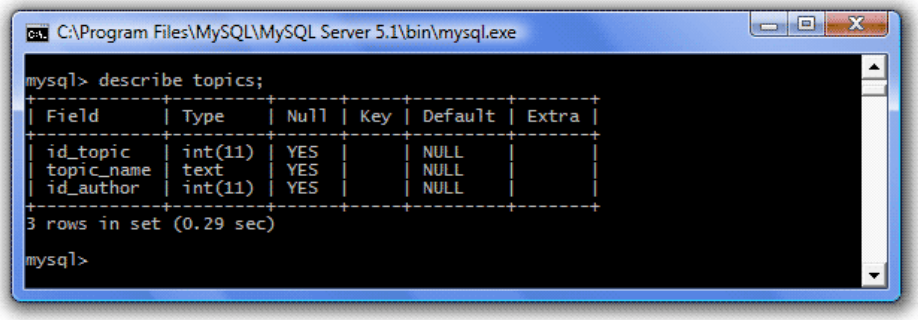
Итак, мы создали БД forum и в ней три таблицы. Сейчас мы об этом помним, но если наша БД будет очень большой, то удержать в голове названия всех таблиц и столбцов просто невозможно. Поэтому надо иметь возможность посмотреть, какие БД у нас существуют, какие таблицы в них присутствуют, и какие столбцы эти таблицы содержат. Для этого в SQL существует несколько операторов:
show databases — показать все имеющиеся БД,
show tables — показать список таблиц текущей БД (предварительно ее надо выбрать с помощью оператора *use*),
describe имя_таблицы — показать описание столбцов указанной таблицы.
Давайте попробуем. Смотрим все имеющиеся базы данных (у вас она пока одна — forum, у меня 30, и все они перечислены в столбик):



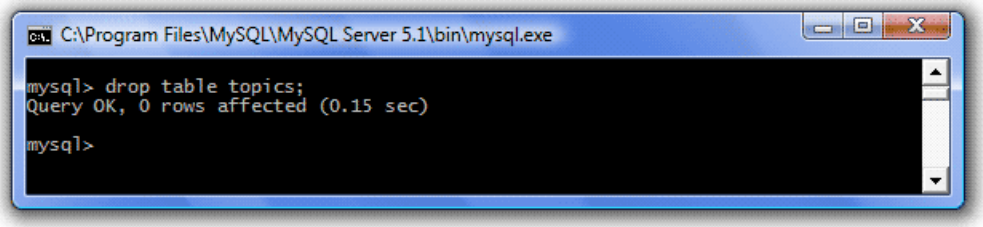
Теперь посмотрим список таблиц БД forum (для этого ее предварительно надо выбрать), не забываем после каждого запроса нажимать Enter:



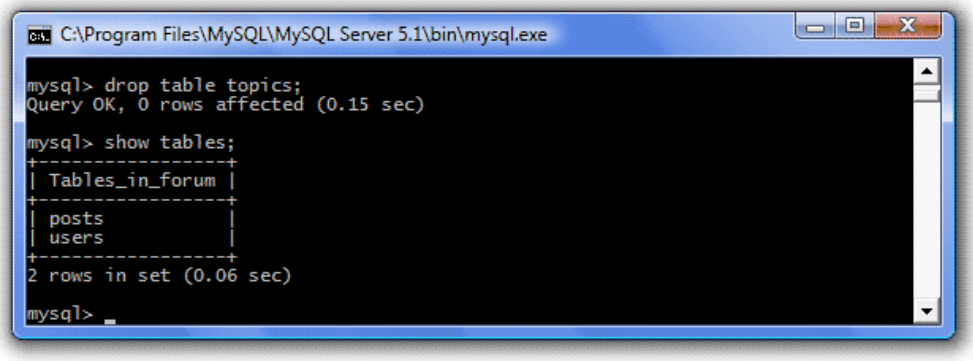
В ответе видим названия наших трех таблиц. Теперь посмотрим описание столбцов, например, таблицы topics:



Первые два столбца нам знакомы — это имя и тип данных, значения остальных нам еще предстоит узнать. Но прежде мы все-таки узнаем какие типы данных бывают, какие и когда следует использовать.
А сегодня мы рассмотрим последний оператор — *drop*, он позволяет удалять таблицы и БД. Например, давайте удалим таблицу topics. Так как мы два шага назад выбирали БД forum для работы, то сейчас ее выбирать не надо, можно просто написать:
drop table имя_таблицы;
и нажать Enter.

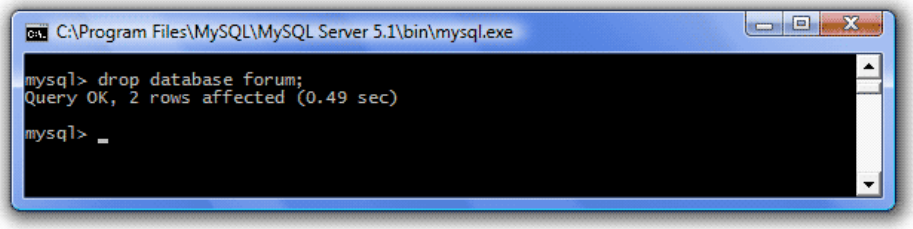


Теперь снова посмотрим список таблиц нашей БД:

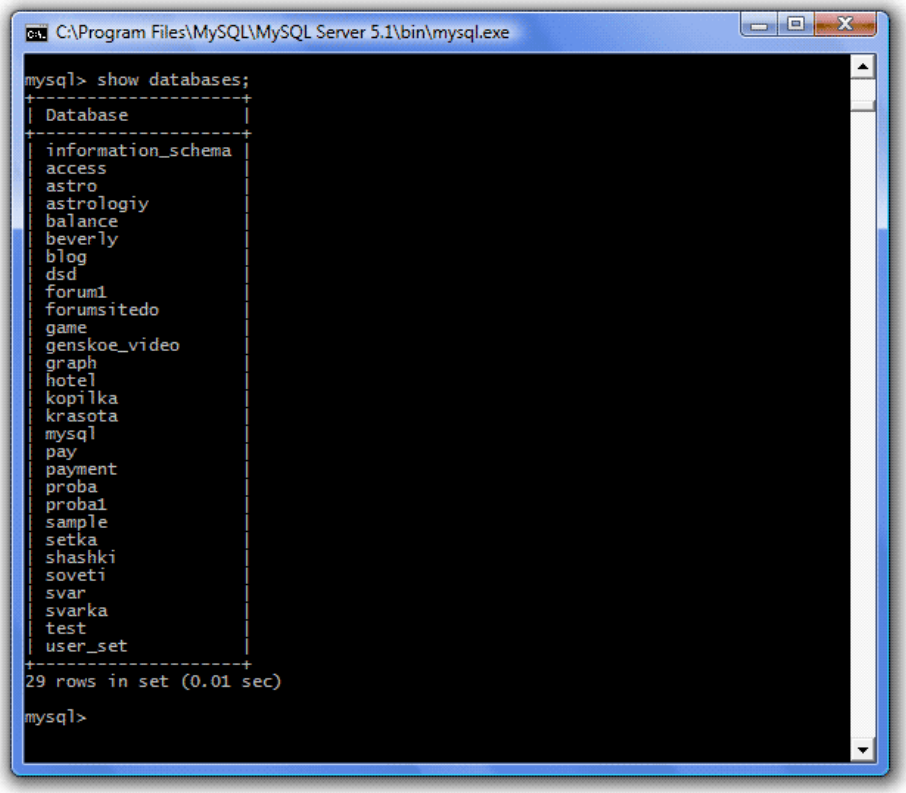


Наша таблица действительно удалена. Теперь давайте удалим и саму БД forum (удаляйте, не жалейте, ее все равно придется переделывать). Для этого напишем:

drop database имя_базы данных;
и нажмем Enter.



И убедитесь в этом, сделав запрос на все имеющиеся БД:



Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;
3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№17

Тема: Работа с журналом аудита базы данных

Цель: изучить модель безопасности операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1.

1.1. Ознакомьтесь с теоретическими основами защиты информации в ОС семейства Windows в настоящих указаниях и конспектах лекций.

1.2. Выполните задания 1.2.1-2.1.8

1.2.1. При выполнении лабораторной работы запустите в программе Oracle VM Virtualbox виртуальную машину Win7Test. Войдите в систему под учетной записью администратора. Все действия в пп 2.2.1-2.2.8 выполняйте в системе, работающей на виртуальной машине.

1.2.2. Создайте учетную запись нового пользователя testUser в оснастке «Управление компьютером» (compmgmt.msc). При создании новой учетной записи запретите пользователю смену пароля и снимите ограничение на срок действия его пароля. Создайте новую группу ”testGroup” и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске C: папку forTesting. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt).

1.2.3. С помощью команды runas запустите сеанс командной строки (cmd.exe) от имени вновь созданного пользователя. Командой whoami посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя. Строку запуска и результат работы этой и всех следующих консольных команд копируйте в файл протокола лабораторной работы.

1.2.4. Убедитесь в соответствии имени пользователя и полученного SID в реестре Windows. Найдите в реестре, какому пользователю в системе присвоен SID S-1-5-21-1957994488-492894223-170857768-1004 (Используйте ключ реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList).

1.2.5.Командой whoami пользователя testUser. В сеансе командной строки пользователя попробуйте изменить системное время командой time. Чтобы предоставить пользователю подобную привилегию, запустите оснастку «Локальные параметры безопасности» (secpol.msc). Добавьте пользователя в список параметров политики «Изменение системного времени» раздела Локальные политики -> Назначение прав пользователя. После этого перезапустите сеанс командной строки от имени пользователя, убедитесь, что в списке привилегий добавилась SeSystemtimePriviege. Попробуйте изменить системное время командой time. Убедитесь, что привилегия «Завершение работы системы» (SeShutdown-Privilege) предоставлена пользователю testUser . После этого попробуйте завершить работу системы из сеанса командной строки пользователя командой shut-down –s. Добавть ему привелегию «Принудительное удаленное завершение» (SeRemoteShutdownPrivilege). Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выполнения можно командой shutdown –a).

1.2.6. Ознакомьтесь с справкой по консольной команде icacls. Используя эту команду, просмотрите разрешения на папку c:\forTesting. Объясните все обозначения в описаниях прав пользователей и групп в выдаче команды.

а) Разрешите пользователю testUser запись в папку forTesting, но запретите запись для группы testGroup. Попробуйте записать файлы или папки в forTesting от имени пользователя testUser. Объясните результат. Посмотрите эффективные разрешения пользователя testUser к папке forTesting в окне свойств папки.

б) Используя стандартное окно свойств папки, задайте для пользователя testUser такие права доступа к папке, чтобы он мог записывать информацию в папку forTesting, но не мог просматривать ее содержимое. Проверьте, что папка forTesting является теперь для пользователя testUser “слепой”, запустив, например, от его имени файловый менеджер и попробовав записать файлы в папку, просмотреть ее содержимое, удалить файл из папки.

в) Для вложенной папки forTesting\Docs отмените наследование ACL от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя папка forTesting\Docs перестала быть “слепой” (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл).

г) Снимите запрет на чтение папки forTesting для пользователя testUser. Используя команду icacls запретите этому пользователю доступ к файлам с расширением txt в папке forTesting. Убедитесь в недоступности файлов для пользователя.

д) Командой icacls запретите пользователю все права на доступ к папке forTesting и разреште полный доступ к вложенной папке forTesting\Docs. Убедитесь в доступности папки forTesting\Docs для пользователя. Удалите у пользователя testUser привилегию

SeChangeNotifyPrivilege. Попробуйте получить доступ к папке forTesting\Docs. Объясните результат.

е) Запустите файловый менеджер от имени пользователя testUser и создайте в нем папку newFolder на диске C. Для папки newFolder очистите весь список ACL командой cacls. Попробуйте теперь получить доступ к папке от имени администратора и от имени пользователя. Кто и как теперь может вернуть доступ к папке? Верните полный доступ к папке для всех пользователей.

ж) Создайте в разделе HKLM\Software реестра раздел testKey. Запретите пользователю testUser создание новых разделов в этом разделе реестра. Создайте для раздела HKLM\Software\testKey SACL, позволяющий протоколировать отказы при создании новых подразделов, а также успехи при перечислении подразделов и запросе значений (предварительно проверьте, что в локальной политике безопасности соответствующий тип аудита включен). Попробуйте от имени пользователя testUser запустить regedit.exe и создать раздел в HKLM\Software. Убедитесь, что записи аудита были размещены в журнале безопасности (eventvwr.msc).

з) С использованием команды whoami проверьте уровень целостности для пользователя testUser и администратора (учетная запись ВПИ). Запустите какое-нибудь приложение (калькулятор, блокнот) от имени testUser и администратора. С использованием утилиты ProcessExplorer (можно найти в папке c:\Utils на виртуальной машине) проверьте уровень целостности запущенных приложений. Объясните разницу. Верните пользователю testUser права на полный доступ к папке forTesting. От имени администратора создайте в папке forTesting текстовый файл someText.txt. Измените уровень целостности этого файла до высокого с использованием команды icacls. Запустите блокнот от имени пользователя testUser, откройте в нём файл someText.txt, измените содержимое файла и попробуйте сохранить изменения. Объясните причину отказа в доступе. Как можно предоставить пользователю testUset доступ к файлу?

1.2.7. Шифрование файлов и папок средствами EFS.

а) От имени пользователя testUser зашифруйте какой-нибудь файл на диске. Убедитесь, что после этого был создан сертификат пользователя, запустив оснастку certmgr.msc от имени пользователя (раздел Личные). Просмотрите основные параметры сертификата открытого ключа пользователя testUser (срок действия, используемые алгоритмы). Установите доверие к этому сертификату в вашей системе.

б) Создайте в папке forTesting новую папку Encrypt. В папке Encrypt создайте или скопируйте в нее текстовый файл. Зашифруйте папку Encrypt и все ее содержимое из меню свойств папки от имени администратора. Попробуйте просмотреть или скопировать какой-нибудь файл этой папки от имени пользователя testUser. Объясните результат. Скопируйте зашифрованный файл в незашифрованную папку (например, forTesting). Убедитесь что он остался зашифрованным. Добавьте пользователя testUser в список имеющих доступа к файлу пользователей в окне свойств шифрования файла. Повторите попытку получить доступ к файлу от имени пользователя testUser.

в) Создайте учетную запись нового пользователя agentUser, сделайте его членом группы Администраторы. Определите для пользователя agentUser роль агента восстановления EFS. Создайте в папке forTesting новый текстовый файл с произвольным содержимым. Зашифруйте этот файл от имени пользователя testUser. Убедитесь в окне подробностей шифрования файла, что пользователь agentUser является агентом восстановления для данного файла. Попробуйте прочитать содержимое файла от имени администратора и от имени пользователя agentUser. Объясните результат.

г) Зашифруйте все текстовые файлы папки forTesting с использованием консольной команды шифрования cipher от имени пользователя testUser (предварительно снимите запрет на доступ к этим файлам, установленный в задании 2.2.6г).

д) Убедитесь, что при копировании зашифрованных файлов на том с файловой системой, не поддерживающей EFS (например, FAT32 на флеш-накопителе), содержимое файла дешифруется.

1.2.8. После демонстрации результатов работы преподавателю восстановите исходное состояние системы: удалите созданные папки и файлы, разделы реестра, удалите учетную запись созданного пользователя и его группы, снимите с пользователя agentUser роль агента восстановления.

1.2.9. Представьте отчёт по лабораторной работе преподавателю и отчитайте работу.

Форма отчета:

-название и цель работы;

-протокол выполнения лабораторной работы, содержащий список консольных команд, составленных при выполнении работы, и результаты их выполнения.

Практическое занятие№18

Тема: Мониторинг нагрузки сервера

Цель: отработать навыки по мониторингу нагрузки сервера

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1. Заполните пропуски

WindowsAPI (Application Programming Interface) - _____
_____
_____
_____
_____

API состоит из большого количества динамических библиотек и содержит множество функций, которые прикладные программы могут использовать для взаимодействия с операционной системой. Каждая операционная система реализует различную подмножество Windows API.

API выполняет роль связующего звена между приложениями и операционной системой. Windows API содержит несколько тысяч функций, сгруппированы в следующие основные категории: _____
_____
_____
_____
_____
_____
_____
_____

API содержит совокупность функций, которые доступны программистам при разработке программ - их называют _____ К ним относятся
_____
_____

Функции ядра - _____
_____
_____
_____
_____

К службам относятся процессы, которые запускаются диспетчером управления служб. Они, как правило, работают в фоновом режиме независимо от других приложений и предназначенны для обслуживания определенных потребностей пользователя или системы. Например, служба TaskScheduler-планировщик, который позволяет управлять запуском других программ.

Windows содержит большой набор функций (подпрограмм), объединенных в отдельные бинарные файлы, которые программы могут динамически загружать во время своего выполнения. Такие библиотеки функций называют _____

_____
_____

Различные программные механизмы, которые операционная система предоставляет программистам для выполнения определенных действий, называют также сервисами, поскольку они предназначены для обслуживания различных потребностей пользователя системы. К таким сервисам относятся _____ Отдельное подмножество составляют неуправляемые системные сервисы (или исполнительные системные сервисы). Они охватывают недокументированные низкоуровневые сервисы операционной системы, которые можно вызвать в пользовательском режиме.

Когда в среде Windows запускается прикладная программа, система создает специальный объект - _____, - который _____. Может показаться, что программа и процесс - понятие похожие, они фундаментально отличаются. Программа - _____, а процесс - _____

Известная утилита для анализа активности процессов-системныйTaskManager (_____). В ядре Windows нет такого понятия, как задачи, поэтому TaskManager _____

Диспетчер задач Windows отображает список активных процессов. Его можно запустить различными способами: _____

В этом окне процессы идентифицируются по имени образа, экземплярами которого они являются. В отличие от других объектов в Windows процессам нельзя присваивать глобальные имена.

Если вкладка Processes окна диспетчера задач показывает список процессов, то содержание вкладки Applications (приложения) отображает список видимых окон верхнего уровня всех объектов "рабочий стол" интерактивного объекта WindowStation. Столбик Status (состояние) _____. Состояние "Running" ("выполняется") _____, aNot Responding ("не отвечает ") - _____

Вкладка Applications позволяет _____

Для предотвращения доступа приложений к критически важным данным операционной системы и устранения риска их модификации Windows использует два режима доступа к процессору (даже если он поддерживает более двух режимов): _____. Код программ работает в _____, тогда как код операционной системы (например, системные сервисы и драйверы устройств) - в _____. В режиме ядра предоставляется доступ ко всей системной памяти и разрешается выполнять любые машинные команды процессора.

Прикладные программы _____ Переключение с пользовательского режима в режим ядра осуществляется _____ _____. Операционная система _____. Перед возвращением управления пользовательскому потоку процессор переключается обратно в пользовательский режим. Благодаря этому операционная система _____

Поэтому ситуация, когда пользовательский поток часть времени работает в пользовательском режиме, а часть - в режиме ядра, обычная. Поскольку подсистема, отвечающая за поддержку графики и окон, функционирует в режиме ядра, то программы, интенсивно работающих с графикой, большую часть времени действуют в режиме ядра, а не в пользовательском режиме. Самый простой способ проверить это -

_____
_____
_____
_____
_____

Задание 2. Диспетчере задач.

Задание 2.1. Просмотр состояния процессов через диспетчер задач.

Просмотр и анализ взаимосвязей процессов и потоков.

Запустите диспетчер задач. Переключитесь на закладку Процессы. В меню Вид выберите пункт Выбрать столбцы… и укажите столбцы согласно рисунка 1. ***Сделайте скриншот вашей работы и сохраните его под именем «Выбор столбцов диспетчера задач»***

Потом определите сколько процессов запущено системой. Для этого я передите на закладку Быстродействие и в меню Вид выберите пункт Загрузка ЦП. (см. рис.2) Например: из рисунка мы видим что системой запущено 53 процесса, загрузка ЦП колеблется от 3-5%, файл подкачки загружен на 931 МБ. ***Сделайте скриншот вашей работы и сохраните его под именем Диспетчер задач. Вкладка "Быстродействие"»***

Теперь запускаем приложение Paint и смотрим на изменения ЦП. Например в примере: загрузка ЦП колеблется в пределах 1-4%, файл подкачки загрузился на 942 МБ. Если сравнить объёмы используемого файла подкачки и доступной физической памяти, то можно сделать вывод что в сумме они дают общий объем физической памяти.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 3. Результат после запуска приложения Paint». Напишите в каких пределах колеблется загрузка ЦП, как изменился файл подкачки.

Просмотр времени работы системы в пользовательском режиме и режиме ядра.

Переключитесь на закладку Быстродействие и в меню Вид выберите пункт Вывод времени ядра. Быстро прокручиваем страницы любого текстового документа. На индикаторе Загрузка ЦП процент работы процессора в пользовательском режиме отражается зеленым цветом, в режиме ядра красным. Из рисунка четко видны изменения работы процессора при прокрутке страниц.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 4. Состояние системы при прокрутке страниц»

Задание 2.2. Просмотр сведений о поддержке многопроцессорных систем.

Согласно следующему заданию откройте диспетчер устройств (Пуск – Панель управления – Диспетчер устройств). В списке устройств раскройте узел Компьютер. В окне свойств (Правой кнопкой свойства) перейдите на закладку Драйвер и с помощью кнопки Сведения просмотрите сведения о файлах драйверов (см. Рисунок 5).

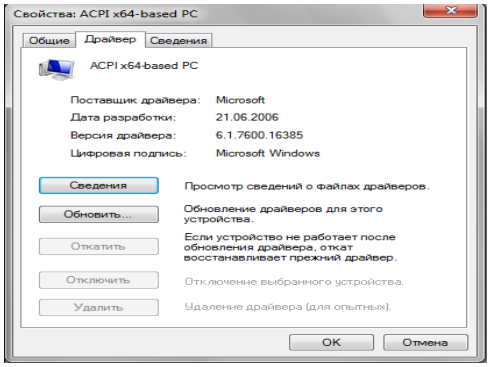


Рисунок 5. Сведения о файлах поддержки многопроцессорных систем

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 5. Сведения о файлах поддержки многопроцессорных систем»

Задание 2.3. Изучение отношения процессов родитель-потомок

1. Запустите командную строку (Пуск – Все программы – Стандартные – Командная строка)

2. Потом наберите startcmd для запуска второго окна командной строки.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 6. Запуск окон командной строки»

3. Далее я откройте диспетчер задач.

4. Переключился на второе окно командной строки.

5. Ввелmspaintдлязапуска Microsoft Paint.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 7. Запуск приложения Paint»

6. Потом выберите второе окно командной строки.

7. Ввел команду exit, тем самым завершив работу второго окна.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 8. Завершение работы второго окна»

8. Потом переключитесь в диспетчер задач. Откройте его вкладку Приложения. Щелкнул правой кнопкой мыши задачу Командная строка (cmd.exe) и выбрал Перейти к процессу.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 9. Диспетчер задач. Переход к процессу cmd.exe»

11. Щелкните процесс Cmd.exe, выделенный цветом.

12. Щелкнув правой кнопкой мыши, выберите команду Завершить дерево процессов.

13. В окне Предупреждение диспетчера задач щелкните кнопку Завершить дерево процессов.

Первое окно командной строки исчезнет, но окно Paintпо прежнему работает.

Сделайте скриншот вашей работы и сохраните его под именем «Рисунок 10. Диспетчер задач. Переход к процессу cmd.exe»

Контрольные вопросы

1. Что такое WindowsAPI
2. Что такое процессы
3. Что такое потоки
4. Что такое задачи
5. Что такое диспетчер задач

Форма отчета: отчетная работа

Практическое занятие№19

Тема: Настройка политики безопасности

Цель: ознакомиться с методами ограничения доступа к информации

Оборудование: тетрадь, ручка, ПК

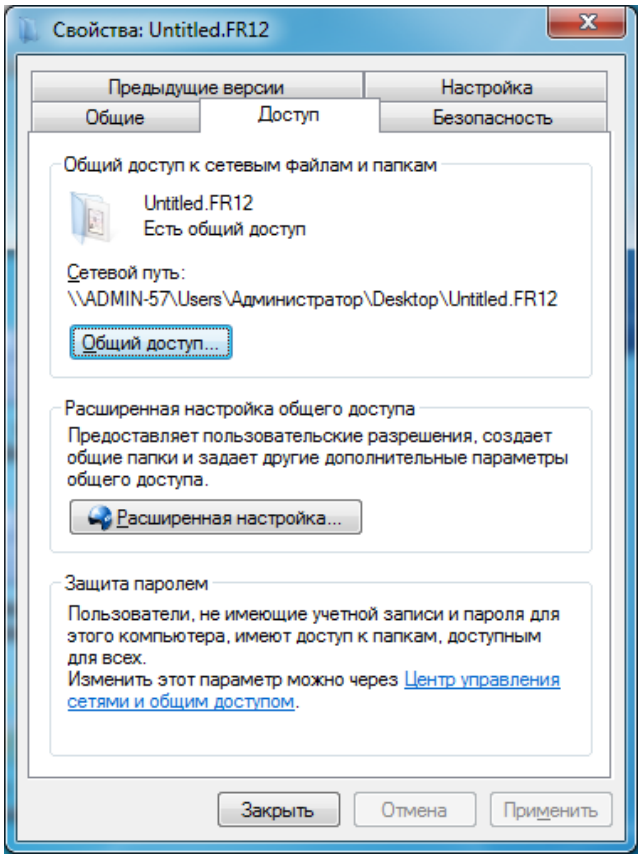
Методические указания: выполните задания

Ход выполнения:

Задание – можно ничего не менять в своих настройках. Просто прогуляйтесь по указанным путям и сделайте соответствующие скрин-шоты.

1. *Освоить средства разграничения доступа пользователей к папкам*:

- выполнить команду «Общий доступ и безопасность» контекстного меню папки (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки) или команду «Свойства»;
- открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;
- с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);
- включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;
- открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;
- открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;



- закрыть окно дополнительных параметров безопасности.

2. *Освоить средства разграничения доступа пользователей к файлам*:

- выполнить команду «Свойства» контекстного меню файла;
- повторить все задания п. 1, но применительно не к папке, а к файлу.

3. *Освоить средства разграничения доступа к принтерам*:

- выполнить команду «Принтеры и факсы» меню «Пуск»;
- выполнить команду «Свойства» контекстного меню установленного в системе принтера;
- повторить все задания п. 1, но применительно не к папке, а к принтеру.

4. *Освоить средства разграничения доступа к разделам реестра операционной системы*:

- с помощью команды «Выполнить» меню «Пуск» запустить программу редактирования системного реестра regedit (regedt32);

- с помощью команды «Разрешения» меню «Правка» редактора реестра определить сведения о правах доступа пользователей к корневым разделам реестра, их владельцах и параметрах политики аудита;
- включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце.

Форма отчета:

1. Тему и цель работы
2. Экранные копии выполнения работы
3. Составьте матрицу доступа по своей (курсовой) ИС.
4. Ответы на контрольные вопросы.

Контрольные вопросы:

1. В чем достоинства дискреционной политики безопасности?
2. В чем недостатки мандатной политики безопасности?
3. Кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
4. В чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам?
5. В чем отличие определения прав на доступ к принтерам по сравнению с определением прав на доступ к папкам и файлам?
6. В чем отличие определения прав на доступ к разделам реестра по сравнению с определением прав на доступ к папкам и файлам?

Практическое занятие№20

Тема: Создание резервных копий базы данных

Цель: формирование знаний по осуществлению резервного копирования и восстановления данных; ознакомление с функциями, методами работы и видами программ-архиваторов.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1. необходимо создать резервные копии базы данных «МММ» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.

Ход работы:

1. Запустите SQL Server Management Studio (SSMS), подключитесь к своему экземпляру SQL Server, используя технологию 1.
2. Создайте папку с именем c:\Student\ВашаПапка\test.
3. Откройте окно нового запроса. Измените контекст на базу данных master, используя технологию 6. Наберите и исполните следующую команду, чтобы создать полную резервную копию базы данных:

BACKUP DATABASE MMM TO DISK = 'C:\.....TEST\AW.BAK’

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

4. Внесите изменение в таблицу «Модель» базы данных МММ. Добавьте одну запись (придумайте сами)/
5. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать резервную копию журнала транзакций и сохранить только что внесенное изменение:

BACKUP LOG MMM TO DISK = ‘C:\.....TEST\AW1.TRN'

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

6. Внесите еще одно изменение в таблицу«Модель».
7. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать разностную резервную копию базы данных:

BACKUP DATABASE MMM TO DISK = ‘C:\.....\TEST\AWDIFF1.BAK' WITH DIFFERENTIAL

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

8. Внесите еще одно изменение в таблицу«Модель».

9. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать полную резервную копию базы данных в указанном месте на диске:

BACKUP LOG MMM TO DISK = ‘C:\....TEST\AW2.TRN'

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

Задание №2. необходимо провести восстановление базы данных «MMM» из сделанных в задании №1 резервных копий.

Ход работы:

1. Если необходимо, запустите SSMS, подключитесь к своему экземпляру SQL Server, используя технологию 1.

2. Выполните восстановление БД из первой полной резервной копии (C:\...TEST\AW.BAK) средствами оболочки SSMS. Для этого выполните:

- В обозревателе объектов вызовите контекстное меню на вашей БД и выберите задачу восстановления базы данных (см. рисунок 6).

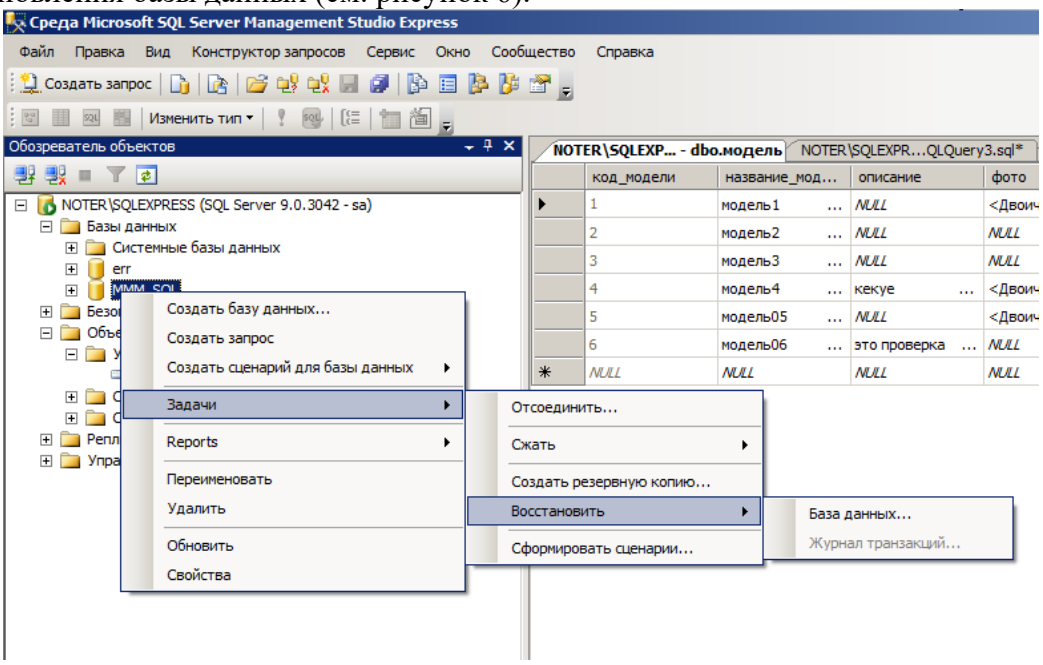


Рисунок 6 – Восстановление БД

- В открывшемся окне необходимо задать следующие параметры восстановления

На закладке «Общие» необходимо выбрать:

1. Базу данных для восстановления (вашу MMM)

2. Выбрать источник набора данных для восстановления с устройства ◊ файл C:\...TEST\AW.BAK

3. После определения файла-источника данных необходимо флажком выбрать базу данных для восстановления (рисунок 7).

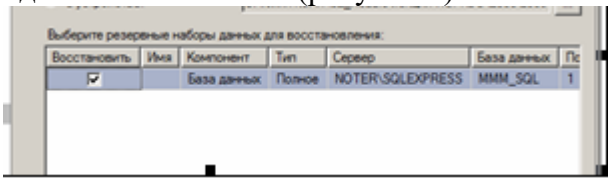


Рисунок 7- Выбор БД для восстановления

На закладке «Параметры»

1. необходимо включить опцию «Перезаписать БД» и «оставить БД готовой к использованию», (рисунок 8).

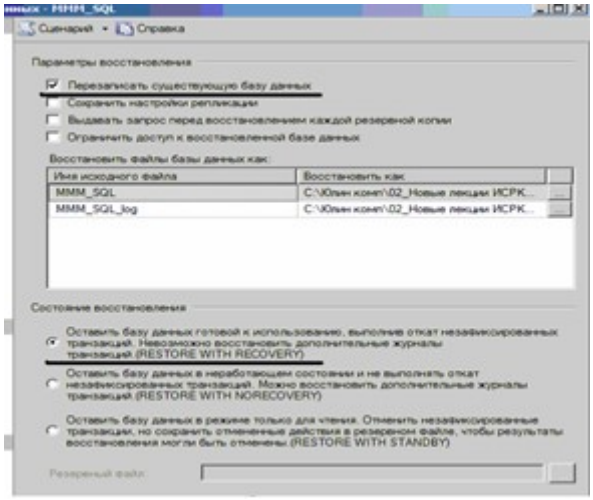


Рисунок 8 – Задание параметров восстановления

3. Нажмите ОК

4. После восстановления БД, откройте таблицу «Модель» и убедитесь, что она не содержит всех добавлений, вносимых вами в процессе выполнения упражнения, так как восстановление происходило из первой резервной копии (без изменений).

Задание №3. необходимо организовывать со стороны клиентского приложения, созданного в Visual Studio удаленное администрирование БД (резервное копирование).

Ход работы:

В Visual Studio

1. Создайте новый проект Windows Application и сохраните его в своей папке под именем Лабы_MMM_2 семестр.

2. В главную форму добавьте меню, изображенное на рисунке 9:

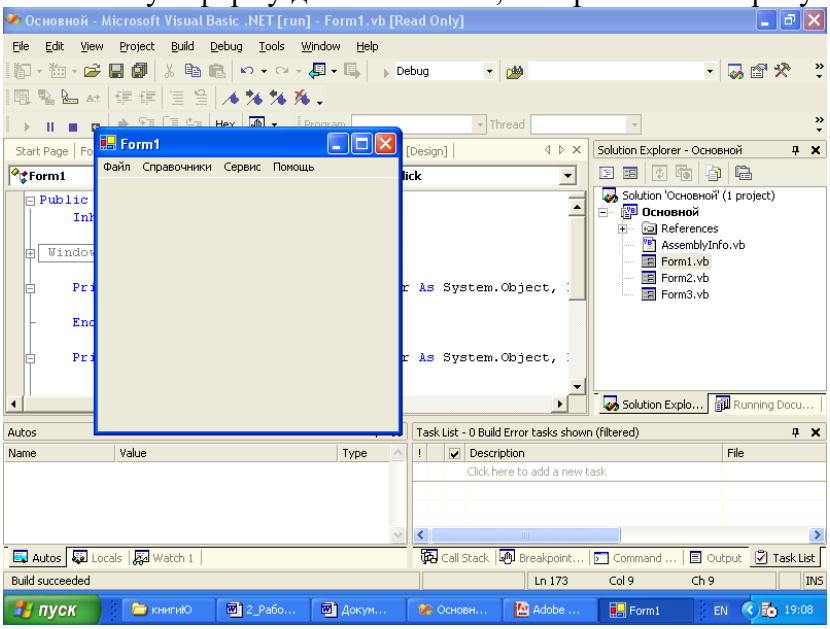


Рисунок 9 – Главное меню проекта

Файл (Открыть, Закрыть, Выход)

Справочники (Модель, Магазин, Дерево моделей)

Заказы (Работа с заказами)

Отчеты (Прайс-лист, Бланк заказов)

Администрирование БД (Резервное копирование, Безопасность)

Сервис (Калькулятор)

Помощь (Справка, О программе)

3. Добавьте новую форму в проект

4. Добавьте на только что созданную форму компоненты в соответствии с рисунком 10.

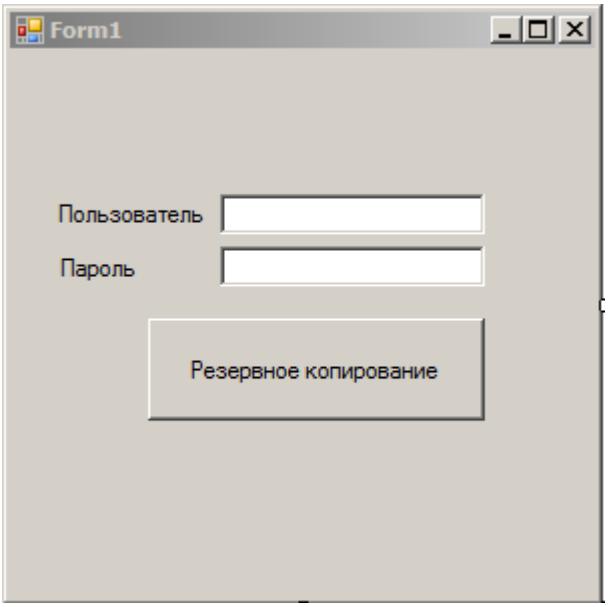


Рисунок 10 – Форма для подключения к серверу

5. Обеспечьте функциональную работу формы (напишите обработчик кнопки «Резервное копирование» с использованием объектов SMO. Описание объектов SMO, их свойств и методов см. в лекционном материале.)

6. Добавьте возможность открытия данной формы при выборе в главной форме пункта меню Администрироване БД ◊ Резервное копирование

7. Запустите проект, проверьте работу формы.

8. Закройте проект

9. Убедитесь в появлении файла резервной копии на диске (файл, который указан в тексте программы).

10. Откройте SSMS. Добавьте в таблицу «Модель» новую строку данных (самостоятельно).

11. Средствами оболочки SSMS, выполните восстановление БД из резервной копии, созданной вашей программой

12. Убедитесь, что после восстановления добавленных строк в таблице «Модель» нет.

Задание №4. Ответьте на вопросы теста и представьте результаты преподавателю.

1. Вы выполняете разностное резервное копирование базы длимых AdveniurtWorks каждые четыре часа, начиная с 04:00. полная резервная копия создается в полночь. Какие данные будут содержаться в разностной резервной копии сделанной в полдень?

1. A Страницы данных, измененные после полуночи.
2. B. Экстенты, измененные после полуночи.
3. C. Страницы данных, измененные после 08:00
4. D. Экстенты. измененные после 08:00.

2. Вы выполняете полное резервное копирование базы данных Adventure Wortks,, которое завершается в полночь. Разностное резервное копирование выполняется по расписанию каждые четыре часа, начиная с 04:00. Резервное копирование журнала транзакций происходит по расписанию каждые пять минут. Какую информацию будет содержать резервная копия журнала транзакций, созданная в 09:15?

1. A. Все транзакции, начатые после 09:10.
2. B. Транзакции, завершенные после 09:10.
3. C. Страницы, измененные после 09:10.
4. D. Экстенты, измененные после 09:10.

Форма отчета: оформление отчета. Отчет о практической работе должен содержать следующие данные:

1. Дату проведения работы;
2. Цель работы;

3. Тему (название);
4. Ход работы, выполненный в тетради;
5. Файл выполненной работы.

Практическое занятие№21

Тема: Восстановление базы данных

Цель: научиться создавать резервные копии с помощью программы **Cobian Backup**

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1

1. Выполнить установку и настройку
2. Составить задание для резервного копирования папки
3. Проверить выполнение задания и продемонстрировать задание в **Cobian Backup**

Установка и настройка **Cobian Backup**

Cobian Backup – программа, позволяющая осуществлять резервное копирование данных.

Основные возможности Cobian Backup:

- Возможность игнорировать или включать объекты в архив.
- Обеспечена полная поддержка протокола FTP в обоих направлениях.
- Архивы Zip и 7-Zip могут включать пустые каталоги.
- Работа со службой фонового копирования данных.
- Тонкая настройка пользовательского интерфейса.
- Улучшенная система запуска и остановки сервиса.
- Не конфликтует с антивирусным программным обеспечением.
- Работа с атрибутами файлов.
- Содержит раздел часто задаваемых вопросов и ответов.
- Многоязычная локализация пользовательского интерфейса.

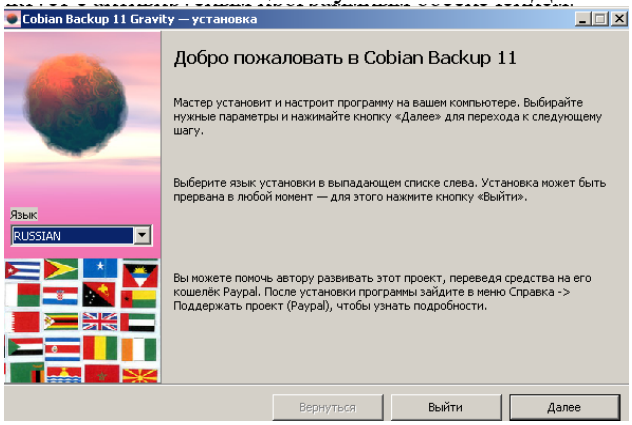
Cobian Backup умеет:

- Создавать резервные копии папок, вложенных папок и файлов.
- Запускать процедуру создания резервной копии вручную или автоматически – регулярно в указанное пользователем время.
- Сжимать резервные копии встроенным архиватором и защищать их с помощью стойких шифров.
- Сохранять резервные копии на удаленном сервере.

Установка и настройка Cobian Backup

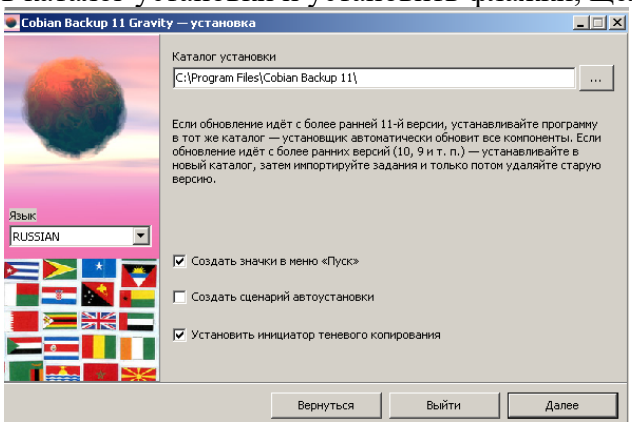
Запустить инсталляционный пакет cbsetup.exe с D:\programm_stud\backup

Указать язык RUSSIAN и щелкнуть по кнопке Далее.

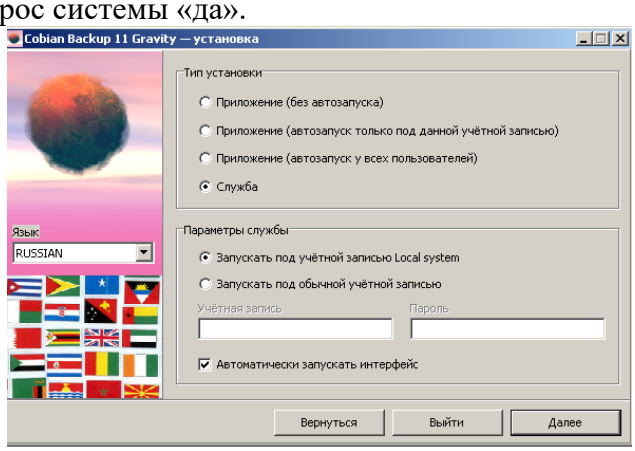


– Принять лицензионное соглашение и щелкнуть по кнопке Далее

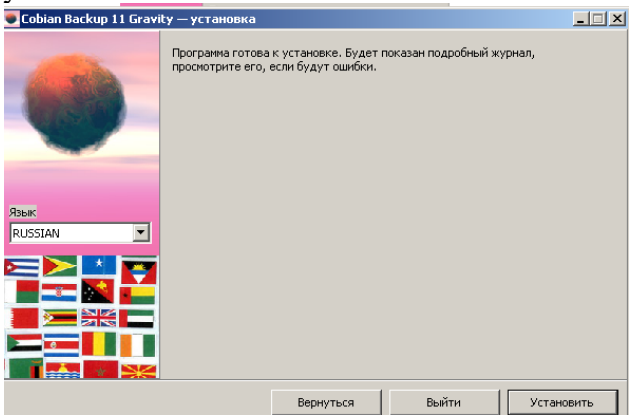
– Указать каталог установки и установить флажки, щелкнуть пор кнопке Далее



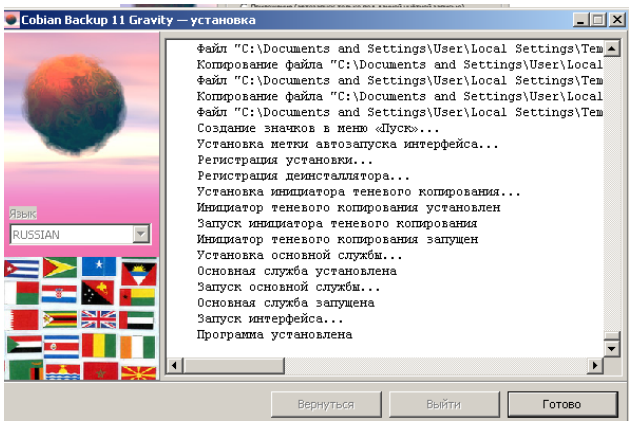
– Указать тип установки и параметры службы(если необходимо обращение к серверу, то указать Запускать под обычной учетной записью), щелкнуть по кнопке Далее. Ответить на вопрос системы «да».



– Щелкнуть по кнопке Установить.



– Проследить за сообщениями системы. Щелкнуть по кнопке Готово

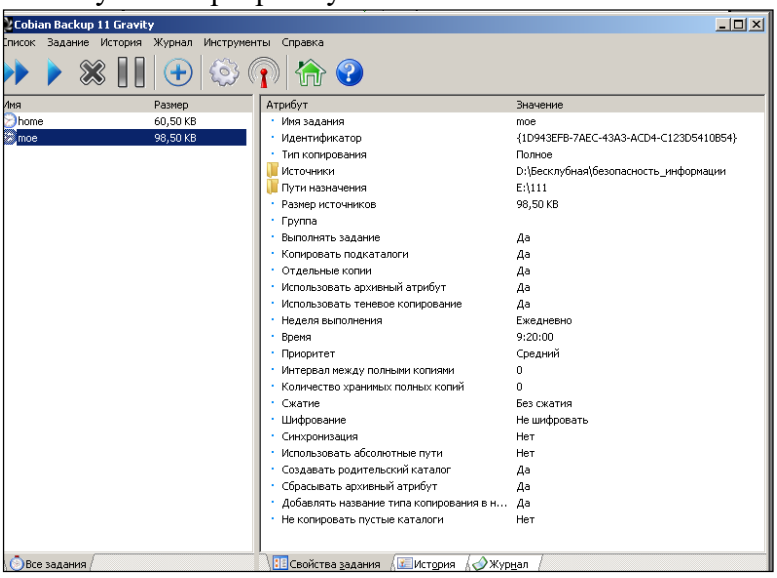


Задание для резервного копирования папки

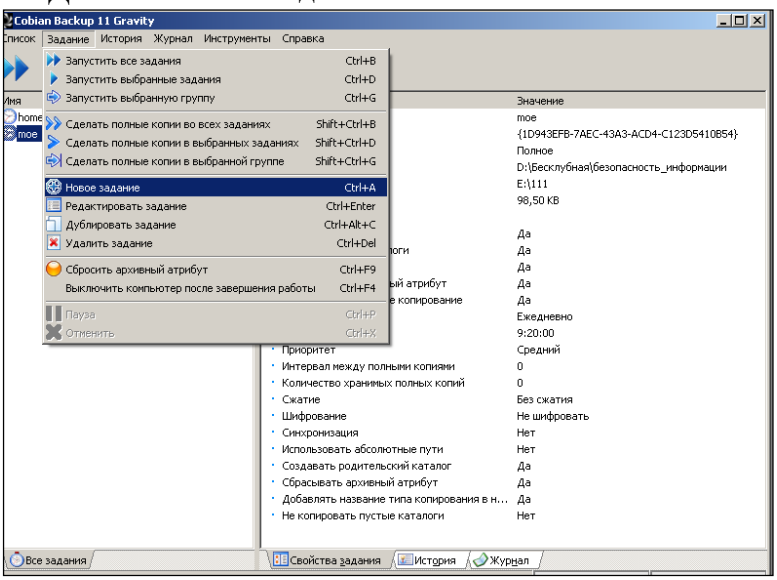
Необходимо ежедневно в 9:20 выполнять резервное копирование с диска D: важной для Вас папки на внешний носитель (флешка).

Выполнение задания.

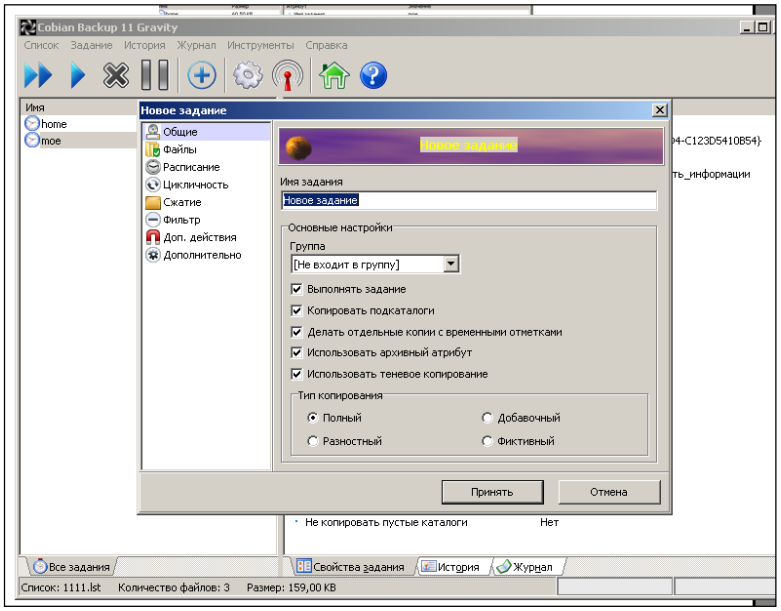
1. Запустить программу



2. Добавить новое задание

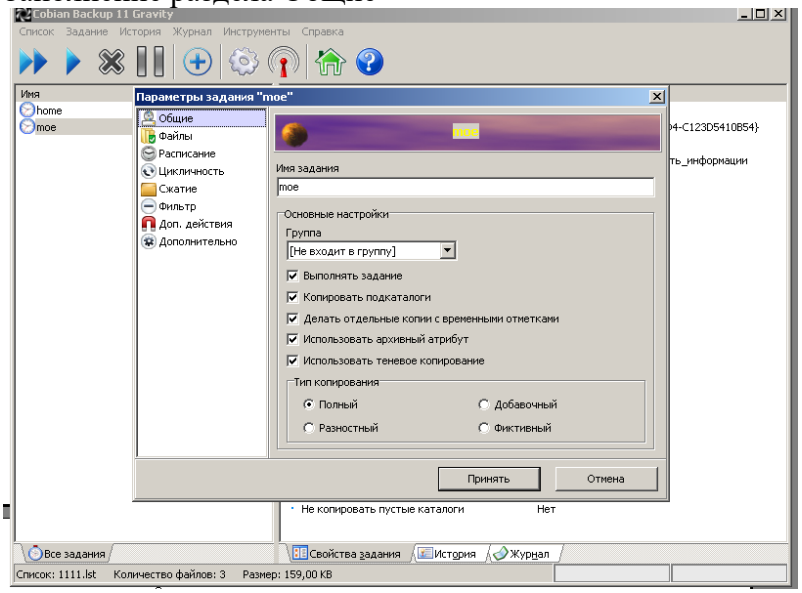


Далее описываем новое задание

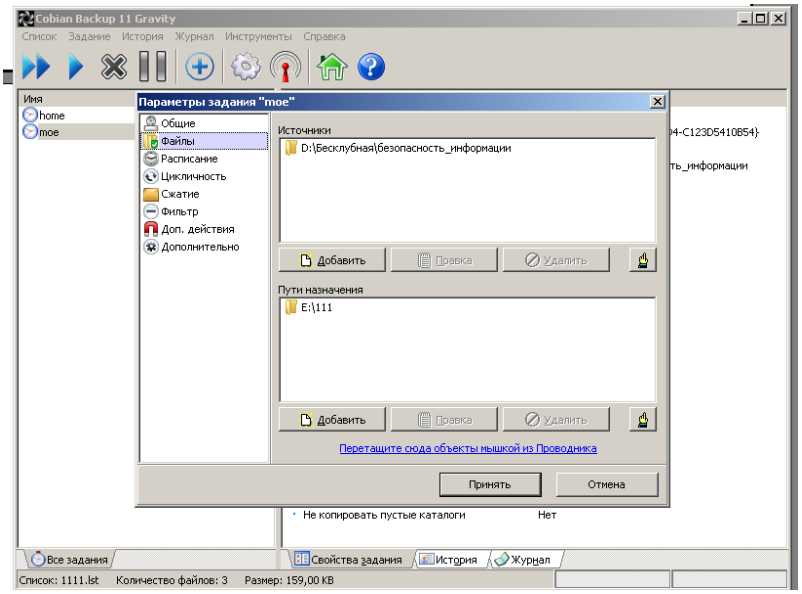


Например:

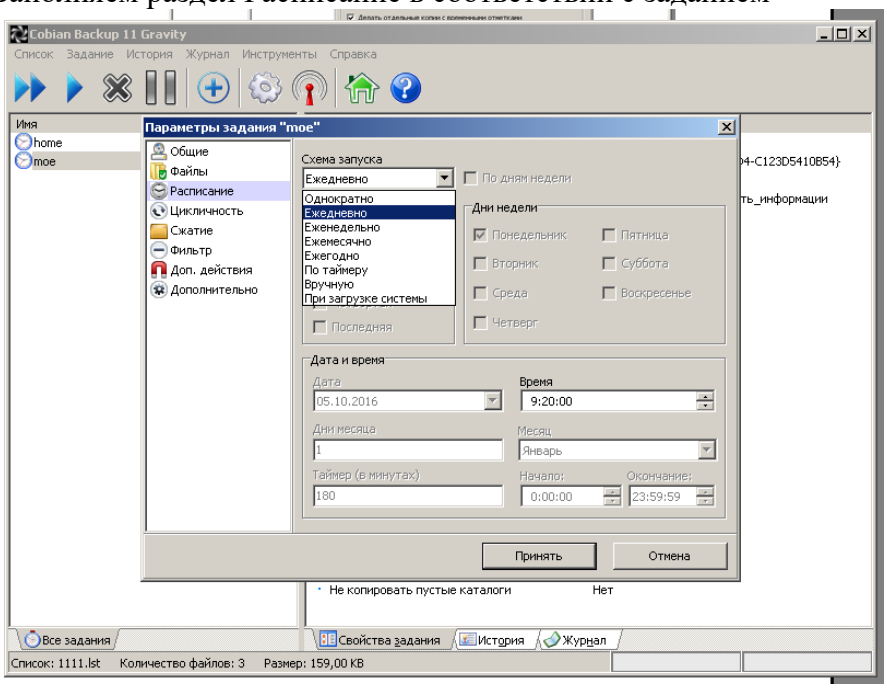
Заполнение раздела Общие



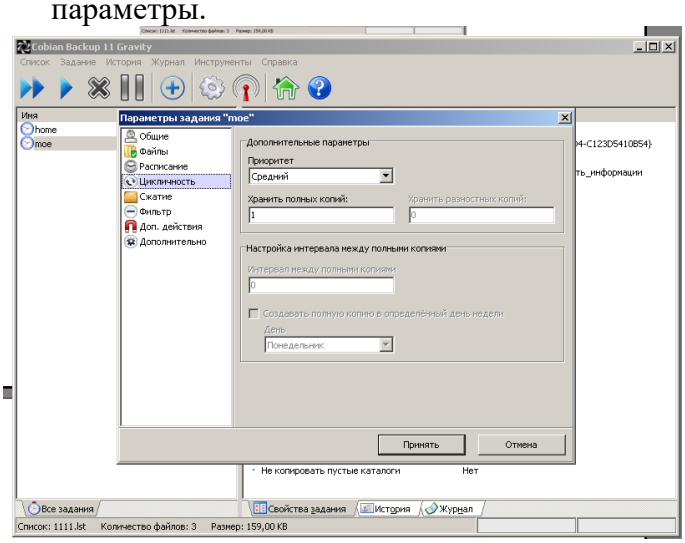
Заполнение раздела Файлы. С помощью кнопки Добавить, добавляем новые записи в список

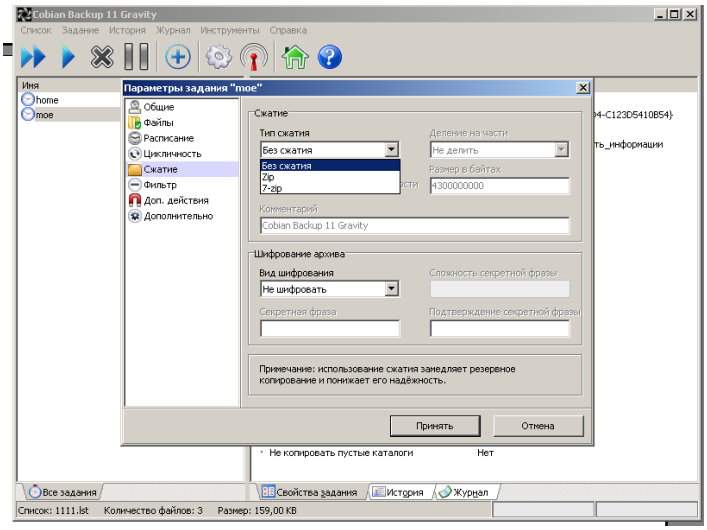


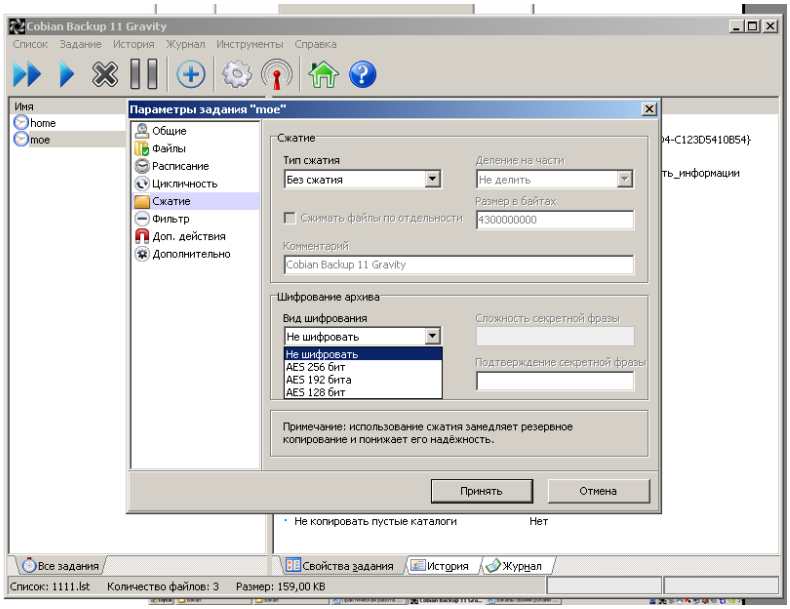
Заполняем раздел Расписание в соответствии с заданием



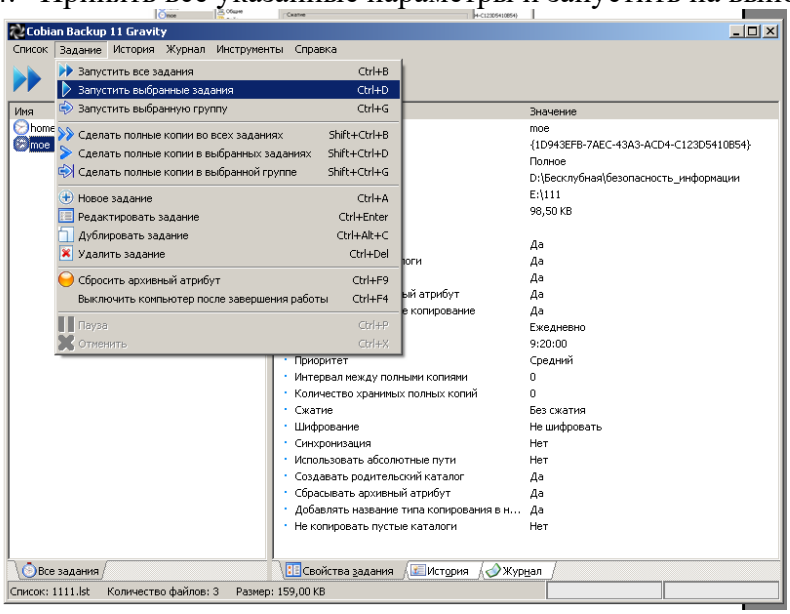
3. Разделы Цикличность и Сжатие выполнить самостоятельно, выбрав нужные параметры.







4. Принять все указанные параметры и запустить на выполнение



5. Проверить наличие папки на внешнем носителе.

Форма отчета: отчетная работа

Практическое занятие№22

Тема: Восстановление носителей информации. Восстановление удаленных файлов

Цель: Получение теоретических и практических навыков программного восстановления данных.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1.

- Добавьте в виртуальную машину виртуальный жесткий диск.
- Запустите виртуальную машину с Linux.
- Запустите fdisk (gdisk или parted) и создайте таблицу разделов MBR с разделами.
- Отформатируйте созданные разделы в файловую систему ext4.
- Установите TestDisk.
- Удалите MBR (или таблицу разделов) с помощью команды DD.
- Восстановите MBR (или таблицу разделов) с помощью TestDisk.
- Смонтируйте восстановленные разделы и создайте там произвольные файлы.
- Удалите созданные файлы.

- С помощью TestDisk восстановите данные.
- Создайте произвольный каталог и запишите туда данные каталога /var/log/ .
- Удалите данные с созданного каталога.
- С помощью PhotoRec восстановите данные.
- Создайте произвольный каталог и запишите туда данные каталога /etc/ .
- С помощью Extundelete или Foremost восстановите данные.

Контрольные вопросы:

1. С помощью какой из программ, используемых в этой лабораторной работе, можно восстановить таблицу разделов?
2. Какие файловые системы поддерживает PhotoRec?
3. Какие форматы поддерживает PhotoRec?
4. Как Foremost восстанавливает файлы?
5. Можно ли восстановить данные с файловой системы NTFS, используя extundelete?
6. Все ли данные скопированные с каталога /var/log/ восстановились?
7. Все ли данные скопированные с каталога /etc/ восстановились?

Форма отчета: отчетная работа

Практическое занятие№23

Тема: Мониторинг активности портов

Цель: формирование умений реализации доступа к базе данных MySQL; формирование знаний о программных интерфейсах доступа к данным.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Подключение в СУБД можно организовать различными способами.

Первый способ. Подключение через ODBC. Для работы с СУБД MySQL 5 через ODBC необходимо скачать и установить MySQL Connectors (**http://dev.mysql.com/downloads/connector/**). После установки, необходимо настроить драйвер ODBC. Рассмотрим по шагам. Нажать «Пуск \ Панель управления \ Администрирование \ Источники данных (ODBC)».

Далее нужно нажать «Добавить»:

Выберите «MySQL ODBC 5.1 Driver»:

В открывшемся окне нужно прописать настройки БД. Data Source name – имя подключения к БД. Можно использовать любую последовательность из латинских символов без пробела. В нашем примере это mysql_bd. Description – описание, носит информативный характер. Server – localhost, порт – 3306. User и Password – пользователь БД, с помощью которого осуществится подключение.

По умолчанию, в примере используется пользователь root, для которого не установлен пароль. Можно создать отдельного пользователя. После ввода имени пользователя и пароля, можно выбрать БД. В выпадающем списке будет указаны все доступные БД. Естественно, и пользователя, и БД нужно было создать заранее.

Второй способ. Подключение через php. Создадим 3 файла.

mysq_pass.php

```
//Файл будет хранить имя пользователя, пароль и имя базы данных.
//Каждое значение нужно написать с новой строки без лишних
//пробелов. Файл должен содержать только 4 строчки
     ?php  die;  ?>
     login
     password
     data_base_name
```

connect_mysql.php

```
//Файл, который устанавливает соединение с БД. Скрипт открывает
```

```
//файл mysql_pass.php, получает имя, пароль и имя БД и
//устанавливает соединение
     <?php
     $access=array();
     $access=file("mysql_pass.php");
     $login_db=trim($access[1]);
     $passw_db=trim($access[2]);
     $db_db=trim($access[3]);
     $db = mysql_connect("localhost", "$login_db", "$passw_db");
     mysql_query("SET CHARACTER SET cp1251");
     mysql_query("SET NAMES cp1251");
     mysql_query("SET              character_set_client='cp1251'");
     mysql_query("SET             character_set_results='cp1251'");
     mysql_query("SET   collation_connection='cp1251_general_ci'");
     mysql_select_db("$db_db", $db);
     if (!$db)
     {
     echo "<p>К сожалению, не доступен сервер mySQL</p>";
     exit();
     }
     if (!mysql_select_db($db_db,$db) )
     {
     echo "<p>К сожалению, не доступна база данных</p>";exit();
     }
     $ver = mysql_query("SELECT VERSION()");
     if(!$ver)
     {
     echo "<p>Ошибка в запросе</p>";
     exit();
     }
?>
```

index.php

```
     //В любом файле, где нужен доступ к БД нужно подключить файл
     //connect_mysql.php, после чего можно исполнять запросы
     <?php
     Error_Reporting(E_ALL & ~E_NOTICE & ~E_WARNING);
     include("connect_mysql.php");
     ?>
```

Все файлы должны находиться в одной директории. В начале и в конце файла не должно быть пустых строк.

Пример

По сценарию работа программы начинается с появления окна авторизации, в котором пользователь вводит свои данные. В таблице ниже перечислены визуальные объекты, их назначение и первоначальная настройка.

Таблица 13

Объект	Тип/Панель	Назначение	Настройка
Login.php	-	*Окно авторизации*	*Система учета оплаты КЦ*
$login0	-	Переменная логина	Получаем из базы данных

$pass0 <input name="login0">	Поле ввода	Переменная пароля Строка для ввода логина	Получаем из базы Данных Размер 25 символов, размер шрифта 12 (size="25" style="font-size: 12px;)
<input name="*pass0*">	TYPE="password"	Строка для ввода пароля	style="font-size:12px;" size="25">
<td><p align="center">Пароль:</td>	-	Поясняющая надпись	Расположить рядом с строкой ввода пароля
<td><p align="center">Логин:</td>	-	Поясняющая надпись	Расположить рядом с строкой ввода логина
Пожалуйста, авторизируйтесь в системе	-	Поясняющая надпись	Расположить сверху таблицы
<img src="key.jpg"	Image	Элемент дизайна	Расположить в левой части формы.
<INPUT VALUE="Войти">	TYPE="submit"	Кнопка войти для перехода на Главную страницу	Расположить под таблицей

В результате должно получится с визуальными компонентами

Кроме визуальных объектов потребуются специальные компоненты для доступа к базам данных, настройка которых зависит от механизма. Далее в таблице приводятся этапы реализации функционала созданного окна.

Следующим этапом служит создание таблицы users, где хранятся пароли и логины пользователей (два вида – пользователя-консультанта и администратора)

Для защиты пароля используется механизм md5, с помощью которого пароли хранятся в базе данных в зашифрованном виде.

Для преобразования символов пароля в шифр необходимо его пропустить через файл кода:

```
<?php
echo md5("ПАРОЛЬ, КОТОРЫЙ НАДО ШИФРОВАТЬ");
?>
```

Например, пароль «ПАРОЛЬ, КОТОРЫЙ НАДО ШИФРОВАТЬ» в зашифрованным виде выглядит так - 1e954982f6ce8d149ede1483f9858767.

Задания

- Изучить правила доступа к базе данных средствами php.
- Связать пользовательский интерфейс с СУБД MySQL.

Форма отчета: отчетная работа

Практическое занятие№24

Тема: Блокирование портов

Цель: формирование умений и навыков блокировки и разблокировки портов подключения устройств

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание

1 Организовать запрет доступа к USB сменным носителям при помощи групповых политик (GPO).

 нажмите "Пуск", команда Выполнить (или сочетание клавиш WIN+R) и введите команду gpedit.msc

 Открываем ветку "Конфигурация компьютера > Административные шаблоны > Система > Доступ к съемным запоминающим устройствам" и в правой части видим политики, применяемые к сменным носителям. В данном разделе GPO можно запретить доступ не только к USB носителям, но и к FDD, CDROM и др.

Задаем необходимые политики и перезагружаем ПК.

2 Организуйте блокировку портов любым из предложенных способов Самый простой способ - использование сторонней программы-фаерволла, ограничивающей доступ к соединениям сообразно политике безопасности. Таких программ, как платных, так и бесплатных, достаточно много на просторах интернета. Можно использовать встроенный в Windows инструмент фильтрации сетевых пакетов. Перейдите в свойства вашего подключения, выберите пункт "Протокол Интернета TCP/IP", нажмите "Свойства", затем нажмите кнопку "Дополнительно", выберите вкладку "Параметры", далее – пункт "Фильтрация TCP/IP" и "Свойства". Поставьте галочку напротив пункта "Включить фильтрацию" и укажите, какие именно пакеты подвергать фильтрации.

Наберите в командной строке команду "netstat -a -n" (без кавычек) и вы получите информацию о всех программах и службах, открывающих порты. Теперь вы можете по желанию прекратить выполнение этих программ и служб или оставить их в покое.

Форма отчета: отчетная работа

Практическое занятие№25

Тема: Проверка наличия и сроков действия сертификатов

Цель: знакомство с использованием сертификатов в автономном компьютере, работа с централизованной инфраструктурой открытого ключа (Pubic Key Infrastucture – PKI). Получение навыка в управлении сертификатами.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание 1 – знакомство со структурой сертификата, самоподписанные сертификаты.

С помощью консоли работы с личными сертификатами пользователя можно познакомиться с возможностями манипулирования уже полученными сертификатами.

На компьютере ClientStand зарегистрируйтесь от имени локального пользователя LStudent.

На этом компьютере нет пользователя LStudent, поэтому мы зарегистрировались от имени пользователя User1.

1. Откройте консоль управления (mmc.exe), добавьте в нее оснастку работы с сертификатами для текущего пользователя.

2. Проверьте наличие или отсутствие сертификатов в разделе персональных сертификатов.

Мы убедились, что личных (персональных) сертификатов у данного пользователя нет.

3. С помощью файлового менеджера на устройстве D: в каталоге «Encripted» зашифруйте файл Encr1.txt с помощью правой кнопки мыши.

На данном компьютере нет диска D, поэтому мы создали папку «Encripted» с файлом Encr1.txt на диске С и будем с ним работать.

Зашифровали файл с помощью свойств данного объекта.

4. В консоли работы с сертификатами проверьте наличие сертификатов в разделе персональных сертификатов.

Так как мы использовали шифрование данных на, то в разделе личные сертификаты появился сертификат шифрования пользователя.

5. Выберите сертификат, просмотрите его свойства. Запишите важнейшие на ваш взгляд из них.

После уточнения данного пункта задания у преподавателя мы рассмотрели состав самого сертификата, а не его свойства. На наш взгляд важнейшие свойства это: статус доверия (это поле отображает статус доверия цепочки сертификатов сертификат может являться надежным, подразумевать доверие и является не надежным),срок сертификата (срок окончания действия сертификата),тип сертификата (отображает формат сертификата), отпечаток(отображает цифровую подпись) .

6. Обратите внимание на то, кто и кому выдал сертификат.

Наш созданный сертификат выдан нами и нам же, то есть используется только данным пользователем для своих нужд и больше никто не сможет им пользоваться.

Задание 2 – управление центром выдачи сертификатов (Certificate Authority – CA), автономный и корпоративный CA

Задача упражнения познакомиться с возможностями получения сертификатов через Web от автономного центра сертификации, а также с методами работы с корпоративным центром выдачи сертификатов.

На компьютере SRV1 зарегистрируйтесь от имени локального пользователя LUser.

На этом компьютере нет пользователя LUser, поэтому мы вошли под учетной записью «Администратор» и будем работать под ним.

Установите центр сертификации на этом компьютере Внимание! При установке указывать имя текущего компьютера – SRV1.

При выполнении данного пункта задания возникла проблема в установке центра сертификации. Для того чтобы ее устранить необходимо через «Панель управления» -> «Установка и удаление программ» установить программу, такую как служба сертификатов. После устранения неисправности, мы подключили центр сертификатов.

Откройте консоль управления (mmc.exe), добавьте в нее оснастку работы с центром сертификации (или выберите соответствующий пункт из меню административных средств).

Откройте панель работы с центром сертификации, посмотрите, были ли уже выданы какие-то сертификаты.

Ранее нами был выдан сертификат ipsecsert через Web, и именно его он показывает в личных сертификатах.

Откройте Обозреватель Интернета. Обратитесь по адресу: http://SRV1/certsrv. Откроется стартовая страница центра выдачи сертификатов.

Стартовая страница находиться по адресу: http://localhost/certsrv/ , где имеется возможность создать новый сертификат через Web.

Через ссылку «запрос сертификата», а затем «расширенный запрос на сертификат» запросите сертификат аутентификации клиента.

В панели работы с центром сертификации MMC в пункте «запросы в ожидании» выдайте запрашиваемый сертификат.

Вернитесь в обозреватель Интернета и, вернувшись к стартовому меню, установите выданный сертификат.

В панели работы с сертификатами клиента убедитесь, что сертификат получен

Мы убедились в том, что сертификат выдан, и присутствует в разделе выданные сертификаты.

Задание 3 – запрос и получение сертификатов с CA.

В случае использования службы Active Directory можно запрашивать сертификаты через панель работы с сертификатами MMC или вообще запрашивать и получать сертификаты автоматически, без участия пользователя. При этом и «одобрения» от администратора центра выдачи сертификатов не потребуется – все проверки выполнит Active Directory.

Выключите все виртуальные машины без сохранения результатов. Запустите виртуальные машины Client и DC1.

Зарегистрируйтесь на компьютере Client1 в домене SAPR от имени пользователя Student.

Запустите MMC, добавьте оснастку работы с сертификатами пользователя.

Мы вошли в домен Sapr под именем Администратор, добавили оснастку.

Из панели управления сертификатами пользователя запросите сертификат для шифрованной файловой системы. Убедитесь, что сертификат будет выдан практически мгновенно. Проверьте на DC1 в центре управления сертификатами факт того, что этот сертификат действительно был выдан.

Мы попытались сделать запрос сертификата для шифрования файловой системы, но у нас ничего не вышло. Невозможно получить такой сертификат, так как нет возможности узнать центр сертификатов на данном компьютере. Такой тип сертификата можно получить, например, с помощью Web, если там поддерживается данный тип сертификата.

Форма отчета: отчетная работа

Практическое занятие№26

Тема: Разработка политики безопасности корпоративной сети

Цель: научиться создавать учетные записи пользователей, локальных групп, блокировать учетные записи пользователей и.т.д.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание: создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись.

Алгоритм выполнения работы:

А. **Создание учетной записи**.

1. Откройте оснастку **Настройка** – **Панель управления** – **Администрирование Управление компьютером**

2. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку Пользователи и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду **Новый пользователь** Появиться окно диалога **Новый пользователь**

4. В поле **Пользователь** введите имя создаваемого пользователя, например, свою фамилию.

Примечание: Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:*[];:=.,<>? Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле **Полное имя** введите полное имя создаваемого пользователя.

6. В поле **Описание** введите описание создаваемого пользователя или учетной записи, например, «*студент ……..*».

7. В поле **Пароль** введите пароль пользователя и в поле **Подтверждение** подтвердите его правильность вторичным вводом.

Примечание: Длина пароля не может превышать 14 символов.

8. Установите или снимите флажки:

- Потребовать смену пароля при следующем входе в систему
- Запретить смену пароля пользователем
- Срок действия пароля не ограничен
- Отключить учетную запись

9. Чтобы создать ещё одного пользователя, нажмите кнопку **Создать** и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку **Создать** и затем **Закрыть**.

В. Создание локальной группы.

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду **Новая группа**.

3. В поле **Имя группы** введите имя новой группы, например, **Студенты.**

Примечание: Имя локальной группы должно быть уникальным. Оно сможет содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле **Описание** введите описание новой группы.

5. В поле **Члены группы** можно сразу добавить пользователей и группы, которые войдут в новую группу: для этого нужно нажать кнопку **Добавить** и выбрать их в списке. Для завершения нажмите кнопку **Создать** и затем **Закрыть**.

C. **Изменение членства в локальной группе**.

1. В окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы.**

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду **Добавить** в группу или Свойства.

4. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку **Добавить**

5. Далее следуйте указателям окна диалога **Выбор: Пользователи или группы.**

6. Для того, чтобы удалить из группы некоторых пользователей, в поле **Члены группы** окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку **Удалить.**

Примечание*: В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и локальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в неё пользователей.*

D. **Временная блокировка учетной записи.**

1. Откройте оснастку **Управление компьютером.**

2. Для этого либо выберите на **Рабочем столе** ярлык **Мой компьютер** и нажмите правую кнопку мыши, после этого выберите пункт контекстного меню **Управление**, либо воспользуйтесь разделом **Администрирование в Панели управления**.

3. В открывшейся оснастке выберите пункты **Служебные программы/Локальные пользователи и группы** .

4. Откройте папку пользователи и выберите учетную запись **Гость.**

5. Нажмите правую кнопку мыши и выберите пункт свойства.

6. В открывшемся окне снимите отметку пункта **Отключить** учетную запись.

7. Нажмите кнопку **ОК** и сделайте вывод о состоянии учетной записи.

8. Выполните пункт 5 и отметьте пункт **Отключить учетную запись**.

Задание для самостоятельной работы:

1. Создайте учетную запись с именем ПЗ-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера(для чего после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.

2. Создайте группу **Информационная безопасность** и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.

3. Заблокируйте учетную запись ПЗ-6 и после этого удалитею

Контрольные вопросы:

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя П38/44? Почему?

Форма отчета: отчетная работа

Практическое занятие№27

Тема: Получение сертификата

Цель: освоить процесс анализа предметной области при проектировании программного обеспечения.

Оборудование: тетрадь, ручка, ПК

Методические указания: выполните задания

Ход выполнения:

Задание.

1 Оформить внешнюю спецификацию.

2 Составить в виде блок-схемы алгоритм решения задачи.

3 Спроектировать и разработать модули программы для решения задачи на любом алгоритмическом языке программирования.

4 Выполнить отладку и тестирование модулей программы.

5 Выполнить инкрементную интеграцию модулей с использованием одного из подходов.

6 Выполнить системное тестирование программы.

7 Оформить отчет по лабораторной работе.

Отчет по лабораторной работе должен включать:

1 Внешнюю спецификацию.

2 Алгоритм решения задачи.

3 Текст программы на языке программирования.

4 Набор тестов для отладки модулей программы.

5 Описание процесса интеграции модулей.

Задача. Задан двумерный массив размерности $n \subseteq m$. Отсортировать элементы строк массива по возрастанию значений, а затем отсортировать строки массива по возрастанию среднего арифметического элементов строк.

Реализовать сортировку разными способами и сравнить эффективность этих способов для разных исходных данных.

Форма отчета: отчетная работа

4.ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

4.1 Основные печатные и (или) электронные издания:

О-1. Перлова, О. Н. Соадминистрирование баз данных и серверов: учеб. для студ. учреждений сред. проф. образования / О.Н. Перлова, О.П. Ляпина. – 3-е изд., стер. – М.: Образовательно-издательский центр «Академия», 2023. – 304 с. – URL: https://academia-moscow.ru/catalogue/4891/616608/. – Режим доступа: Электронная библиотека «Academia-moscow». – Текст: электронный.

О-2. Федорова, Г.Н. Разработка модулей программного обеспечения для компьютерных систем: учеб. для студ. учреждений сред. проф. образования / Г.Н. Федорова. – 6-е изд., стер. – М.: Образовательно-издательский центр «Академия», 2024. – 384 с. – URL: https://academia-moscow.ru/catalogue/4891/725112/. – Режим доступа: Электронная библиотека «Academia-moscow». – Текст: электронный.

О-3. Федорова, Г.Н. Разработка, администрирование и защита баз данных: учебник / Г.Н. Федорова. – 6-е изд., перераб. – М.: Образовательно-издательский центр «Академия», 2024. – 288 с. – URL: https://academia-moscow.ru/catalogue/4891/794910/. – Режим доступа: Электронная библиотека «Academia-moscow». – Текст: электронный.

О-4. Зверева, В. П. Сопровождение и обслуживание программного обеспечения компьютерных систем: учебник / В.П. Зверева, А.В. Назаров. – 4-е изд., стер. – М.: Образовательно-издательский центр «Академия», 2024. - 256 с.

– URL: https://academia-moscow.ru/catalogue/4891/768343/. – Режим доступа: Электронная библиотека «Academia-moscow». – Текст: электронный.

4.2 Дополнительные печатные и (или) электронные издания (электронные ресурсы):

Д-1. Гохберг, Г.С., Информационные технологии: учебник для студ. учреждений сред. проф. образования / Г.С. Гохберг, А.В. Зафиевский, А.А. Короткин. – 2-е изд., стер. – М.: Издательский центр «Академия», 2018. – 240 с.

Д-2. Румянцева, Е.Л., Слюсарь В.В. Информационные технологии: учеб. пособие / Под ред. проф. Л.Г. Гагариной. – М.: ИД «Форум»: ИНФРА-М, 2009. – 256 с.

Д-3. Перлова, О.Н. Соадминистрирование баз данных и серверов: учебник для студ. учреждений сред. проф. образования / О.Н. Перлова, О.П. Ляпина. – М.: Издательский центр «Академия», 2018. – 304 с.

Д-4. Федорова, Г.Н. Разработка модулей программного обеспечения для компьютерных систем: учебник для студ. учреждений сред. проф. образования / Г.Н. Федорова. – 3-е изд., испр. – М.: Издательский центр «Академия», 2019. – 384 с.

Д-5. Федорова, Г.Н. Разработка, администрирование и защита баз данных: учебник для студ. учреждений сред. проф. образования / Г.Н. Федорова. – 3-е изд., испр. – М.: Издательский центр «Академия», 2019. – 288 с.

Д-6. Зверева, В.П. Сопровождение и обслуживание программного обеспечения компьютерных систем: учебник для студ. учреждений сред. проф. образования / Зверева, А.В. Назаров. – М.: Издательский центр «Академия», 2018 – 256 с.

Д-7. Учебник. Администрирование серверов с помощью управления на основе политик. Microsoft TechNet [Электронный ресурс]. – Режим доступа: www.url: https://technet.microsoft.com/ru-ru/library/bb522659(v=sql.120)/. – 03.02.2025.

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В МЕТОДИЧЕСКИЕ УКАЗАНИЯ

№ изменения, дата внесения, №страницы с изменением	
Было	Стало
Основание: Подпись лица, внесшего изменения	