Краевое государственное автономное
профессиональное образовательное учреждение
«Кунгурский колледж агротехнологий и управления»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ РАБОТ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
ПМ.07 СОАДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ И СЕРВЕРОВ
09.02.07 «Информационные системы и программирование»

2023 г.

Рассмотрено на заседании МК информационных дисциплин от «30» августа 2023 г.

Председатель МК
А.В.Атушкина

Утверждаю
Зам. директора
Л.И.Петрова

Организация-разработчик: ГБПОУ «ККАТУ»

Составитель: А.В.Атушкина

Пояснительная записка

Методические указания по выполнению лабораторных и практических работ по ПМ 07. Соадминистрирование баз данных и серверов разработаны в соответствии с рабочей программой профессионального модуля и предназначены для приобретения необходимых практических навыков и закрепления теоретических знаний, полученных обучающимися при изучении профессионального модуля, обобщения и систематизации знаний перед экзаменом.

Методические указания предназначены для обучающихся специальности 09.02.07 Информационные системы и программирование.

ПМ 07. Соадминистрирование баз данных и серверов относится к профессиональному циклу, изучается на 4 курсе и при его изучении отводится значительное место выполнению практических работ.

Освоение содержания ПМ 07. Соадминистрирование баз данных и серверов во время выполнения практических работ обеспечивает достижение обучающимися следующих **результатов:**

Код	**Наименование результата обучения**
ВД 7	*Соадминистрирование баз данных и серверов*
ПК 7.1	Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов
ПК 7.2	Осуществлять администрирование отдельных компонент серверов
ПК 7.3	Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

Код трудовой функции	Наименование
ТФ A/01.4	Трудовые действия – Сбор в соответствии с трудовым заданием документации заказчика касательно его запросов и потребностей применительно к типовой ИС; – Анкетирование представителей заказчика в соответствии с трудовым заданием; – Интервьюирование представителей заказчика в соответствии с трудовым заданием; – Документирование собранных данных в соответствии с регламентами организации.
	Необходимые умения – Проводить анкетирование; – Проводить интервьюирование; – Собирать исходную документацию.
	Необходимые знания – Возможности типовой ИС; – Предметная область автоматизации; – Инструменты и методы выявления требований; – Технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии; – Архитектура, устройство и функционирование вычислительных систем; – Коммуникационное оборудование; – Сетевые протоколы; – Основы современных операционных систем; – Основы современных систем управления базами данных; – Устройство и функционирование современных ИС; – Современные стандарты информационного взаимодействия систем; – Программные средства и платформы инфраструктуры информационных технологий организаций; – Системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников; – Отраслевая нормативная техническая документация; – Источники информации, необходимой для профессиональной деятельности; – Современный отечественный и зарубежный опыт в профессиональной деятельности; – Основы бухгалтерского учета и отчетности организаций; – Основы налогового законодательства Российской Федерации; – Культура речи; – Правила деловой переписки.

ТФ А/09.4	Трудовые действия – Установка операционных систем в соответствии с трудовым заданием; – Настройка операционных системы для оптимального функционирования ИС в соответствии с трудовым заданием; – Установка СУБД в соответствии с трудовым заданием; – Настройка СУБД для оптимального функционирования ИС в соответствии с трудовым заданием; – Установка прикладного ПО, необходимого для функционирования ИС в соответствии с трудовым заданием; – Настройка прикладного ПО, необходимого для оптимального функционирования ИС, в соответствии с трудовым заданием.
	Необходимые умения – Устанавливать операционные системы; – Устанавливать СУБД; – Устанавливать прикладное ПО.
	Необходимые знания – Основы системного администрирования; – Основы администрирования баз данных; – Коммуникационное оборудование; – Сетевые протоколы; – Архитектура, устройство и функционирование вычислительных систем; – Основы современных операционных систем; – Основы современных систем управления базами данных; – Устройство и функционирование современных ИС; – Источники информации, необходимой для профессиональной деятельности; – Современный отечественный и зарубежный опыт в профессиональной деятельности.

Рабочая программа профессионального модуля предусматривает проведение практических работ в объеме 84 часа.

Порядок выполнения практической работы

- записать название работы, ее цель в тетрадь;
- выполнить основные задания в соответствии с ходом работы;
- выполнить индивидуальные задания.

Рекомендации по оформлению практической работы

Задания выполняются обучающимися по шагам. Необходимо строго придерживаться порядка действий, описанного в практической работе.

Результаты выполнения практических работ необходимо сохранять в своей папкена компьютере или USB – накопителе.

В случае пропуска занятий обучающийся осваивает материал самостоятельно в свободное от занятий время и сдает практическую работу с пояснениями о выполнении.

Требования к технике безопасности при выполнении лабораторных/практических работ

Вводный инструктаж

Инструкция №1 ПРАВИЛА ПОВЕДЕНИЯ СТУДЕНТОВ В КАБИНЕТЕ ИНФОРМАТИКИ

Кабинет информатики относится к кабинетам повышенной опасности, находясь в нем необходимо соблюдать требования настоящей инструкции.

1. Не заходите в кабинет без разрешения преподавателя.

2. Во время перемены все студенты выходят в коридор. В кабинете кроме преподавателя могут находиться только дежурные.

3. Запрещается находиться в кабинете в верхней одежде, грязной обуви.

4. Не бегайте по кабинет - можете получить травму или повредить оборудование.

5. Не бросайте мусор в кабинете, этим вы создаете пожарную опасность.

6. Будьте внимательны и дисциплинированны, точно выполняйте указания преподавателя.

7. Не приступайте к выполнению работы без разрешения преподавателя.

8. Не пользуйтесь электрическими розетками для шалости, это опасно для вашей жизни.

Инструктаж №2 ПРАВИЛА РАБОТЫ СТУДЕНТОВ ЗА КОМПЬЮТЕРОМ ПЕРЕД ВЫПОЛНЕНИЕМ РАБОТЫ необходимо выслушать преподавателя о ее содержании и ходе выполнения.

ВО ВРЕМЯ РАБОТЫ

1. Компьютер можно включать только после разрешения преподавателя.

2. ЗАПРЕЩАЕТСЯ:

-прикасаться к проводам, лишенных изоляции;

-включать компьютер со снятым корпусом;

-производить подключение устройств к включенному компьютеру;

-прикасаться руками и острыми предметами к экрану монитора, внутренним частям компьютера;

-есть за компьютером;

-включать компьютер сразу же после его выключения (необходимо подождать 10-15 секунд).

3. Обнаружив неисправность в электрических устройствах, находящихся под напряжением, необходимо немедленно отключить источник электропитания и сообщить об этом преподавателю.

4. Не оставляйте рабочего места без разрешения преподавателя.

ПОСЛЕ ОКОНЧАНИЯ РАБОТЫ

1. Корректно завершите работу компьютера.

2. Сдай рабочее место преподавателю.

Инструктаж №3 ПРАВИЛА ПОЖАРНОЙ БЕЗОПАСНОСТИ

1. В кабинете должны, быть средства для тушения пожара: огнетушитель.

2. Кабинет должен содержаться в чистоте. Весь сгораемый мусор следует систематически выносить.

3. В кабинете не допускается хранение легковоспламеняющихся жидкостей.

4. ЗАПРЕЩАЕТСЯ:

-допускать к работе студентов, не ознакомленных с правилами техники безопасности;

-оставлять без присмотра включенное в электрическую сеть оборудование;

-подвешивать электропроводку на гвоздях, использовать электропровода с поврежденной изоляцией, некалиброванные предохранители, обертывать электрические лампы бумагой или тканью, подвешивать стенды, таблицы и пр. на электропровода;

-работа в кабинете с нагревательными приборами;

-производить сложный ремонт компьютерной техники.

5. По окончании работы необходимо тщательно осмотреть помещение, устранить все недочеты, отключить напряжение электросети с помощью рубильника.

6. В случае возникновения пожара необходимо:

-отключить напряжение электрической сети;

-немедленно эвакуировать студентов;

-принять меры по тушению пожара;

-сообщить о пожаре по телефону 01 или 112.

Критерии оценки выполнения практических работ

Оценки	Критерии оценок
«5»	- обучающийся подбирает необходимые для выполнения предлагаемых работ источники знаний (литература, материалы, инструменты), показывает необходимые для проведения практической работы теоретические знания. Правильно оформлена практическая работа, соблюдена технологическая последовательность выполнения данного вида работ. Работа оформлена аккуратно.
«4»	- практическая работа выполняется обучающимся в полном объёме и самостоятельно. Обучающийся использует указанные преподавателем источники информации. Могут быть неточности и небрежность в оформлении работы. Работа показывает знания обучающимися основного теоретического материала, но имеются незначительные ошибки при оформлении практической части роботы.
«3»	- обучающийся выполняет и оформляет практическую работу полностью с помощью преподавателя или хорошо подготовленных и уже выполнивших на «отлично» данную работу других обучающихся.
«2»	- практическая работа не выполнена полностью за отведенное время по неуважительной причине.

Перечень практических работ

№ п/п	Наименование раздела, темы, занятия	Кол-во часов
МДК. 07.01 Управление и автоматизация баз данных		**64**
Тема 7.1.1. Принципы построения и администрирования баз данных		**8**
1.	Пр.р.№1 Построение схемы базы данных	4
2	Пр.р.№2 Составление словаря данных	4
Тема 7.1.2. Серверы баз данных		**10**

1	Пр.р.№3 Разработка технических требований к серверу баз данных	2
2	Пр.р.№4 Разработка требований к корпоративной сети	2
3	Пр.р.№5 Конфигурирование сети	2
4	Пр.р.№6 Сравнение технических характеристик серверов	2
5	Пр.р.№7 Формирование аппаратных требований и схемы банка данных	2
Тема 7.1.3. Администрирование баз данных и серверов		**34**
1	Пр.р.№8 Установка и настройка сервера	4
2	Пр.р.№9 Установка и настройка сервера под UNIX	4
3	Пр.р.№10 Выполнение запросов к базе данных	6
4	Пр.р.№11 Выполнение изменений в базе данных	4
5	Пр.р.№12 Создание триггеров	4
6	Пр.р.№13 Создание запросов и процедур на изменение структуры базы данных	4
7	Пр.р.№14 Работа с журналом аудита базы данных	4
8	Пр.р.№15 Мониторинг нагрузки сервера	4
Экзамен		6
МДК.07.02 Сертификация информационных систем		**20**
Тема 7.2.1. Защита и сохранность информации баз данных		**8**
1	Пр.р.№1 Настройка политики безопасности	2
2	Пр.р.№2 Создание резервных копий базы данных. Восстановление базы данных	2
4	Пр.р.№4 Восстановление носителей информации. Восстановление удаленных файлов	2
6	Пр.р.№6 Мониторинг активности портов. Блокирование портов	2
Тема 7.2.2 Сертификация информационных систем		**6**
1	Пр.р.№8 Проверка наличия и сроков действия сертификатов	2
2	Пр.р.№9 Разработка политики безопасности корпоративной сети	2
3	Пр.р.№10 Получение сертификата	2
Экзамен		6
Итого		**84**

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные печатные издания

1. Фуфаев Э.В. Разработка и эксплуатация удаленных баз данных: учебник для студ. учреждений сред.проф. образования. – М.: Издательский центр «Академия», 2018. – 304 с.

Основные электронные издания

1. Администрирование серверов с помощью управления на основе политик. Microsoft TechNet: Учебник [Электронный ресурс]. URL: https://technet.microsoft.com/ru-ru/library/bb522659(v=sql.120). Доступ свободный. Дата обращения 20.08.2023.

Практическая работа №1

Настройка политики безопасности

Цель работы: освоение средств администратора, предназначенных для:

- *регистрации пользователей и групп в системе, определения их привилегий;*
- *определения параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе;*
- *определения параметров политики безопасности;*
- *определения параметров политики аудита;*
- *просмотра и очистки журнала аудита;*
- *разграничения доступа субъектов к папкам и файлам;*
- *обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы;*
- *определения параметров политики ограниченного использования программ.*

Общие положения

Управление зарегистрированными пользователями

Для управления зарегистрированными пользователями необходимо войти в операционную систему с правами администратора. Открыть список зарегистрированных пользователей можно через меню Пуск | Панель управления | Администрирование | Управление компьютером |

Локальные пользователи и группы.

Для создания нового пользователя необходимо выбрать пункт Пользователи и с помощью команды контекстного меню «Новый пользователь» создать учетную запись. Для добавления пользователя в группу необходимо выделить нужного пользователя и выполнить команду контекстного меню «Свойства», далее на открывшемся окне «Свойства пользователя» выбрать вкладку «Членство в группах» и с помощью кнопок «Добавить», «Дополнительно» и

«Поиск» включить вновь созданного пользователя в нужную группу.

Для создания новой группы пользователей необходимо открыть список групп Пуск | Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Группы и создать новую группу с помощью команды контекстного меню «Создать группу».

Для назначения прав пользователям необходимо открыть окно настройки прав пользователей Пуск | Панель управления | Администрирование | Локальная политика безопасности

| Локальные политики | Назначение прав пользователя.

Для обеспечения дополнительной защиты базы учетных записей с помощью шифрования нужно начать работу с программой syskey с помощью команды «Выполнить» меню «Пуск». Для настройки вариаций генерации системного ключа нужно нажать кнопку «Обновить».

Настройка элементов политики безопасности

Для управления настройкой политики безопасности необходимо войти в систему с правами администратора и открыть окно определения параметров политики безопасности Пуск | Панель управления | Администрирование | Локальная политика безопасности.

Для обеспечения использования пользователями доверенного канала при вводе паролей необходимо установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL» с помощью меню Пуск | Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности.

Настройка политики использования паролей осуществляется с помощью меню Пуск | Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности | Политики учетных записей | Политика паролей:

– *Параметр безопасности «Максимальный срок действия пароля» определяет период времени (в днях), в течение которого можно использовать пароль, пока система не потребует от пользователя сменить его. Срок действия пароля может составлять от 1 до 999 дней; значение 0 соответствует неограниченному сроку действия пароля.*

– *Параметр безопасности «Минимальная длина пароля» определяет минимальное количество знаков, которое должно содержаться в пароле пользователя. Можно установить значение от 1 до 14 знаков, либо 0 знаков, если пароль не требуется.*

– *Параметр безопасности «Минимальный срок действия пароля» определяет период времени (в днях), в течение которого пользователь должен использовать пароль, прежде чем его можно будет изменить. Можно установить значение от 1 до 998 дней либо разрешить изменять пароль сразу, установив значение 0 дней.*

– *Параметр безопасности «Пароль должен отвечать требованиям сложности» определяет, должен ли пароль отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:*

- *Не содержать имени учетной записи пользователя или частей полного имени пользователядлиной более двух рядом стоящих знаков;*
- *Иметь длину не менее 6 знаков;*
- *Содержать знаки трех из четырех перечисленных ниже категорий:*

1. *Латинские заглавные буквы (от A до Z);*
2. *Латинские строчные буквы (от a до z);*
3. *Цифры (от 0 до 9);*
4. *Отличающиеся от букв и цифр знаки (например, !, $, #, %).*

Освоение средств определения политики аудита

Для определения политики аудита необходимо открыть окно определения параметров политики аудита (Пуск | Панель управления | Администрирование | Локальная политика

безопасности | Локальные политики | Политика аудита) и с помощью параметров политики аудита установить регистрацию в журнале аудита успешных и неудачных попыток

−входа в систему;
−доступа к объектам;
−доступа к службе каталогов;
−изменения политики;
−использования привилегий;
−отслеживания процессов;
−системных событий;
−событий входа в систему;
−управления учетными записями.

Для просмотра и очистки журнала безопасности необходимо открыть окно просмотра журнала аудита событий безопасности (Пуск | Панель управления | Администрирование | Просмотр событий | Журналы Windows | Безопасность), выполнить команду «Свойства» контекстного меню (или команду Действие | Свойства). Для ознакомления со средствами эффективного анализа журнала аудита событий безопасности нужно открыть журнал аудита событий безопасности и с помощью команды «Фильтр» отобрать записи к просмотру всего журнала.

Освоение средств определения политики ограниченного использования программ

Для определения политики ограниченного использования программ необходимо:

−открыть окно определения уровней безопасности политики ограниченного использования программ (Пуск | Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Уровни безопасности);
−открыть окно определения дополнительных правил политики ограниченного использования программ (Пуск | Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Дополнительные правила).

Освоение средств разграничения доступа пользователей к файлам и папкам

Для разграничения доступа к файлам и папкам необходимо выполнить команду «Свойства» контекстного меню Вашей папки или файла и выбрать вкладку «Безопасность» (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке

«Вид» окна свойств папки). Для просмотра полного набора прав доступа к папке и файлу для каждого из имеющихся в списке субъектов необходимо с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки.
Разграничить доступ к файлу (папке) можно с помощью кнопки «Добавить» и с помощью кнопок «Дополнительно» и «Поиск» открыть список зарегистрированных пользователей и групп и выбрать нужного пользователя.

Для разграничения доступа к объектам в операционной системе предусмотрено наличие системной программы по управлению списками контроля доступа (CACLS). Для работы с системной программой необходимо начать сеанс работы в режиме командной строки (Пуск | Программы | Стандартные | Командная строка). Далее в строке приглашения ввести название программы, ознакомиться с ее назначением и параметрами.

Освоение средств обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы

Для выполнения операции шифрования файлов и папок нужно выполнить команду

«Свойства» контекстного меню Вашей папки или файла, и на вкладке «Общие» окна свойств нажать кнопку «Другие». Далее включить выключатель «Шифровать содержимое для

защиты данных», нажать кнопку «Применить» и в окне подтверждения изменения атрибутов нажать кнопку «Ok».

При шифровании данных на компьютере необходимо предусмотреть способ восстановления этих данных на случай, если что-то произойдет с ключом шифрования. Если ключ шифрования потерян или поврежден и способ восстановления данных отсутствует, данные будут потеряны. Данные будут также потеряны, если повреждена или утеряна смарт-карта, на которой хранился ключ шифрования. Чтобы гарантировать постоянный доступ к зашифрованным данным, нужно сделать резервные копии сертификата и ключа шифрования. Если компьютером пользуются несколько человек или если для шифрования файлов используется смарт-карта, нужно создать сертификат восстановления файла. Для создания резервной копии EFS-сертификата необходимо:

1. *Открыть диспетчер сертификатов (Нажмите кнопку «Пуск», в поле «Поиск» введите certmgr.msc и нажмите клавишу «ВВОД»). В левой области дважды щелкните папку (Личная | Сертификаты).*
2. *В основной области щелкните сертификат, содержащий пункт «Шифрованная файловая система» в группе «Назначения». Если имеется несколько EFS-сертификатов, нужно сделать резервное копирование для всех.*
3. *В меню «Действие» выберите пункт «Все задачи» и щелкните «Экспорт». В окне мастера экспорта сертификатов нажмите кнопку «Далее», выберите параметр «Да, экспортировать закрытый ключ» и нажмите кнопку «Далее».*
4. *Щелкните «Файл обмена личной информацией» и нажмите кнопку «Далее». Введите пароль, который следует использовать, подтвердите его, а затем нажмите кнопку «Далее». Процесс экспорта создаст файл для хранения сертификата.*
5. *Введите имя файла и его расположение (полный путь) или нажмите кнопку «Обзор», перейдите к нужному месту, введите имя файла и нажмите кнопку «Сохранить». Последовательно нажмите кнопки «Далее» и «Готово». Храните резервную копию EFS-сертификата в надежном месте.*

Права пользователей

Политика безопасности системы является одной из важнейших составляющих в обеспечении надежной и защищенной работы Windows XP. Настройка политики безопасности осуществляется в программе Local Security Settings: Пуск\Панель управления\ Администрирование\ Локальная политика безопасности\Назначение прав пользователя

После запуска программы Назначение прав пользователя появится окно Локальные параметры безопасности (рис.1.1.)

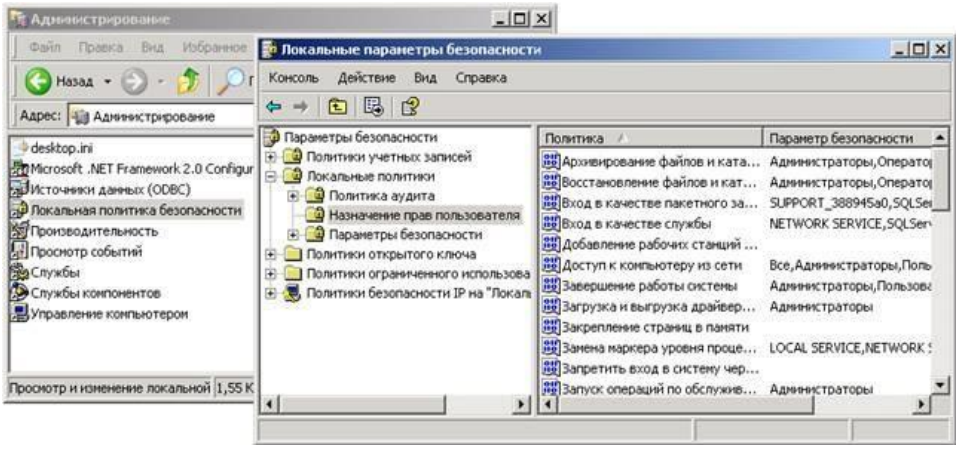


Рисунок 1.1 - Окно Локальные параметры безопасности

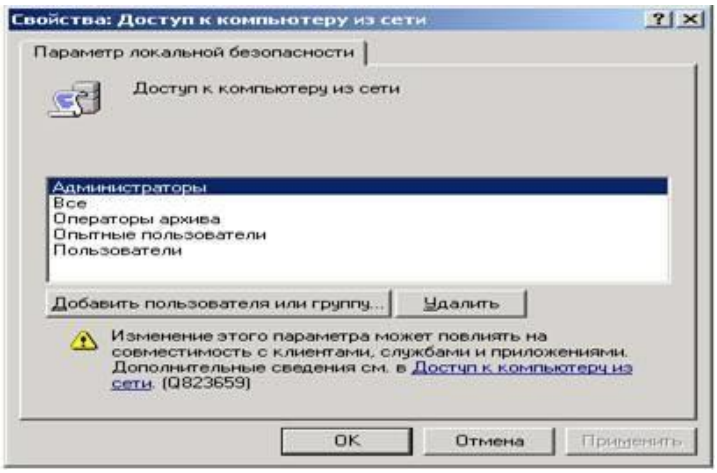


Рисунок 1.2 - Окно Параметр локальной безопасности

Основные пункты политики безопасности

1. *Пункт Доступ к компьютеру из сети – определяет, какие именно пользователи и группы пользователей могут получать доступ к данному компьютеру по компьютерной сети. Если компьютер не подключен к локальной сети, рекомендуется запретить доступ пользователей извне, это позволит избежать атак взломщиков и их проникновение в систему при работе в Интернете. Для запрета доступа сетевых пользователей к компьютеру следует:*

- *в окне Политика программы Назначение прав пользователя щелчком мыши выбрать политику Доступ к компьютеру из сети;*
- *появится окно Параметр локальной безопасности Доступ к компьютеру из сети (рис.1.2.);*
- *выделить всех пользователей (или лишних пользователей) при помощи указателя мыши иклавиши Shift;*
- *сделать щелчок по кнопке Удалить;*
- *нажать кнопку ОК.*

Пользователи, которым разрешен доступ к компьютеру, должны быть отображены в данном пункте политики безопасности, иначе они не смогут войти в систему. Если пользователи в списке окна отсутствуют, то их следует добавить при помощи кнопки Добавить пользователя или группу. Для этого следует:

- *сделать щелчок по кнопке Добавить пользователя или группу;*
- *в появившемся диалоговом окне сделать щелчок по кнопке Дополнительно;*
- *в окне Пользователи или группы нажать кнопку Поиск;*
- *в нижней части окна появится список всех пользователей и групп;*
- *щелчком выбрать нужную строку нажать кнопку ОК;*
- *в появившемся диалоговом окне в поле Введите имена выбираемых объектов появится выбранный пользователь (группа), нажать кнопку ОК;*
- *выбранный пользователь (группа) будет отображен в окне Доступ к компьютеру из сети.*

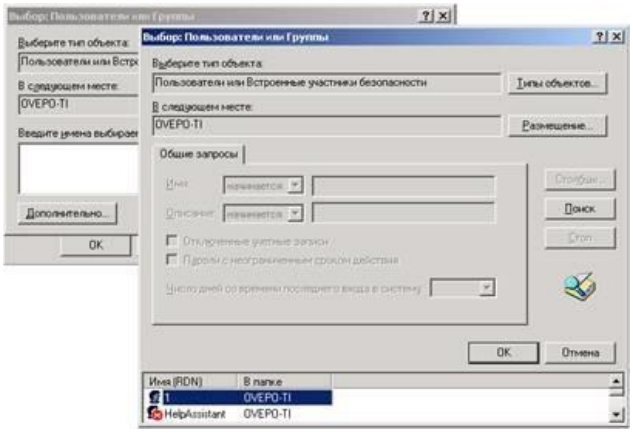


Рисунок 1.3 - Добавление пользователей или групп

2. *Пункт Разрешать вход в систему через службу терминалов является аналогичным предыдущему, но вход пользователей в систему осуществляется в качестве клиентов терминал-сервера. Если данный сервис не используется, то рекомендуется аналогичным методом запретить вход в систему всех пользователей, убрав их из значения данного пункта как клиентов терминал- сервера. В случае необходимости всегда можно добавить нужных пользователей и их группы при помощи кнопки Добавить пользователя или группу (рис.1.4.).*

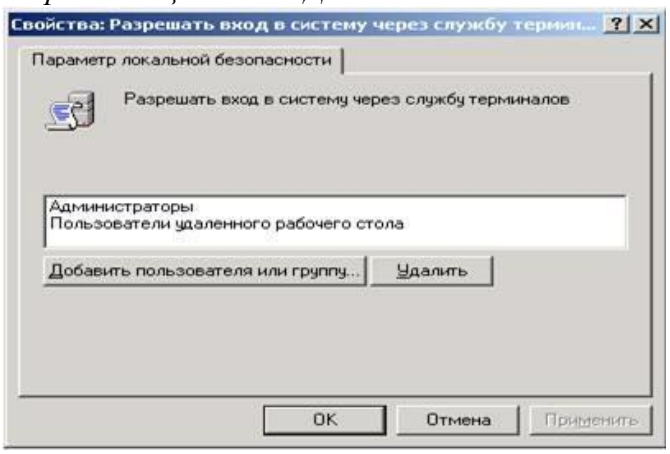


Рисунок 1.4 - Окно Разрешить вход в систему через службу терминалов

3. *Пункт Изменение системного времени, позволяющий пользователям, перечисленным в нем, менять системное время, а также просматривать календарь, появляющийся на экране при двойном щелчке по текущему времени на панели задач. По умолчанию данной возможностью обычные пользователи не смогут воспользоваться. Для разрешения пользователям выполнять такое действие следует их внести в список данного пункта политики безопасности при помощи кнопки Добавить пользователя или группу (рис.1.5.).*

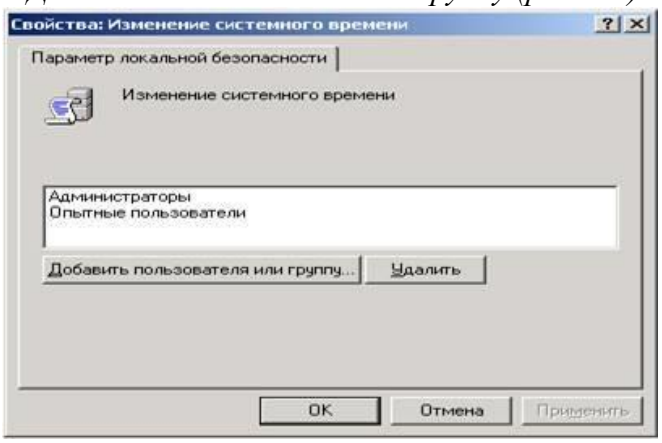


Рисунок 1.5 - Окно Изменение системного времени

4. *Пункт Отладка программ позволяет указать пользователей, которые смогут подсоединять свой отладчик к процессам и производить их отладку. Следует включать в этот пункт только тех пользователей, которым это действительно нужно, например, системный администратор и системные программисты. Не следует давать это право другим пользователям, так как этой возможностью могут воспользоваться вирусы для заражения системы, запущенные под одной из пользовательских записей, имеющей право на отладку процессов.*

5. *Пункт Отказ в доступе к компьютеру из сети содержит пользователей и их группы, которым запрещен вход в систему по компьютерной сети. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки Добавить пользователя или группу (рис.1.6.).*

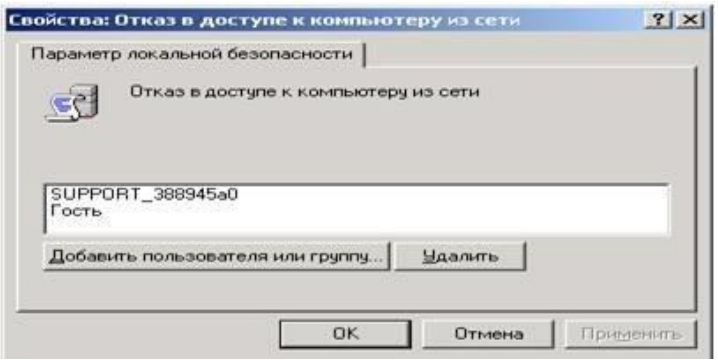


Рисунок 1.6 - Окно Отказ в доступе к компьютеру из сети

6. *Пункт Отклонить локальный вход содержит пользователей и их группы, которым запрещен локальный вход в систему. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки Добавить пользователя или группу (рис.1.7.).*

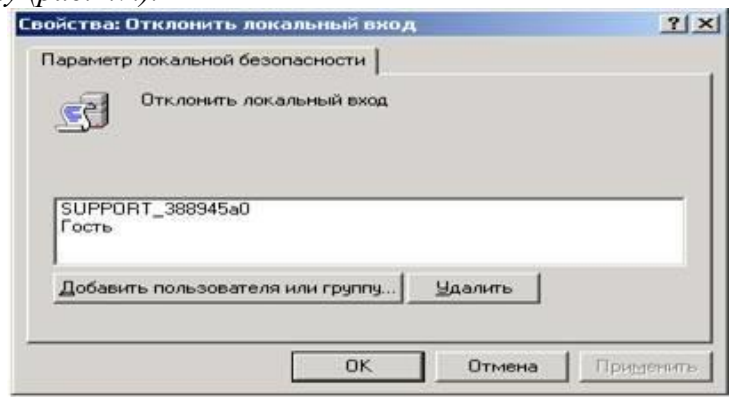


Рисунок 1.7 - Окно Отлонить локальный вход

7. *Пункт Запретить вход через службу терминалов также содержит пользователей и их группы, которым запрещен вход в систему как клиентов терминал-сервера. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки Добавить пользователя или группу (рис.1.8.).*

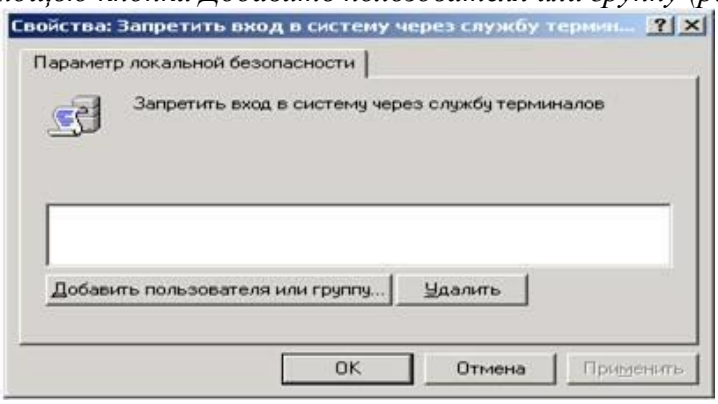
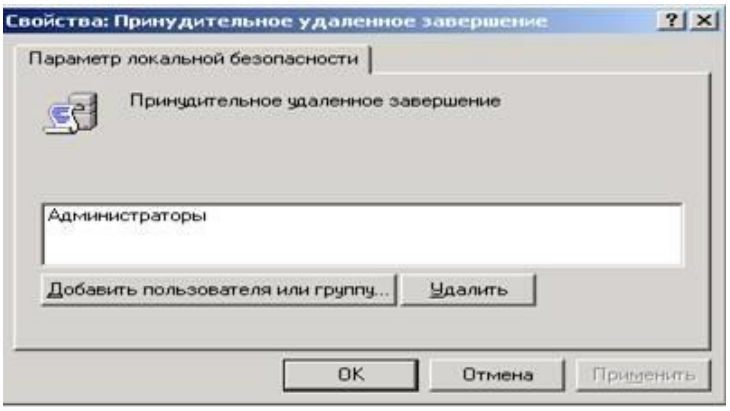


Рисунок 1.8 - Окно Запретить вход в систему через службу терминалов

С помощью трех перечисленных выше опций локальной политики безопасности можно запретить пользователям, которые по структуре организации не должны получать доступа, вход в систему. Этим можно предотвратить внутренние коллизии организации и защитить данные от их искажения или разрушения пользователями, которые удаленно пытаются ими воспользоваться.

8. *Пункт Принудительное удаленное завершение является очень важным в настройке локальной политики безопасности, так как если его не настроить соответствующим образом, то система может получить команду на выключение или перезагрузку от удаленно пользователя. Поэтому в данном пункте следует указывать только пользователей, которым действительно может потребоваться с машин, находящихся в локальной сети, выключить или перезапустить*



систему.

Рисунок 1.9 - Окно Принудительное удаленное завершение

9. *Пункт Загрузка и выгрузка драйверов устройств позволяет указать, кто из пользователейможет динамически устанавливать и выгружать драйвера устройств. Это право необходимо для установки драйверов устройств, имеющих спецификацию Plug and Play.*

10. *Пункт Локальный вход в систему является очень важным и определяет, какие пользователи и их группы могут локально входить в систему.*

11. *Пункт Управление аудитом и журналом безопасности относится к механизму аудита системы и определяет, какие пользователи и их группы могут устанавливать аудит доступа к определенным объектам, таким как файлы, ключи реестра и пр. По умолчанию в данном пункте перечислена лишь одна группа локальных системных администраторов.*

12. *Пункт Изменение параметров среды оборудования определяет пользователей, которые будут иметь право в Windows XP менять значения системных переменных. По умолчанию на это имеют право только пользователи, принадлежащие локальной группе администраторов.*

13. *Пункт Запуск операций по обслуживанию тома позволяет указать пользователей и их группы, которые будут иметь право выполнять задачи по поддержанию работы накопителей, такие как очистка диска или его дефрагментация. Выполнение данных задач, по умолчанию, доверяется только пользователям из группы системных администраторов.*

14. *Пункт Восстановление файлов и каталогов позволяет указывать пользователей и их группы, которые могут выполнять операцию восстановления файлов и директорий из сохраненных копий, а также ставить им необходимые права доступа. По умолчанию в системе такими пользователями являются члены группы системных администраторов, а также операторы сохранения данных.*

15. *Пункт Завершение работы системы указывает, кто из локальных пользователей, имеющих учетные записи в системе, имеет право на ее выключение или перезагрузку. По умолчанию на это имеют право все пользователи. Однако, в ряде случаев, может потребоваться запретить выполнять данные функции некоторым пользователям. Например, если нужно, чтобы компьютеры работали в то время, когда некоторые пользователи их пытаются отключить. В этом случае нужно убрать этих пользователей из данного пункта. Особенно это может быть полезно, если определенные пользователи пытаются выключить компьютер, на котором находится информация, используемая удаленно другими пользователями.*

16. *Пункт Овладение файлами или иными объектами отвечает за возможность пользователей, перечисленных в нем, брать на себя право становиться владельцами файлов и объектов.Этими объектами могут быть структуры Active Directory, ключи реестра, принтеры и процессы. По умолчанию на это имеют право только пользователи группы системных администраторов. Добавление к этому пункту пользователей означает предоставление им всех прав по доступу к различным объектам.*

Глобальные параметры безопасности системы

Глобальные параметры безопасности устанавливаются в разделе локальной политики безопасности Параметры безопасности (рис.1.10).

Пуск\Панель управления\Администрирование\Локальная политика безопасности\Параметры безопасности

Рассмотрим наиболее важные пункты.

1. Пункт Учетные записи: Состояние учетной записи 'Администратор' предоставляет возможность выбора: будет ли учетная запись администратора системы включена или отключена, при нормальном функционировании системы. В случае использования системы в безопасном режиме запись администратора будет включена, независимо от значения данного пункта. Для изменения значения этого пункта следует его выбрать двойным щелчком мыши и в появившемся окне поставить флажок в соответствующем режиме (рис.1.11.)

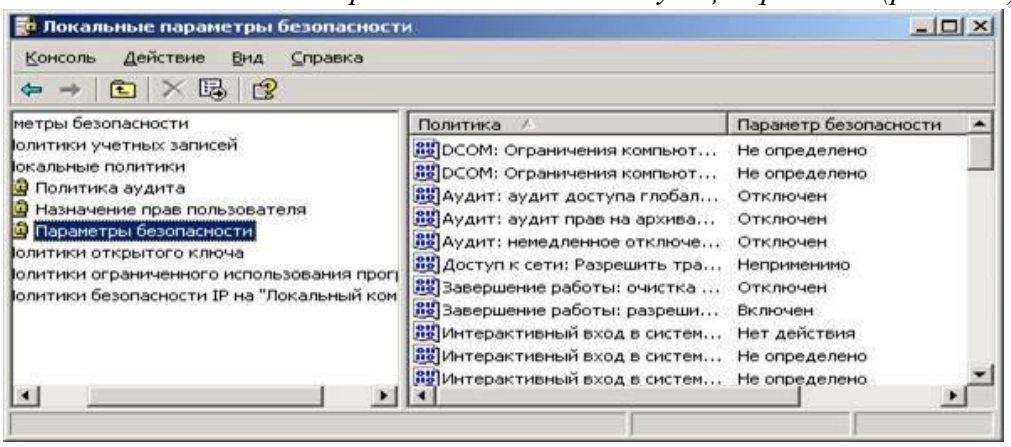


Рисунок 1.10 - Окно Параметры безопасности

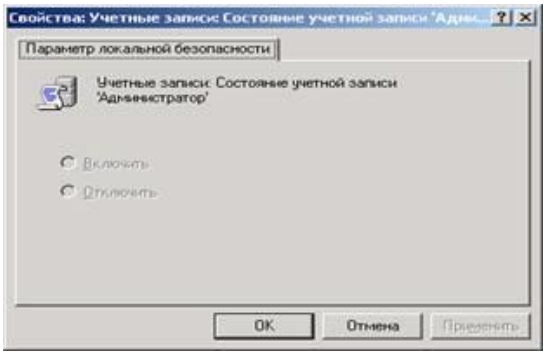


Рисунок 1.11 - Окно Состояние учетной записи 'Администратор'

Отключение учетной записи системного администратора может быть полезно, т. к. это дает гарантированную защиту от атак взломщиков на эту учетную запись. Если необходимо включить учетную запись системного администратора, то это можно сделать под учетной записью другого пользователя, принадлежащего к группе системных администраторов, или в защищенном режиме работы операционной системы.

Пункт Учетные записи: Состояние учетной записи 'Гость' позволяет отключать учетную запись гостя, т. к. для входа под данной учетной записью не требуется пароль, что может нарушить политику прав доступа пользователями. Учетная запись Гость по умолчанию отключена.

Пункт Accounts: Limit local account use of blank passwords to console logon only, в случае включения позволяет ограничить доступ к незащищенным паролями консольным учетным

записям локальных пользователей со стороны различных сетевых сервисов, например: терминал-сервера, Telnet и FTP. По умолчанию, в целях защиты системы от сетевых атак, данный пункт включен.

Пункт Accounts: Rename administrator account позволяет переименовать встроенную учетную запись администратора системы. Это делается в целях защиты от атаки методом подбора паролей. Чтобы изменить имя учетной записи администратора, нужно дважды щелкнуть мышью по имени этого пункта и в появившемся окне ввести новое имя этой учетной записи.

Пункт Audit: Audit the use of Backup and Restore privilege позволяет контролировать выполнение всех операций сохранения и восстановления данных. Система будет сохранять сообщения обо всех резервируемых и восстанавливаемых файлах и папках. Это очень удобно для проведения контроля за операциями резервирования и восстановления данных. Для работы данного пункта необходимо включение в политике аудита опции Аудит использования привилегий. По умолчанию данный пункт локальной политики безопасности отключен.

Пункт Audit: Shut down system immediately if unable to log security audits является очень полезным и позволяет после своего включения, в случае обнаружения операционной системой невозможности производить запись событий аудита, произвести автоматическое выключение системы. Невозможность записи аудита событий системы обычно связана с переполнением хранилища этих сообщений. Для продолжения нормальной работы системы необходимо войти в нее под учетной записью администратора и произвести в программе:

Пуск\Панель управления\Администрирование\Просмотр событий

очистку всех этих сообщений, возможно, предварительно их сохранив. Это является гарантией того, что все действия системы или пользователей будут контролироваться администратором.

Пункт Devices: Prevent users from installing printer drivers – позволяет запретить пользователям устанавливать драйвера принтеров под их учетными записями.

Пункт Devices: Restrict CD-ROM access to locally logged-on user only позволяет ограничить доступ сетевых пользователей к локальному CD-ROM-приводу системы. Это может быть полезно, когда нужно чтобы сетевые пользователи имели доступ только к тем ресурсам, к которым они должны его иметь.

Пункт Devices: Restrict floppy access to locally logged-on user only позволяет ограничить доступ сетевых пользователей к локальному CD-ROM-приводу системы. Это может быть полезно, когда вы хотите, чтобы сетевые пользователи имели доступ только к тем ресурсам, к которым они должны его иметь. Это позволит локальным пользователям приватно работать с их личными носителями.

Пункт Devices: Unsigned driver installation behavior позволяет указать поведение системе, при попытке пользователей установить драйвер, не прошедший процедуру сертификации Microsoft. Он может иметь три значения:

- *Silent succeed – происходит инсталляция этого драйвера и никаких сообщений не выдается;*
- *Warn but allow installation – происходит предупреждение пользователя о том, что драйвер не прошел сертификацию, но инсталляция продолжается. Данный пункт используется по умолчанию;*

- *Do not allow installation – накладывается запрет на установку драйверов системы, не прошедших сертификацию.*

Пункт Interactive logon: Do not display last user name, в случае своего включения, запрещает показ системе имени пользователя, который в ней работал последним. Это удобно в тех случаях, когда нужно избежать подбора паролей взломщиками к учетным записям пользователей системы, т. к. если у них не будет не только пароля, но и имени учетной записи пользователя, то их задача может стать в два раза сложнее. Данный пункт работает только в том случае, если отключен экран приветствия системы.

Пункт Interactive logon: Do not require CTRL+ALT+DEL, в случае его выключения, производит отображение на экране таблички, требующей от пользователя нажатия комбинации клавиш CTRL+ALT+DEL для входа в систему. В случае включения этого пункта данное сообщение системы появляться не будет. Данный пункт работает только в том случае, если отклю-чен экран приветствия. Смысл ввода этой комбинации клавиш для входа в систему заключается в том, что она обрабатывается только системой. И это гарантирует то, что в операционную систему входит человек, а не программа по подбору паролей пользователей. Таким образом, данное сообщение может быть дополнительным барьером, охраняющим систему от взломщиков.

Пункт Interactive logon: Prompt user to change password before expiration устанавливает количество дней до конца срока действия пароля пользователя, когда система будет предупреждать пользователя об этом. Данный пункт имеет смысл только в том случае, если пароли пользователей имеют определенный срок действия.

Пункт Recovery console: Allow automatic administrative logon устанавливает автоматический вход системного администратора в консоль восстановления системы. Это удобно тем, что не требует ввода пароля администратора, но по той же причине, создает большие проблемы с безопасностью, так как консолью восстановления с администраторскими правами сможет воспользоваться любой желающий.

Пункт Recovery console: Allow floppy copy and access to all drives and all folders, в случае его включения, позволяет вам использовать команду SET консоли восстановления, которая может помочь установить следующие значения переменных:

- *AllowWildCards – переменная включает поддержку масок у команд, например, DEL;*
- *AllowAllPath – переменная позволяет получить доступ ко всем файлам и папкам системы.*
- *AllowRemovableMedia – переменная позволяет копировать файлы на сменные носители,например, гибкие диски;*
- *NoCopyPrompt – переменная запрещает системе выдавать дополнительные сообщения при перезаписи существующего файла.*

С помощью данного пункта можно скопировать или удалить информацию с жесткого диска системы. Поэтому не рекомендуется совмещать его использование с включенным предыдущим пунктом, позволяющим вход в консоль восстановления системы без администраторского пароля,т. к. можно лишиться всей информации.

Пункт Shutdown: Allow system to be shut down without having to log on позволяет, в случае его включения, производить выключение операционной системы до непосредственного входа в нее пользователями. Если вы не хотите, чтобы пользователи, не имеющие на это прав, выключали систему, установите данный пункт в положение Отключен.

Пункт Shutdown: Clear virtual memory pagefile является чрезвычайно важным в обеспечении безопасности вашей системы. При выключении системы в ее файле подкачки остаются данные, которые использовались в работе различными пользовательскими приложениями. Среди этих данных могут быть, частично или полностью, ваши документы, с которыми вы работали в

течение сеанса работы с системой. Впоследствии, во время вашего отсутствия, эти данные могут быть кем- либо извлечены из файла подкачки. Таким образом, возможна утечка информации. И чтобы этого не случилось, системе может потребоваться очищать свой файл подкачки. Это можно сделать, включив данный пункт. Однако учтите, время очистки файла займет некоторое дополнительное время, и система будет выключаться чуть дольше.

Политика обновления

Любое программное обеспечение содержит ошибки (баги), т. к. на этапе проектирования приложений и систем невозможно все предусмотреть. Поэтому в любом приложении появляются места кода, которые работают не так, как рассчитывали разработчики, что может привести к нештатной работе программного обеспечения, а также появлению новых ошибок или уязвимостей при его работе.

Для выявления ошибок все компании-разработчики стараются тестировать свое программное обеспечение, т. е. проверять работу программного обеспечения в шоковых для него условиях, когда его ограничивают в размере доступной памяти, дискового пространства, скорости работы центрального процессора и пр. На этом этапе вылавливаются ошибки и вносятся ис- правления в код программного обеспечения, улучшающие его стабильность (робастность) или отказоустойчивость. Однако эти меры лишь частично позволяют избавиться от наиболее явных ошибок, которые проявили себя в тестировании. В н. в. не существует аппаратных или математических методов, позволяющих избавиться от ошибок в программном обеспечении на этапе его разработки.

После долгих поисков компании-разработчики нашли простой метод, который позволяет практически со стопроцентной вероятностью избавиться от ошибок в конечных продуктах, находящихся у пользователей. Этим методом является периодическое обновление программных продуктов. Компании разработчики решили, что в идеале программное обеспечение должно работать двадцать четыре часа в сутки, семь дней в неделю и в его работе не должно быть никаких нештатных ситуаций, вызванных ошибками. Это можно достигнуть с помощью грамотной политики обновления, которая используется практически в любом современном программном продукте, т. е. система периодически выходит в Интернет и проверяет сайт компании-разработчика на появление обновлений к программному обеспечению.

Компания-разработчик для программного продукта периодически помещает на своем сайте исправления, обновления и дополнения. Исправления – это специальные заплатки для программного обеспечения, которые исправляют существующие в нем ошибки, замеченные пользователями или специалистами компании. Обновления включают различные обновления программного продукта и заплатки от обнаруженных в нем ошибок. Дополнения добавляют программному продукту определенную функциональность.

Обновления для пользователей Windows XP позволяют не только избежать ошибок ОС, проявляющихся при ее использовании, но и практически гарантированно защитить ее от взломщиков и вирусов, т. к. исправляются все замеченные ошибки в системе безопасности. Алгоритм работы системы обновления Windows XP настроен на периодическую проверку сайта компании Microsoft на наличие различных обновлений и скачивание или предупреждение пользователя, в зависимости от его настроек. Все настройки политики безопасности Windows XP находятся в программе Система:

Пуск\Настройка\Панель управления\Система

Все операции настройки политики обновления ОС, а также выполнения процедуры обновления и получения от нее различных сообщений возможны только под учетной записью администратора системы. После запуска программы появится окно, в котором нужно выбрать закладку Автоматическое обновление (Automatic Updates) (рис.1.12). На закладке можно

установить один из четырех параметров, которые будут определять частоту обновления системы:

1. *Автоматически (рекомендуется), Automatic (recommended) – параметр устанавливается операционной системой Windows по умолчанию и означает регулярное обновление системы, заданное в двух нижерасположенных параметрах: частоты обновления и времени обновления. По умолчанию Windows XP будет обновляться каждый день в три часа (рис.1.12.). Скачивание обновлений операционной системы может происходить параллельно с работой в Интернете, т. к. операционной системой резервируется двадцать процентов пропускной способности канала связи с Интернетом, что позволяет быстро и незаметно скачивать системные обновления с сайта Microsoft.*

Рисунок 1.12 - Закладка Автоматическое обновление программы Система

Если пользователь работает на домашнем компьютере, достаточно производить обновления системы раз в неделю. Если система является корпоративной или часто находится в Интернете, рекомендуется проводить каждодневное обновление, чтобы надежно защититься от сетевых взломщиков. Если система скачает обновления, и они будут готовы к инсталляции, система сообщит об этом. Если же за время выхода в Интернет система не успеет скачать все обновления, они будут скачаны в следующий раз. Все скачанные и установленные обновления можно удалить, воспользовавшись для этого программой Установка и удаление программ: Пуск\Панель управления\Установка и удаление программ.

2. *Загружать обновления, пользователь назначит время установки, Download updates for me, butlet me choose when to install them опция позволяет операционной системе самостоятельно скачивать обновления, но для их установки она должна спросить разрешения у пользователя.*
3. *Уведомлять, но не загружать и не устанавливать их автоматически, Notify me but don'tautomatically download or install them опция позволяет операционной системе проверять наличие обновлений, но запрещает их непосредственное скачивание или установку. Эта опция полезна, если пользователь сам устанавливаете обновления, например, с компакт-диска, также она позволяет сэкономить на интернет-трафике.*
4. *Отключит автоматическое обновление, Turn off Automatic Updates опция запрещает работу системы обновления Windows.*

Выполнение работы

Задание 1. *Изучите:*

1) *настройку Политики безопасности на своем ПК.*
2) *настройку Параметров безопасности на своем ПК.*
3) *настройку Политики обновления на своем ПК.*

Задание 2. *Ответьте на вопросы:*

1. *Определите назначение политики безопасности системы.*
2. *Где производится настройка политики безопасности системы?*
3. *Как запретить доступ сетевых пользователей к компьютеру?*
4. *Как разрешить доступ сетевым пользователям, которым разрешено работать в системе ккомпьютеру?*
5. *Определите назначения пункта политики безопасности Разрешать вход в систему черезслужбу терминалов.*
6. *Как предоставить определенной группе пользователей вносить изменения в системное время?*
7. *Определите назначение пункта политики безопасности Отладка программ.*
8. *Каким образом запретить вход определенной группе пользователей в систему по локальнойсети?*
9. *Определите назначение пункта политики безопасности Принудительное удаленное завершение.*
10. *Как установить пользователей и их группы, которые могут локально входить в систему?*
11. *Как запретить определенной группе пользователей завершать работу системы, и в какихслучаях это актуально?*
12. *В каком разделе производится настройка глобальных параметров безопасности?*
13. *Определите назначение политики обновления.*
14. *Как произвести настройку политики обновления?*
15. *Какие события безопасности должны фиксироваться в журнале аудита?*
16. *Какие параметры определяют политику аудита?*
17. *Какие факторы влияют на определение размеров доменов безопасности?*
18. *Какие дополнительные возможности разграничения доступа к информационным ресурсампредоставляет шифрующая файловая система?*

Практическая работа № 8. Установка и настройка сервера

1. Цель практической работы

Познакомиться с основными принципами создания базы данных в MS SQL Server. Изучить операции, проводимые с базами данных в целом. Получить навыки использования программы "SQL Server Management Studio" для создания, удаления, регистрации, подключения, извлечения метаданных, резервного копирования и восстановления базы данных. Изучить SQL-операторы для создания, подключения и удаления базы данных. Познакомиться с основными принципами управления учетными записями и ролями.

2. Исходные данные

Студент получает индивидуальный вариант исходных данных с кратким описанием предметной области, который используется при выполнении всех описанных в данном пособии практических работ. При этом каждая очередная Практическая работа является продолжением выполненной ранее и поэтому они должны обязательно выполняться последовательно.

3. Используемые программы

1.Работающий на компьютере ***сервер "MS SQL Server"****.*

2. Установленная платформа ***.NET Framework****.*

3. *Операционная система* ***Microsoft Windows.***

*4. Приложение "****SQL Server Management Studio****", установленное налокальном компьютере.*

4. Теоретические сведения

На сегодняшний день известно более двух десятков серверных СУБД, из которых наиболее популярными являются Oracle, Microsoft SQL Server, Informix, DB2, Sybase, InterBase, MySQL.

Для выполнения практических работ будет использоваться сервер " Microsoft SQL Server".

Microsoft® SQL Server™ *— это система анализа и управления реляционными базами данных в решениях электронной коммерции,производственных отраслей и хранилищ данных.*

Microsoft SQL Server *— система управления реляционными базами данных (СУБД), разработанная корпорацией Microsoft. Основной используемый язык запросов —* ***Transact-SQL****, создан совместноMicrosoft и Sybase. Transact-SQL является реализацией стандарта*

ANSI/ISO по структурированному языку запросов (SQL) с расширениями. Используется для работы с базами данных размером от персональных до крупных баз данных масштаба предприятия; конкурирует с другими СУБД в этом сегменте рынка.

В SQL Server имеется большой набор интегрированных служб, расширяющих возможности использования данных: вы можете составлять запросы, выполнять поиск, проводить синхронизацию, делать отчеты, анализировать данные. Все данные хранятся на основных серверах, входящих в состав центра обработки данных. К ним осуществляется доступ с настольных компьютеров и мобильных устройств. Таким образом, вы полностью контролируете данные независимо от того, где вы их сохранили.

Система SQL Server позволяет обращаться к данным из любого приложения, разработанного с применением технологий Microsoft .NET и Visual Studio, а также в пределах сервисно-ориентированной архитектуры и бизнес-процессов — через Microsoft BizTalk Server. Сотрудники, отвечающие за сбор и анализ информации, могут работать с данными, не покидая привычных приложений, которыми они пользуются каждый день, например приложений выпуска 2007 системы Microsoft Office.

В Microsoft SQL базы данных хранятся в виде обычных файлов на диске. Какминимум на одну БД приходится таких ***файлов 2: *.mdf и *.ldf.*** *В первом хранятся сами данные, таблицы, индексы и пр., а во втором находится т.н. transaction log, в котором находится информация необходимая для восстановления БД.*

Файл с базой данных *представляет собой набор страниц одинакового размера. Размер страницы задается при создании базы данных и может быть изменен только при ее восстановлении из резервной копии. Чтение и запись данных в базе данных осуществляется постранично.*

Все операции с базой данных должны производиться только посредством команд к SQL-серверу. *Для клиентских приложений эти файлы абсолютно бесполезны и при правильной организации доступа пользователей к файлам в сети, вообще не должны быть доступны.*

Сервер СУБД не имеет интерфейса пользователя *и для выполнения операций с базой данных ему необходимо посылать команды либо с помощью командной строки или с помощью какой-либо прикладной программы.*

Для выполнения операций с базой данных при проведении практических работпредлагается использовать программу " ***SQL Server Management Studio****"(рис. 1), представляющую собой наиболее распространенное и удобное средствоадминистрирования баз данных под управлением MS SQL Server (Среда ManagementStudio Express доступна для свободной загрузки из центра загрузки Майкрософт.*

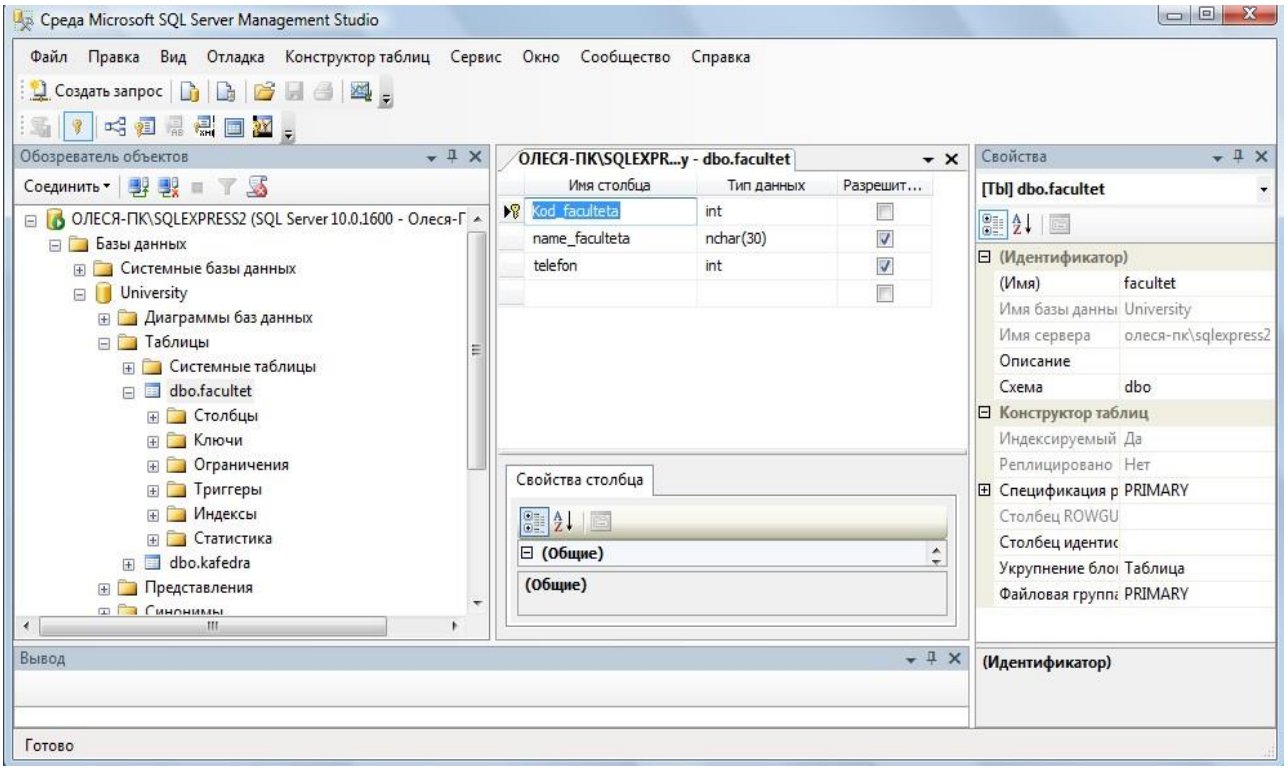


Рис. 1. Программа SQL Server Management Studio

Среда SQL Server Management Studio *— это интегрированная среда для доступа, настройки, управления, администрирования и разработки всех компонентов SQL Server. Среда SQL Server Management Studio объединяет большое число графических средств с набором полнофункциональных редакторов сценариев для доступа к SQL Server разработчиков и администраторов с любым опытом работы.*

Среда SQL Server Management Studio обеспечивает следующие основные возможности:

- *поддерживает большинство административных задач для SQL Server;*
- *единая интегрированная среда для управления SQL Server Database Engine и разработки;*
- *новые управляющие диалоговые окна для управления объектами в компоненте SQL Server Database Engine, службах Analysis Services, Reporting Services, Notification Services и выпуске SQL Server Compact, позволяющие выполнять действия немедленно, направлять их в редактор кода или включать эти действия в сценарий для последующего выполнения;*
- *экспорт и импорт регистрации сервера среды SQL Server Management Studio из одной среды Management Studio в другую;*
- *сохранение и печать XML-файлов плана выполнения и взаимоблокировок, созданных приложением SQL Server Profiler, просмотр их в любое время и отправка для анализа администратору;*
- *новые окна сообщений об ошибках и информационных сообщений, предоставляющие гораздо больше сведений и позволяющие отправлять в Майкрософт комментарии о сообщениях, копировать сообщения в буфер обмена и отправлять их по электронной почте в службу поддержки;*
- *встроенный веб-обозреватель для быстрого обращения к библиотеке MSDN или получения интерактивной справки;*
- *встроенная справка от сообществ в Интернете и т.д.*

Большинство действий с базой данной MS SQL Server в среде Среда SQL Server Management Studio может быть осуществлено двумя способами: ***либо выполнением операторов языка SQL*** *в окнах "**Script Execute**" (подключение к базе данных не обязательно) и "**SQL Editor**" (требуется подключение к базе данных), либо с использованием меню и диалоговых*

окон. В последнем случае операторы SQL, которые требуются для выполнения данного действия, будут сгенерированы и выполнены средой SQL Server Management Studio автоматически.

1. Изучите историю ***MS SQL Server,*** *используя поисковую систему браузера, ответьте на вопросы и оформите ответы в отчет:*

1. *Язык SQL какой компанией был создан и в каком году?(IBM, 1970 г)*
2. *Изначально он назывался как? (SEQUEL - Structured English Query Language)*
3. *Какой язык лег в основу* ***SQL Server?*** *(T-SQL - Transact - SQL)*
4. *Для какой операционной системы появилась сетевая СУБД SQL Server версия 1.0? (для операционной системы IBM OS/2)*
5. *Дополните: СУБД SQL Server версия 1.0 создавалась фирмой _____ и двумя ее подрядчиками. Назовите подрядчиков? (Microsoft и Sybase)*
6. *Заполните таблицу*

n/n	***Компания(компании) разработчиков***	***Год создания версии SQL***	***Номер версии***

7. *Добавьте:*

SQL Server – это …(реляционная СУБД)

SQL Server Management Studio - …(основная утилита для работы с базами данных)

II. Установите приложения и установите подключения, оформите в отчет полученные результаты.

Установка MS SQL Server и

1. *Перейдите по ссылке* https://www.microsoft.com/ru-RU/download/details.aspx?id=104781
2. *Выберите английский язык, обратите внимание на системные требования и минимальные требования к оборудованию.*
3. *Выберите пункт Скачать.*
4. *Запустите exe файл.*
5. *Выберите тип установки – Базовая*
6. *Определите русский язык, Принять*
7. *В итоге у вас появляется окно, см. рис. 1*

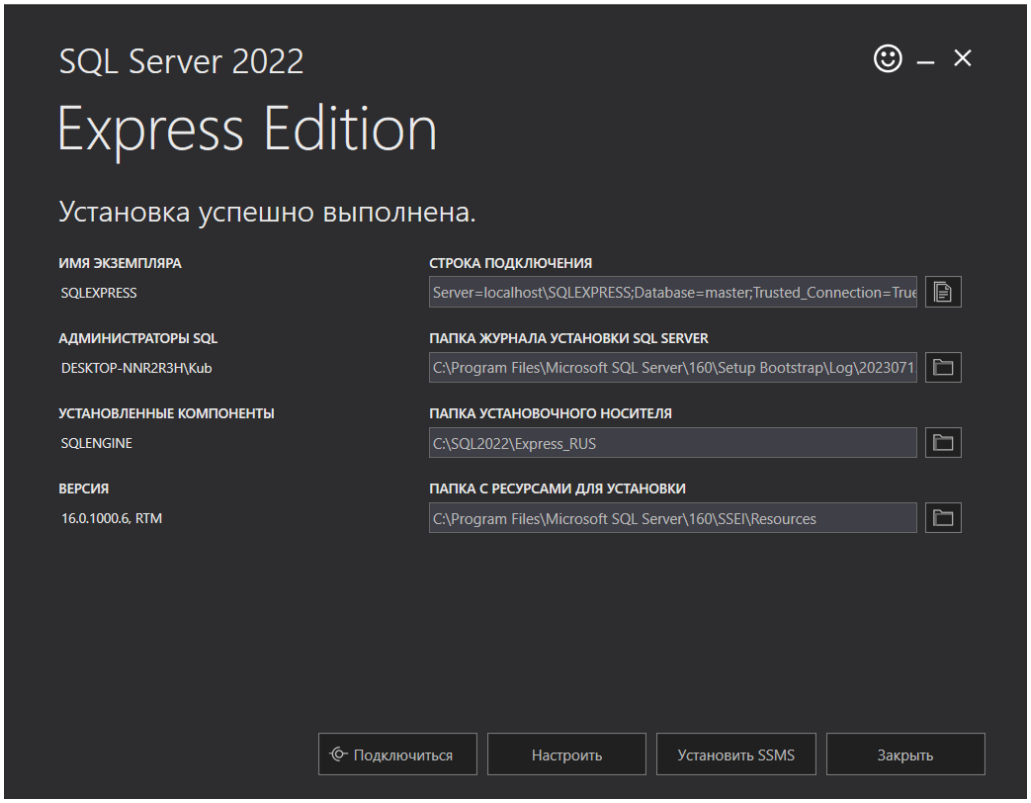


рис. 1

8. *Перейдите к пункту Установить SSMS — это интегрированная среда для управления любой инфраструктурой SQL, от SQL Server до баз данных SQL Azure*
9. *Обратите внимание на системные требования для установки SSMS и минимальные требования к оборудованию.*
10. *Выберите пункт Бесплатная загрузка для SQL Server Management Studio (SSMS) 19.1*
11. *Загрузится установочный файл, запустите установочный файл и следуйте инструкциям.*
12. *Установка завершена. Выберите пункт Закрыть.*
13. *Убедитесь, что приложение установилось.*

Подключение к Microsoft SQL Server с помощью SSMS

1. *Запустите среду SSMS и в окне Соединение с сервером введем данные для того, чтобы подключиться. В поле* ***Имя сервера*** *введите имя экземпляра ядра СУБД. В экземпляре SQL Server по умолчанию имя сервера совпадает с именем компьютера. Для именованного экземпляра SQL Server именем сервера является <computer_name>\<instance_name>, например* ***ACCTG_SRVR\SQLEXPRESS, см. рис. 2***

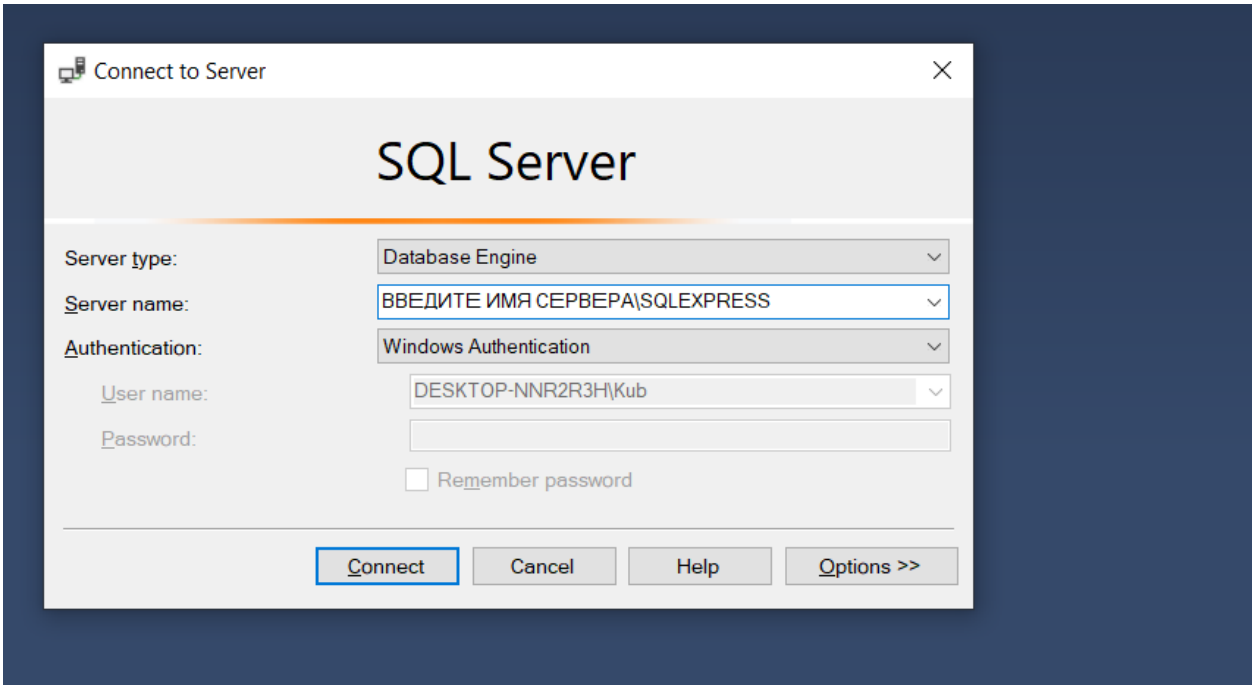


рис.2

5. Задание

Практическую работу следует выполнять в следующем порядке:

1. *Создать рабочую папку для хранения файлов, получаемых при выполнении практическойработы.*
2. *На основании индивидуального задания выбрать имя файла создаваемой базы данных. Для имени лучше всего выбрать одно или несколько английских слов, соответствующих наименованию предметной области. Использование для имени русских слов, записанных латинскими буквами, не допускается.*
3. *Открыть приложение " Среда SQL Server Management Studio ".*
4. *Создать соединение с локальным или удаленным сервером.*
5. *Создать базу данных для своей предметной области с помощью диалога, выбрав локальный сервер "**Имя_компьютера\SQLEXPRESS**"*
6. *Создать базу данных.*
7. *Извлечь метаданные для автоматической генерации команды создания базы данных.*
8. *Удалить базу данных, выполнив команду "**Database/Drop Database**" (База данных/Удалить базу данных).*
9. *Создать базу данных вторым способом, выполнив в окне "**Script Executive**" операторы, полученные при извлечении метаданных перед предыдущим удалением.*
10. *Создать резервную копию базы данных.*
11. *Удалить базу данных.*
12. *Восстановить базу данных из резервной копии.*
13. *Сохранить файл сценария на сервере в папке "Студент", дав ему имя «лаб.№1» и стандартное расширение "***.sql**".*

6. Ход работы

2.6.1. Создание соединения с сервером

Выполните следующие инструкции:

*Работа с приложением **SQL Server Management Studio** начинается с создания соединения с установленным сервером. Убедитесь вначале, что сервер Microsoft SQL Server на локальной машине или на сервере компьютерного класса установлен и работает.*

Откройте приложение " SQL Server Management Studio ".

*В диалогом окне **Соединение с сервером** подтвердите заданные по умолчанию параметры и нажмите кнопку **Соединить**, см. рис.2.*

*Для соединения необходимо, чтобы поле **Имя сервера** содержало имя компьютера,*

на котором установлен SQL Server.

*Если компонент **Database Engine** является именованным экземпляром, то поле **Имя сервера** должно также содержать имя экземпляра в формате*

<имя_компьютера>\<имя_экземпляра>.

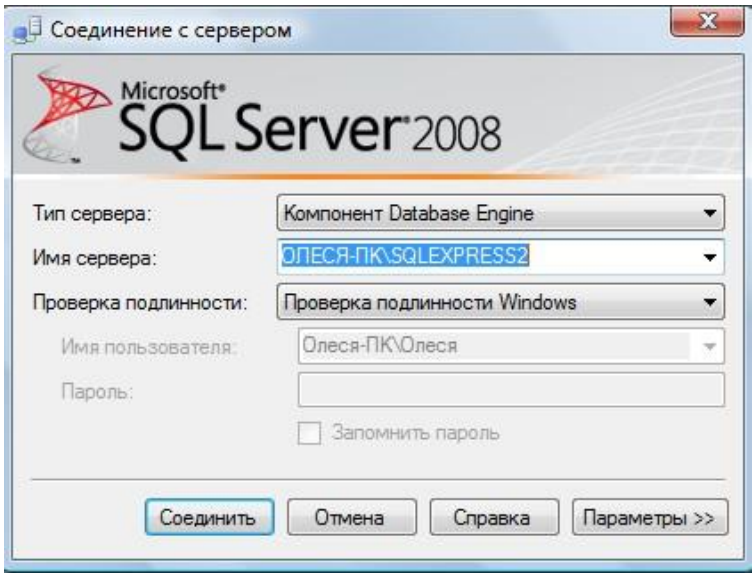


Рис. 2. Создание соединения с серверомВ параметрах указываем:

Тип сервера –** Компонент **Database Engine.

***Имя сервера**. Подключение может быть **локальным** или **удаленным**. Представляет собой название компьютера в сети, на котором установлен сервер СУБД. Если сервер установлен на том же компьютере, где сейчас работает пользователь, то в качестве имени используется имя компьютера и идентификатор сервера;*

***проверка подлинности** – Windows (по умолчанию),*

***имя пользователя** –имя пользователя по умолчанию, зарегистрированного на сервере MS SQL Server (задается при установке сервера),*

***пароль** – пусто или пароль для пользователя, заданного для сервера MS SQL Server;*

*Нажмите кнопку **Соединить**. Если соединение будет совершенно успешно, то на экране появятся данные сервера.*

Среда Management Studio представляет данные в виде окон, выделенных для отдельных типов данных. Сведения о базе данных отображаются в обозревателе объектов и окнах документов.

Обозреватель объектов является представлением в виде дерева, в котором отображаются все объекты базы данных на сервере. Он может содержать базы данных компонента SQL Server Database Engine, служб Analysis Services, служб Reporting Services, служб Integration Services и SQL Server Compact.

*Обозреватель объектов включает сведения по всем серверам, к которым он подключен. При открытии среды Management Studio пользователю предлагается применить при подключении обозревателя объектов параметры, которые использовались в прошлый раз. Чтобы подключиться к любому из серверов, следует дважды щелкнуть его в компоненте «**Зарегистрированные серверы**», однако регистрировать его не обязательно, см. рис.1.*

Окно документов представляет собой наиболее крупную часть среды Management Studio. В окнах документов могут размещаться редакторы запросов и окна обзора. По

*умолчанию отображается страница «**Сводка**», подключенная к экземпляру компонентаDatabase Engine на текущем компьютере.*

2.6.2. Общие сведения о базах данных MS SQL Server

*Кроме четырех системных баз, SQL Server может обрабатывать до **32 734** базданных, определяемых пользователем.*

База данных представляет собой:

- *набор взаимосвязанных таблиц;*
- *связанный набор страниц, выделенных для хранения данных MS SQL Server;*
- *совокупность данных при архивации;*
- *два и более файла;*
- *важную совокупность данных для целей защиты и управления.*

Файлы базы данных

База данных состоит из двух и более файлов, каждый из которых может использоваться лишь одной базой.

*У файлов существуют два имени: **логическое и физическое**. **Логическое имя** подчиняется стандартным правилам выбора имен объектов SQL Server. **Физическое имя** представляет собой полное имя любого локального или сетевого файла. Максимальное число файлов в базе данных — 32 768. **Файлы делятся на три типа:***

- ***Первичные файлы**. Используются для хранения данных и информации, определяющих начальные действия с базой. База данных содержит лишь один первичный файл. Стандартное расширение — **.mdf**.*
- ***Вторичные файлы**. Одна или несколько вспомогательных областей для хранения данных. Могут использоваться для распределения операций чтения/записи по нескольким дискам. Стандартное расширение — **.ndf**.*
- ***Файлы журналов**. Содержат журналы транзакций базы данных. База данных содержит по крайней мере один файл журнала. Стандартное расширение — **.ldf**. Перед непосредственной записью транзакций в файл данных все вносимые изменения записываются в журнал.*

Группы файлов

Группы файлов предназначены для объединения нескольких файлов. Каждый файл может входить не более чем в одну группу. Файлы журналов не могут принадлежать никаким группам. Группы файлов используются для распределения операций чтения/записи по нескольким дискам. Если группа содержит более одного файла, операции записи распределяются между файлами группы. Базы данных могут содержать до 32 768 групп файлов.

У каждой базы данных имеется ***первичная группа файлов****. Она содержит первичный файл данных и все файлы, которые не были явно назначены в другую группу файлов. Имя первичной группы файлов —* ***PRIMARY****.*

2.6.3. Создание и регистрация базы данных

Для создания базы данных можно использовать один из ***двух способов****:*

Первый способ создания БД*. Выполнить команду "****База данных/Создать базу данных...****" в программе SQL Server Management Studio, ввести параметры создаваемой базы данных в диалоговом окне "****Создание базы данных****" (рис. 3) и нажать кнопку [OK].*

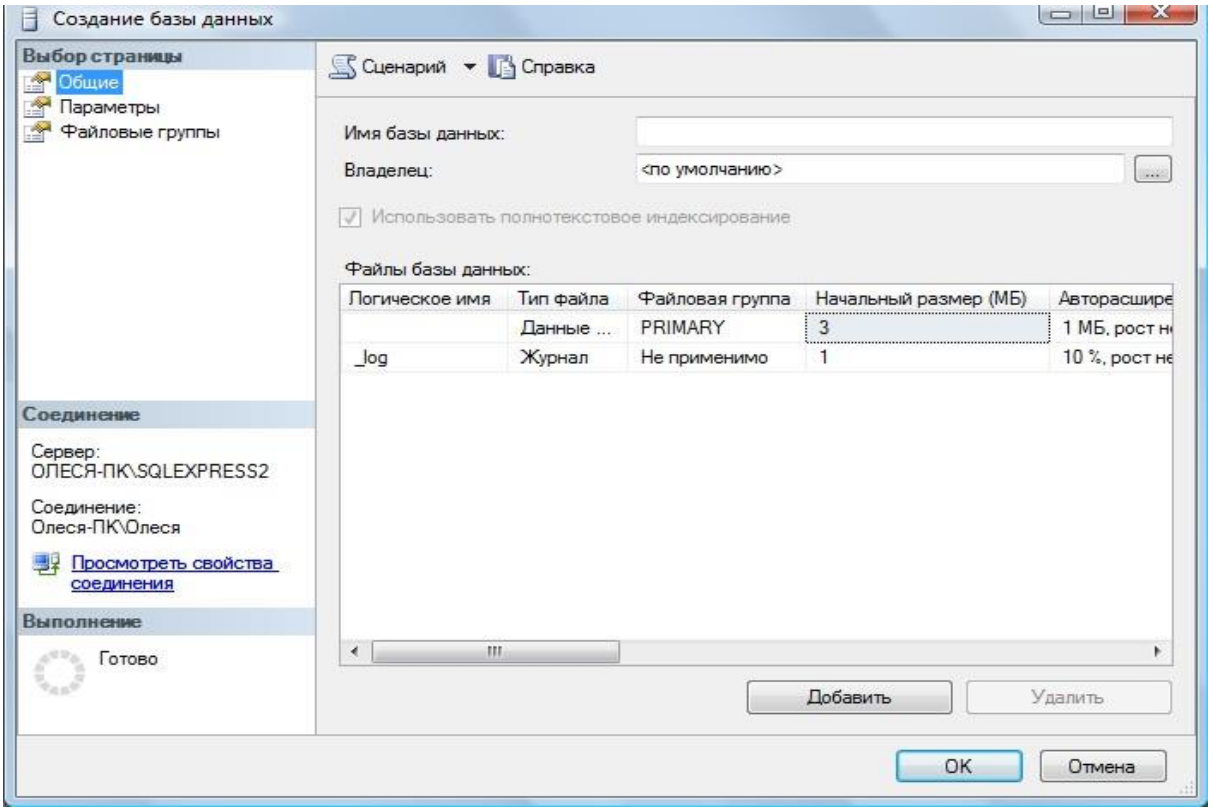


Рис. 3. Диалоговое окно создания базы данных

В поле ***Имя базы данных*** *введите имя нашей будущей базы данных, например –*

University*.*

Поле ***Владелец*** *- задан по умолчанию, в зависимости от настройки сервера.*

Папка с базой данных будет создана по умолчанию на диске ***C:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS2\MSSQL\DATA \.***

Прежде чем нажать кнопку ***Добавить****, просмотрите* ***Параметры*** *и* ***Файловые группы*** *для создаваемой базы данных.*

*После нажатия на кнопку [****OK****] программа " SQL Server Management Studio " создастбазу данных, имя которой вы увидите в обозревателе объектов, а также сгенерирует необходимый*

SQL-код для создания базы данных с теми свойствами, которые указаны в этом диалоговом окне и передаст его серверу СУБД для выполнения.

Пример этих операторов приведен на рис. 4. (нажмите на имени базы данных ***University*** *правой клавишей и из контекстного меню выберите* ***Создать скрипт как.. CREATE****). Если параметры введены правильно, база данных будет создана.*

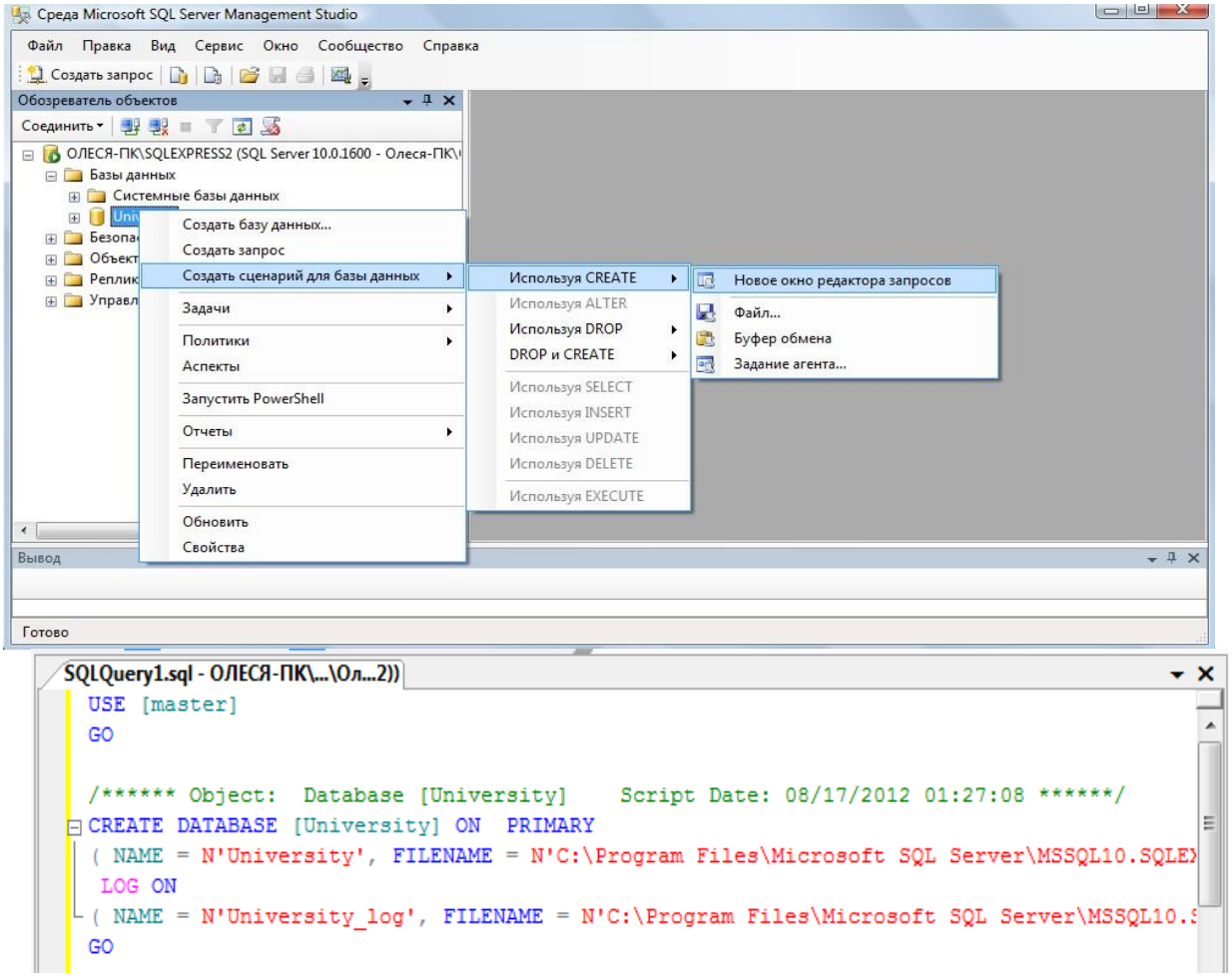


Рис. 4. Сгенерированный sql-код созданной базы данных

*Содержащиеся в сценарии операторы отделяются друг от друга символом "**;**". Сценарий может содержать поясняющие комментарии двух видов:*

*многострочный комментарий (начинается символами "**/***" и заканчивается символами "***/**") и однострочный комментарий, который начинается символами "**--**" и продолжается до конца строки.*

При создании базы данных возможны следующие типичные ошибки:

1. *На целевом компьютере не запущен или не установлен сервер СУБД –т.е. выполнять команду создания базы данных просто некому.*
2. *На целевом компьютере нет каталога, в котором предполагается создатьбазу данных.*
3. *Файл, в котором должна будет находиться база данных на сервере, уже существует.*

После создания базы данных вся введенная о базе данных информация запоминается программой SQL Server Management Studio и в окно редактора в дерево на вкладке "Проводник" добавляется узел с зарегистрированной базой данных (рис. 5).

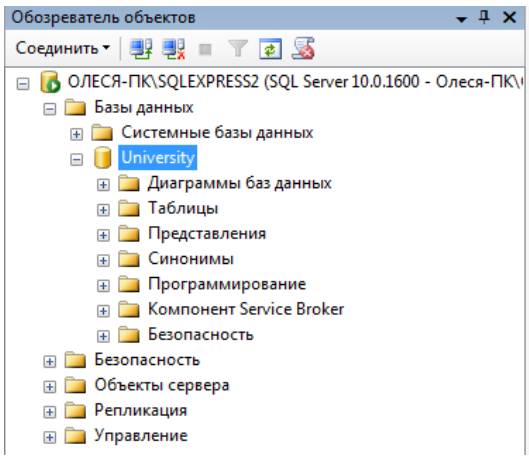
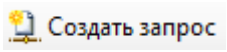
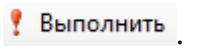


Рис. 5. Перечень зарегистрированных баз данных в SQL Server Management Studio

Второй способ создания БД. *Выполнить в программе SQL Server Management Studio команду* ***"Создать запрос"*** 

на панели инструментов, затем ввести команду, создающую базу данных в окне "Script Execute" (рис. 3) и нажать кнопку 

.

Команда CREATE DATABASE - Создание базы данных MS SQL Server

Базы данных создаются командой ***CREATE DATABASE****. Создание баз данных разрешается любому пользователю с ролью системного администратора или всем, кому системный администратор предоставил такое право. Команда* ***CREATE DATABASE*** *имеет следующий синтаксис:*

```
01. CREATE DATABASE имя_базы
02. [ ON [PRIMARY] ([ NAME = логическое_имя_файла, ]
03. FILENAME = 'имя_файла_ОС'
04. [, SIZE = размер]
05. [, MAXSIZE = { максимальный_размер | UNLIMITED } ]
06. [, FILEGROWTH = приращение] )
07. | {FILEGROUP имя_группы_файлов FILEDEFINITIONS}
08. [,...n] ]
09. [LOG ON {[ NAME = логическое_имя_файла, ]
10. [FILENAME = 'имя_файла_ОС'
11. [, SIZE = размер]
12. [, MAXSIZE = { максимальный_размер | UNLIMITED } ]
13. [, FILEGROWTH = приращение] } [,...n]
14. [FOR LOAD | FOR ATTACH]
```

Если при создании базы не указан первичный файл данных и/или файл журнала, то отсутствующий файл (или файлы) создается с именем по умолчанию.

Физические файлы будут находиться в стандартном каталоге.

Первичному файлу присваивается имя ***имя_базы.mdf****, а файлу журнала —* ***имя_базы_log.ldf****.*

Если размер файлов не задан, то при создании размер первичного файла совпадает с размером первичного устройства базы **model**, *а размер файла журнала и вторичных файлов данных равен 1 Мбайт. Он может быть и больше, если размер*

первичного файла базы данных model превышает 1 Мбайт. Хотя имена и размеры файлов указывать не обязательно, на практике это всегда следует делать. SQL Server создает базу данных за два этапа. На первом этапе база model копируется в новую базу данных, а на второмэтапе инициализируется все неиспользуемое пространство.

Команда ***CREATE DATABASE*** *имеет следующие параметры:*

- ***PRIMARY*** *— файл определяется как первичное устройство.*
- ***NAME*** *— логическое имя; по умолчанию совпадает с именем файла.*
- ***FILENAME*** *— полное имя файла на диске.*
- ***SIZE*** *— исходный размер файла. Минимальный размер файла журнала равен 512Кбайт.*
- ***MAXSIZE*** *— максимальный размер файла.*
- ***UNLIMITED*** *— размер файла не ограничивается.*
- ***FILEGROWTH*** *— приращение размера в мегабайтах (MB), килобайтах (KB) илипроцентах (%). По умолчанию приращение равно 10%.*
- ***FOR LOAD*** *— обеспечивает обратную совместимость со сценариями SQL, написанными для предыдущих версий SQL Server.*
- ***FOR ATTACH*** *— указывает, что файлы базы данных уже существуют.*

Пользователь, создавший базу данных, является ее владельцем. Все параметры конфигурации базы копируются из базы model, если только при создании базы не был указан параметр ***FOR ATTACH.*** *В этом случае параметры конфигурации читаются из существующей базы данных. Рассмотрим некоторые примеры команды* ***CREATE DATABASE****:*

/ База данных со стандартным размером и именами файлов */*

```
01. CREATE DATABASE test1
02. /* Данные – 2 Мбайт, файл журнала – по умолчанию */
03. CREATE DATABASE test2
04. ON (FILENAME = 'c:\d1.mdf', SIZE = 2, NAME = 'd1')
05. /* Первичный файл – 10 Мбайт, одна группа файлов
06. g1 и журнал размером 10 Мбайт */
07. CREATE DATABASE test3
08. ON PRIMARY (FILENAME ='c:\test3.mdf',
09. SIZE = 10 , NAME = 'd1'),
10. FILEGROUP g1 (FILENAME – 'c:\g1.mdf',
11. SIZE = 10 , NAME = 'g1')
12. LOG ON (FILENAME ='c:\test3.ldf',
13. SIZE = 10, NAME = 'log1')
```

Задача 1. *Создайте sql-скрипт создания новой базы данных под именем* ***Educator*** *на* ***"D:\Базы данных\Группа\ФИО_студента\Название_БД.mdf****, с первичным устройством, с исходным размером файла в 10 Мбайт и запустите на выполнение скрипт(кнопка*  *на панели инструментов). Выполните в окне обозревателя объектов* ***Обновление****. Сохраните созданный скрипт в текущую папку под именем* ***1.sql****.*

После успешного выполнения и обновления проводника у вас должна появится новая база данных.

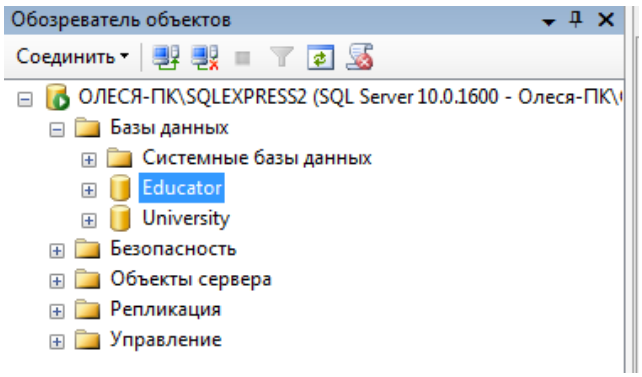


Рис. 6. Окно проводника после выполнения сценария создания базы данных

2.6.4. Подключение к базе данных

Чтобы подключиться к зарегистрированной базе данных, надо выбрать нужную базу данных в списке (рис. 5) и сделать двойной щелчок мышкой на выбранной базе данных.

Если все параметры подключения были введены правильно, то произойдет подключение к базе данных, название подключенной базы данных в окне "Обозревателя объектов" будет выделено жирным шрифтом, а также появятся вложенные узлы с объектами, содержащимися в подключенной базе данных (рис. 7).

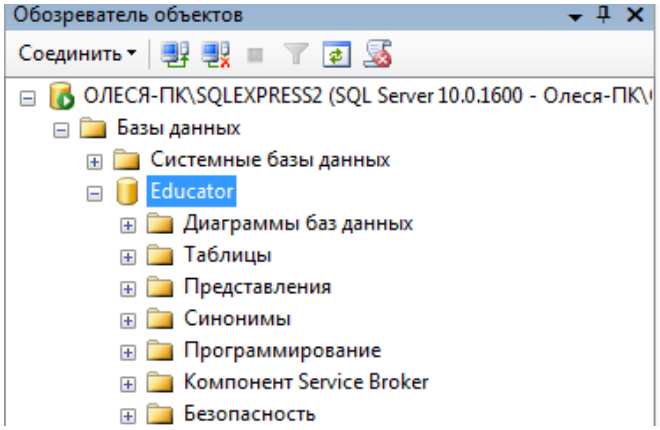


Рис. 7. Зарегистрированные базы данных в SQL Server Management Studio

После подключения к базе данных можно просматривать имеющиеся объекты, создавать новые, вносить и просматривать данные, а также проводить операции с имеющимися объектами.

*После создания БД в окне **Обозревателя объектов** (его можно вызвать по **<F8>**) выбираем **DataBases (Базы данных)** и откроется список БД, в котором откроем созданную БД (если она не появилась, то в окне **Object Explorer** нажать **<F5>** для обновления списков), которая состоит из восьми вложенных разделов (некоторые содержат еще дополнительные разделы), соответствующих объектам СУБД SQL Server:*

Database Diagrams (Диаграммы БД)	***Views (Представления)***	***Programmability (Объекты программирования)***
Tables (Таблицы)	***Synonyms (Синонимы)***	***Security (Безопасность)***
Service Broker	***Storage***	

На начальном этапе раздел созданной БД пуст, за исключением некоторых объектов, которые создаются по умолчанию, например в разделе ***Security/ Users*** *создаются пользователи, которые имеют право на доступ к объектам БД, их можно изменить.*

2.6.5. Удаление базы данных

Для удаления базы данных можно использовать один из трех способов:

*1. Выполнить в программе " SQL Server Management Studio " команду контекстного меню "****Удалить****" , выбрав перед этим в списке базу данных, а затем подтвердить свое желание в диалоговом окне.*

2. Выполнить оператор ***DROP DATABASE*** *в SQL-редакторе.*

3. *Удалить файл с базой данных.*

Синтаксис оператора ***DROP DATABASE:***

DROP DATABASE database_name;

2.6.6. Резервное копирование и восстановление

Резервное копирование *(****backup****) базы данных и* ***восстановление*** *из резервной копии (****restore****) – два важнейших и наиболее частых процесса, осуществляемых администраторами баз данных.*

Резервное копирование базы данных – единственный надежный способ предохранить данные от потери в результате поломки диска, сбоев электропитания, действий злоумышленников и ошибок в программах. В процессе резервного копирования создается независимый от платформы "снимок" базы данных, с помощью которогоможно перенести данные на другую операционную систему или даже другую платформу. ***Полный цикл:*** *резервное копирование и восстановление из резервной копии приводит к корректировке статистической информации, является средством от излишнего "разбухания" базы данных и необходимой операцией обслуживания базы данных. Кроме того, миграция от одной версии сервера к другой также происходит при помощи процесса* ***backup/restore.***

Для создания резервной копии базы данных с помощью программы " SQL Server Management Studio " необходимо подключиться к базе данных, выбрать из контекстного меню базы данных ***Задачи/ Создать резервную копию****. В открывшемся диалоговом окне "****Мастер резервного копирования****" задать несколько параметров и нажать кнопку [****Выполнить****], см. рис.8.*

После выбора пути и файла для резервной копии в окне ***Back Up Database*** *нажатием на ОК запускаем процесс создания резервной копии. В случае успешной работы появится сообщение.*

*В результате будет создан файл с резервной копией. Стандартным расширением таких файлов для " SQL Server Management Studio " является "*****.bak****". Файл с резервной копией базы данных обычно на порядок меньше оригинала.*

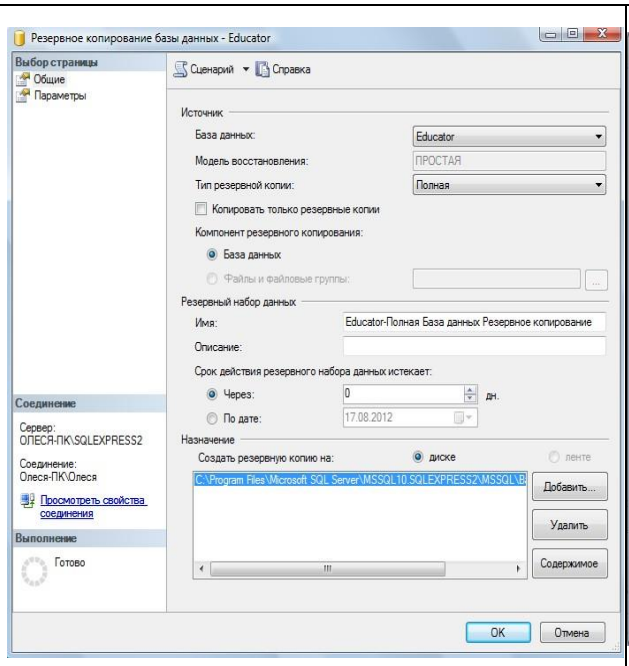


Рис.8. Создание резервной копии базы данных

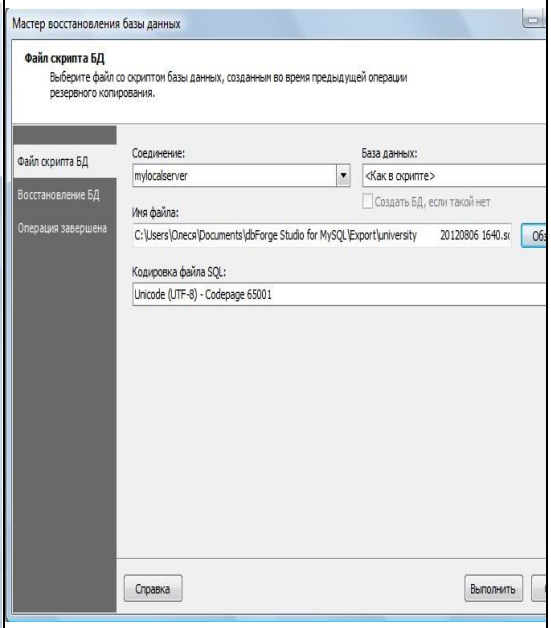


Рис.9. Восстановление базы данных

*Для восстановления базы данных из резервной копии используется команда "**База данных/ Восстановление базы данных**. В результате откроется диалоговое окно "**Мастер восстановления баз данных**", в котором надо выбрать имя БД куда будет восстанавливаться база данных, в которую будет помещен результат, способ восстановления, файл, из которого будет восстанавливаться база данных, отмечаем выбранную резервную копию, и нажать кнопку [**Восстановить**], см.рис.9. Запускаем процесс восстановления. В случае успешного выполнения получим сообщение.*

Резервное копирование и восстановление базы данных, наряду с процессом извлечения метаданных и последующего выполнения полученного сценария, можно использовать при переносе разрабатываемой базы данных между различными компьютерами для обеспечения самостоятельной работы студентов над практическими работами и курсовым проектом.

***Самостоятельно** Выполните вначале резервирование, а затем восстановление базы данных.*

*Удалите базу данных **Educator** с помощью скрипта сохраните sql-запрос.*

7. Копирование и перенос на другой сервер БД

*Для просмотра, запуска, остановки служб MS SQL Server необходимо запустить утилиту **SQL Server Configuration Manager** (рис. 10).*

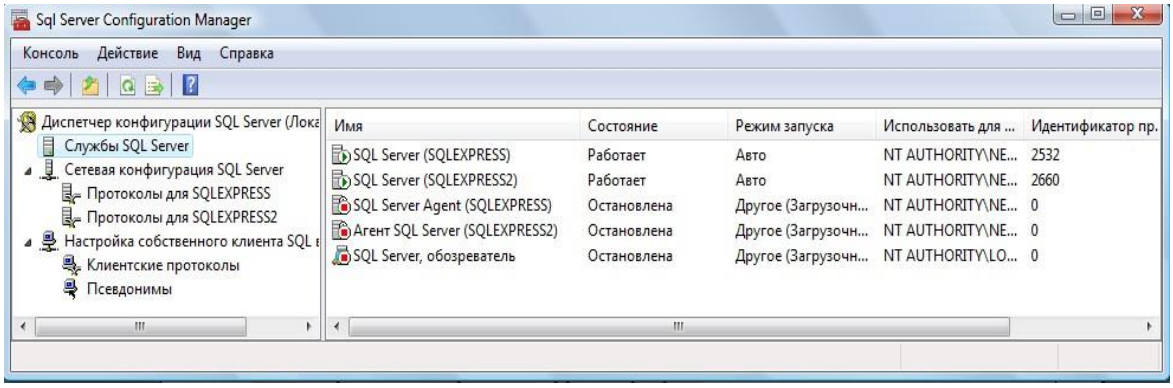


Рис.10. Список служб сервера БД

*Для того **чтобы скопировать БД** необходимо остановить службу **SQL Server** (в ее контекстном меню выбрать **Stop**). Далее в подпапке **…\MSSQL.1\MSSQL\Data** скопировать файлы с вашим названием БД (по умолчанию их два). Не забудьте потом снова запустить службу **SQL Server** (в ее контекстном меню выбрать **Start**).*

*Для того **чтобы подключить** скопированную **БД** на другом сервере, нужно предварительно скопировать ваши файлы в папку **…\MSSQL.1\MSSQL\Data** соответствующего сервера. Далее запустить утилиту **SQL Server Management Studio.** В появившемся окне с названием **Object Explorer** Проводник объектов (его можно вызвать по <**F8**>) выбираем **DataBases (Базы данных)** и по <правой кнопке мыши> в контекстном меню (рис. 5) выбираем **Attach… (Присоединить…**). В появившемся окне **Attach DataBases** (Присоединение базы данных) нажать <**Add**> и выбрать ваш файл БД с расширением **.mdf**.*

8. *Системные базы данных*

Системные базы данных сервера, создаваемые при установке, и их файлы представлены в таблице 1.

Название	Назначение	Размещение
Master	Хранит всю информацию сервера, включая учетные записи и параметры, сведения о всех базах и нахождении их первичных файлов с данными об инициализации баз данных пользователя.	Master.mdb – файл данных (75.mb) Mastlog.ldf – журнал транзакций (1 mb)
TempDB	Хранит все временные системные и пользовательские объекты: таблицы, переменные, хранимые процедуры, курсоры и т.п.	Temppdb.mdf – файл данных (8 mb) Templog.ldf – журнал транзакций (0.5 mb)
Model	Является шаблоном, задаваемых администратором и используемым для создания любых пользовательских баз данных. Содержит параметры по умолчанию, которые можно переопределять при создании соответствующей базы данных пользователя.	Model.mdf – файл данных (0.75 mb) Model.ldf – журнал транзакций (0.75 mb)
MSDB	Хранит информацию, относящуюся к автоматизации администрирования и управления сервером.	Msdbdata – файл данных (3.5 mb) Msdblog – журнал транзакций (0.75 mb)
		Всего – 22.75 mb

Все системные и пользовательские базы данных содержат в обязательном порядке 18 системных таблиц, которые хранят информацию, определяющие структуру и организацию соответствующей базы данных.

MSSQL Server *поддерживает два основных класса приложений клиентского типа:*

1. *приложения реляционных баз данных, использующие команды Transact - SQL с расширениями ODBC и набор стандартных функций и объектно-ориентированных методов;*
2. *web - приложения, использующие команды Transact - SQL или запросы наязыке Xpath и документы XML.*

Оба класса приложений используют API интерфейс баз данных типа OLE DB илиODBC.

2.2. Основные принципы управления учетными записями и ролями в MS SQL Server

2.2.1. Список системных процедур и команд, которые позволяют реализоватьполитику разделения прав между пользователями БД.

Название встроеннойпроцедуры	***Описание***
sp_grantlogin	*– позволяет использовать пользователей или группы ОС для соединения с Microsoft SQL Server™, используя* ***Windows Authentication****.* *Этот пример позволяет пользователю Windows NT Corporate\BobJ соединяться с SQL Server. Например,* ***EXEC sp_grantlogin 'Corporate\BobJ'***

sp_defaultdb	*Изменяет для пользователя БД по умолчанию* *Этот пример устанавливает БД по умолчанию pubs для пользователя Victoria. Например,* ***EXEC sp_defaultdb 'Victoria', 'pubs'***
sp_grantdbaccess	*Добавляет учетную запись из раздела security в текущую БД, для учетных записей Microsoft Windows также дает разрешениена доступ к текущей БД.* ***Синтаксис:*** ***EXEC sp_grantdbaccess [@loginame =] 'login' [,[@name_in_db =] 'name_in_db' [OUTPUT]]*** *Этот пример добавляет учетную запись Corporate\GeorgeW втекущую БД и присваивает псевдоним внутри БД Georgie.* *Например,* ***EXEC sp_grantdbaccess 'Corporate\GeorgeW', 'Georgie'***
sp_revokedbaccess	*Удаляет информацию об учетной записи из текущей БД.* ***Синтаксис:*** ***EXEC sp_revokedbaccess [@name_in_db =] 'name'*** *Этот пример удаляет учетную запись Corporate\GeorgeW из текущей БД.* ***EXEC sp_revokedbaccess 'Corporate\GeorgeW'***
sp_addrole	*Создает новую роль в текущей БД.* *Этот пример создает новую роль в текущей БД с названием Managers.* ***EXEC sp_addrole 'Managers'***
sp_addrolemember	*В текущей БД назначает роль конкретному пользователю.* ***Пример A.*** *Этот пример добавляет учетную запись Corporate\JeffL из Windows NT в БД Sales как пользователя Jeff. Jeff затем получает роль Sales_Managers в БД Sales.* ***USE Sales*** *--сделать текущей БД Sales* ***GO*** *–выполнить команду, а потом запустить следующую* ***EXEC sp_grantdbaccess 'Corporate\JeffL', 'Jeff'GO*** ***EXEC sp_addrolemember 'Sales_Managers', 'Jeff'*** ***Пример B.*** *Этот пример добавляет пользователя SQL Server с именем Michael к роли Engineering в текущей БД.* ***EXEC sp_addrolemember 'Engineering', 'Michael'***
sp_helprotect	*Показывает список привилегий, ассоциированных с ролью.*
sp_helprolemember	*Показывает список пользователей БД, входящих в указанную роль*

sp_addsrvrolemember	*Присвоение встроенной серверной роли для существующей учетной записи* ***sp_addsrvrolemember [@loginame =] 'login' , [@rolename =*** ***] 'role'*** *Например:* ***sp_addsrvrolemember 'Admin_DB', 'sysadmin'***
sp_dropsrvrolememb e r	*Удаление встроенной серверной роли для учетной записи или группы* ***sp_dropsrvrolemember [@loginame =] 'login' , [@rolename =*** ***] 'role'*** *Например:* ***sp_dropsrvrolemember 'Admin_DB' , 'sysadmin'***
sp_helpsrvrole	*Описание только встроенных ролей в SQL Server* ***sp_helpsrvrole [[@srvrolename =] 'role']*** *Например:* ***sp_helpsrvrole 'sysadmin'***
sp_helpsrvrolemember	*Возвращает список ролей и учетных записей, которым присвоены эти роли* ***sp_helpsrvrolemember [[@srvrolename =] 'role']*** *Например:* ***sp_helpsrvrolemember 'sysadmin'***
sp_srvrolepermission	*Возвращает список ролей и разрешений, которые присвоены этим ролям* ***sp_srvrolepermission [[@srvrolename =] 'role']*** *Например:* ***sp_srvrolepermission 'sysadmin'***

sp_addlogin ***sp_adduser***	*Создание новой учетной записи в SQL Server в разделе Sequrity:* ***sp_addlogin [@loginame =] 'login'[, [@passwd =] 'password']*** ***[, [@defdb =] 'database']*** ***[, [@deflanguage =] 'language'][, [@sid =] sid]*** ***[, [@encryptopt =] 'encryption_option']*** *Например:* ***sp_addlogin 'login1',sysname, 'DB_Books'*** *Создает пользователя в SQL Server без PUBLIC в БД 'DB_Books'.* *Нужно еще использовать* ***sp_adduser [@loginame =] 'login'[, [@name_in_db =] 'user']*** ***[, [@grpname =] 'group'],*** ***Пример:*** *Создана база данных DB_Books. В ней создан пользователь Admin_DB с серверной ролью sysadmin, с ролью в БД db_owner.* *Создать в QueryAnalyzer нового пользователя с именем Public_ и паролем Public_1 (пароль не должен совпадать с именемпользователя) с помощью следующих команд (не забудьтенажать F5 для запуска команд на выполнение):* ***EXEC sp_addlogin 'Public_','Public_1', 'DB_Books'*** ***use DB_Books*** ***EXEC sp_adduser 'Public_','Public_'*** *В БД DB_Books создан пользователь Public_ с ролью в БДDB_Books public.*
Deny (отрицание)	*Этот пример запрещает несколько системных привилегий длянескольких пользователей.* *Пользователи не могут использовать системные привилегии* ***CREATE DATABASE*** *or* ***CREATE TABLE****, если они ненаделены им через команду* ***GRANT.Пример:*** ***DENY CREATE DATABASE, CREATE TABLE*** ***TO Mary, John, [Corporate\BobJ]*** ***DENY SELECT, INSERT, UPDATE, DELETE ON authors TO*** ***Mary, John, Tom***

Grant (предоставлять)	*This example grants multiple statement permissions to the users Mary and John, and the Corporate\BobJ Windows NT group.* ***GRANT CREATE DATABASE, CREATE TABLE TO Mary, John, [Corporate\BobJ]*** *Назначение разрешения на выборку (SELECT) для роли PUBLIC в таблице Authors:* ***GRANT SELECT ON Authors TO public***
Revoke (отменять)	*This example revokes multiple statement permissions from multipleusers.* ***REVOKE CREATE TABLE, CREATE DEFAULT FROM Mary, John*** *This example removes the denied permission from Mary and, through the SELECT permissions applied to the Budget role, allowsMary to use the SELECT statement on the table.* ***REVOKE SELECT ON Budget_Data TO Mary***

2.2.2. Создание пользователей для доступа к серверу через утилиту Microsoft SQL Server Management Studio

Создадим новую учетную запись *для нашей базы данных* **University**. *Для этого выберите в Обозревателе объектов раздел* ***Безопасность/Имена входа***. *Добавьте новое* ***имя входа – Proba****, установите опцию* ***Проверка подлинности SQL Server****, присвойте свой пароль, примените к выбранной базе данных, установите язык по умолчанию – русский.*

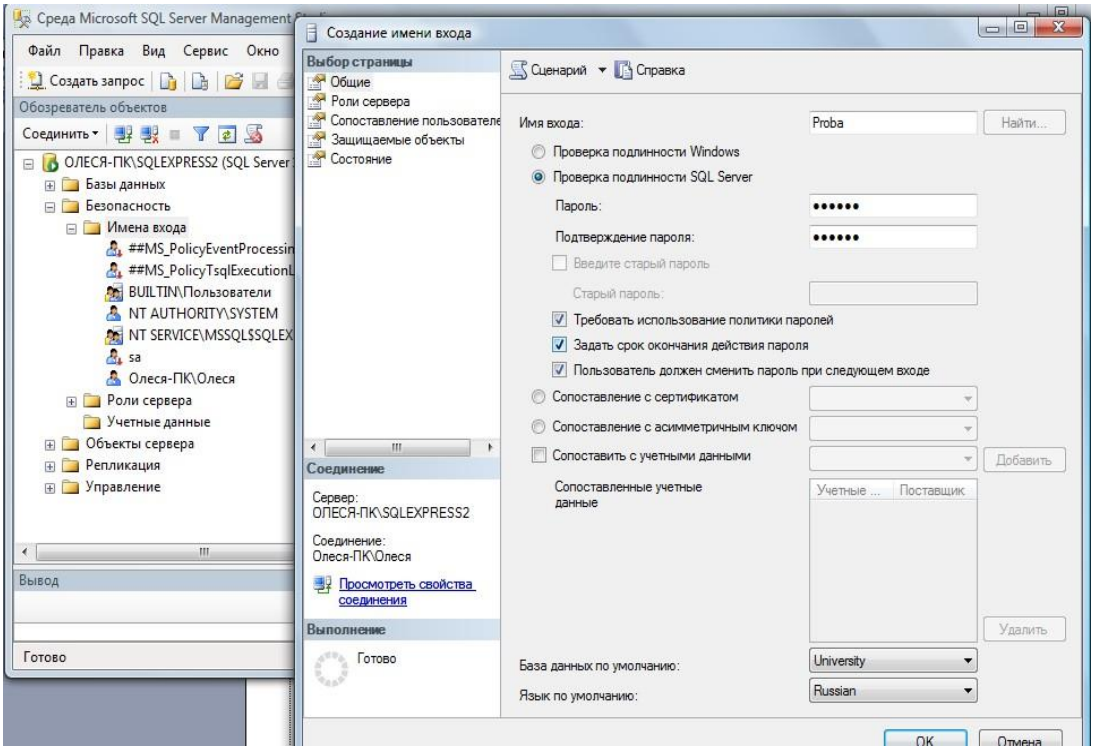


Рис. 2.1. Раздел Безопасность (Security) для работы с пользователями и создание нового пользователя (при SQL Server аутентификации нужно снять галочки с ***Enforce passwordpolicy****)*

Прежде чем добавлять нового пользователя просмотрите его назначенные серверные роли. Для этого в этом же окне выберите раздел ***Роли сервера****. Установите для пользователя* ***Proba*** *роль* ***sysadmin****.*

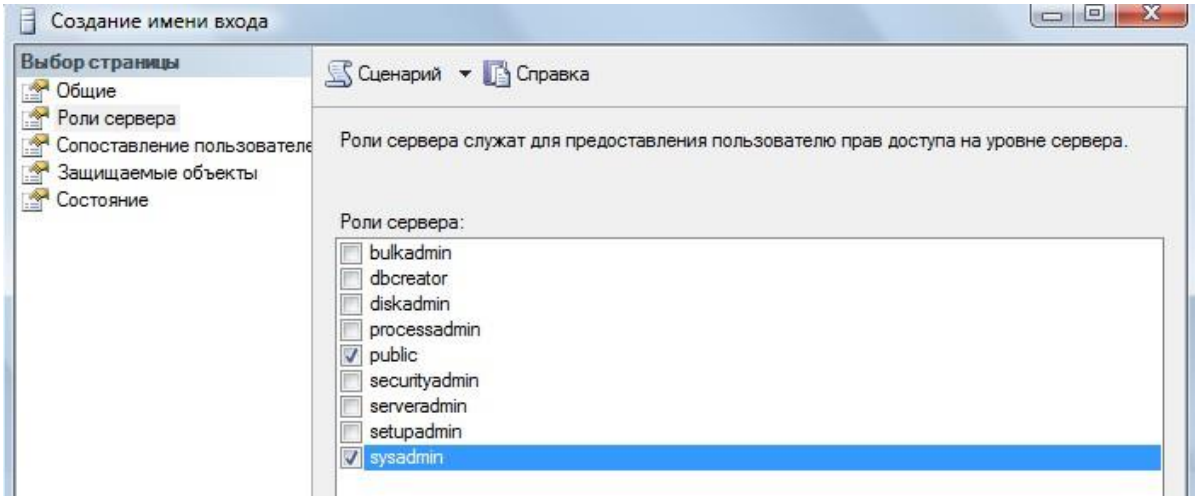


Рис. 2.2. Настройка серверной роли для нового пользователя (весь список серверныхролей с их привилегиями в конце работы)

Далее просмотрите раздел ***Сопоставление пользователя****. Установите для базы данных* ***University*** *у пользователя* ***Proba*** *права доступа* ***Db_owner****, означающие, что пользователь может выполнять* ***любые действия с БД****. Ниже перечислены все возможные варианты прав доступа.*

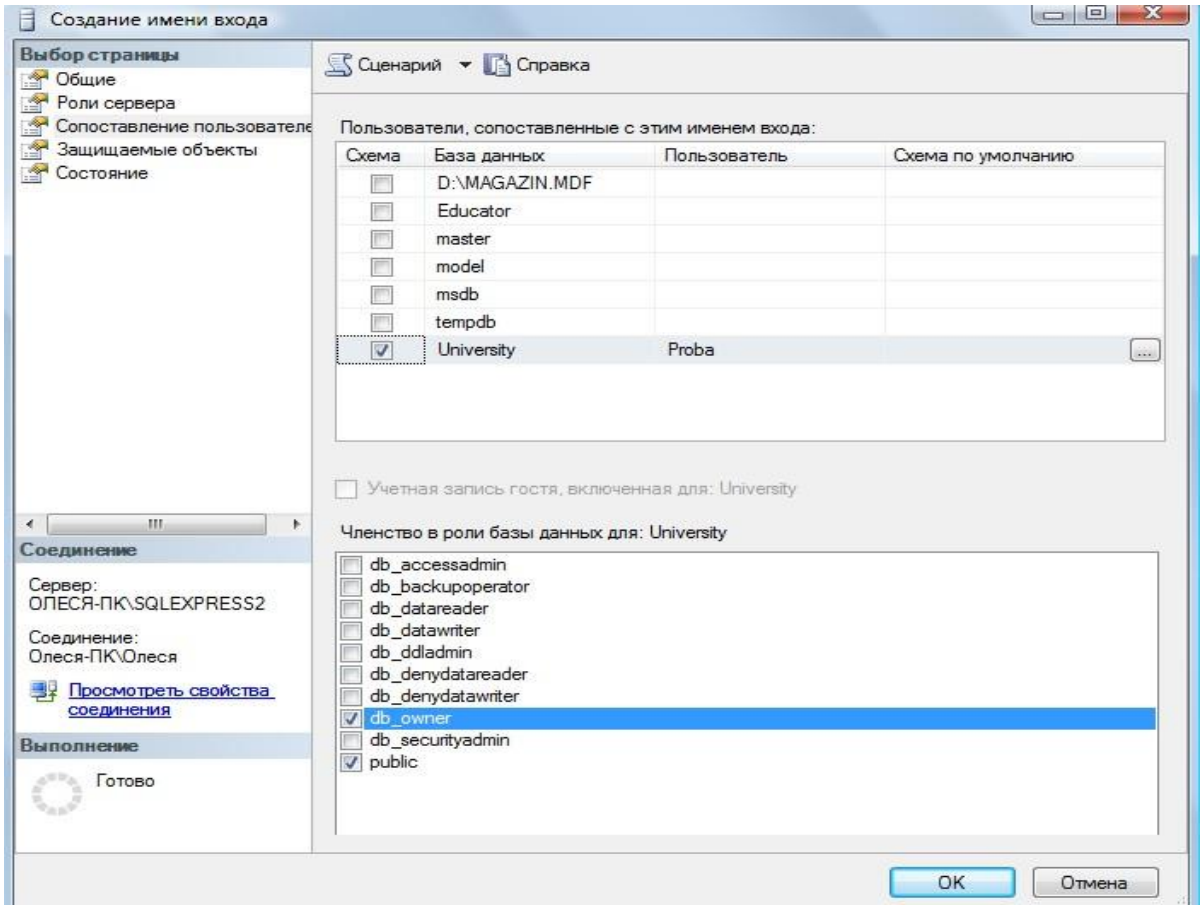


Рис. 2.3. Настройка роли базы данных для нового пользователя (весь список ролей базданных с их привилегиями ниже)

Перечень ролей БД:

Public *– минимальные права доступа к БД (на просмотр)* ***Db_owner*** *– может выполнять любые действия с БД* ***Db_accessadmin*** *– добавляет и удаляет пользователей БД*

Db_sequrityadmin *– управляет ролями в БД и разрешениями на запуск команд и работу с объектами БД*

Db_ddladmin *– добавляет, изменяет и удаляет объекты БД* ***Db_backupoperator*** *– осуществляет резервное копирования БД* ***Db_dataSTUDENT*** *– может просматривать все данные в каждой таблице в БД*

Db_datawriter *- может добавлять, удалять и изменять данные в каждой таблице в БД*

Db_denydataSTUDENT *– запрет на просмотр всех данных в каждой таблице в БД*

Db_denydatawriter *- запрет на добавление, удаление и изменение всех данных в каждой таблице в БД*

Далее перейдите на раздел ***Состояние****. Установите опции* ***Разрешение к подключению к ядру СУБД*** *– предоставить и* ***имя входа*** *включить.*

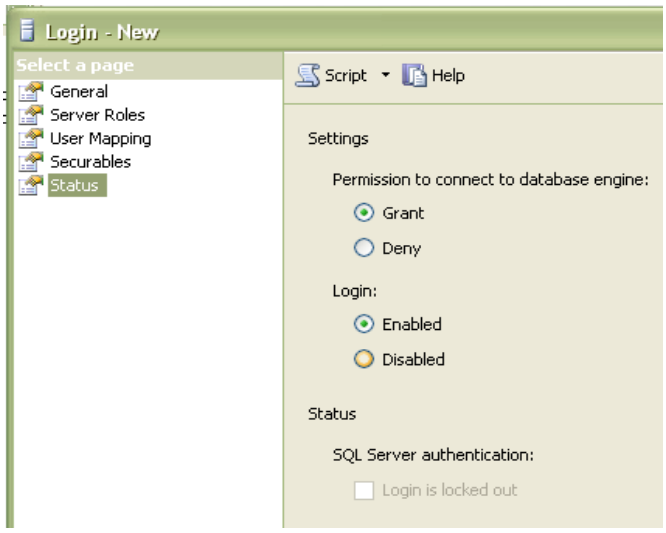


Рис. 4.4. Разблокирование создаваемой учетной записи

После нажатия на <OK> в БД появится пользователь ***Proba*** *с правамисобственника БД, который может выполнять все манипуляции с БД* ***University****.*

Откройте в окне обозревателя объектов БД **University** *и перейдите на вкладку* ***Безопасность****, там вы найдите только что созданного пользователя.*

2.2.3. Создание ролей программно

Для упрощения управления правами доступа в системе создаются ***роли****, которые затем можно назначать* ***группе пользователей****.*

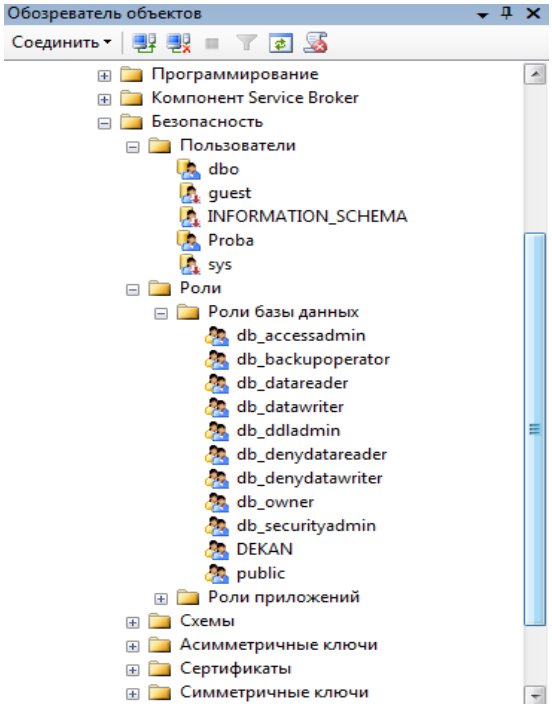
Создадим для нашего примера роли декана ***(DEKAN)*** *и студента* ***(STUDENT)****.*

Пример *создания роли декана:*

USE University --сделать текущей БД UniversityEXEC sp_addrole 'DEKAN'

*Эти операторы набрать на странице, вызванной нажатием кнопки <****Создатьзапрос****>.*

Для запуска команд на выполнение нажать Выполнить *.Сохраните запрос.*



Повторный запуск тех же команд сгенерирует ошибки типа ***«В БД ужесуществует роль DEKAN»****.*

Чтобы просмотреть, что роль добавлена, откройте вкладку ***Безопасность/Роли/Роли базы данных****.*

Пример *создания роли студента:*

USE University --сделать текущей БД universityEXEC sp_addrole 'STUDENT'

Декан** должен обладать правами на **чтение, удаление, изменение, добавление во все таблицы БД University**, а также должен иметь возможность запускать на исполнение процедуры и функции БД University. Поэтому роли декана из системных привилегий назначаем **EXECUTE**, а из привилегий доступа к объектам назначаем **DELETE, INSERT, UPDATE, SELECT.

***Студент** должен обладать правами **на чтение из таблиц**. Поэтому роли читателя из привилегий доступа к объектам назначаем **SELECT**.*

Оператор представления привилегий

Синтаксис:

GRANT <привилегия>, ...ON < объект >, …

TO <имя>

[WITH grant option];

*Атрибут **WITH GRANT OPTION** дает право пользователю самому раздавать права, которые он получил.*

*С помощью оператора **GRANT** для каждого пользователя формируется список привилегий, привилегии управляют работой сервера данных с точки зрения защиты данных. Выполнению каждой транзакции предшествует проверка привилегий пользователя, сеанс которого породил транзакцию.*

Например (не выполнять):

GRANT select, update (Sales, num) ON Sales_data TO user1WITH GRANT OPTION

*Пользователь, предоставивший привилегию другому, называется **грантор** (grantor — предоставитель). Привилегия является предоставляемой, если право на нее можно предоставить другим пользователям.*

***PUBLIC** — имя роли, которую получает пользователь при добавлении в список пользователей конкретной БД, включает в себя минимальный набор прав на чтение данных из таблиц и представлений в БД.*

*Для примера (немного забегая вперед) создадим таблицу **Discuplinu**. Без объяснения синтаксиса выполните следующий sql-запрос:*

USE University --сделать текущей БД universitycreate table Discuplinu (

Kod_Discuplinu int NOT NULL primary key,name_Discuplinu nchar(30) NULL, kol_chasov int NULL

);

Выполните код и обновите вкладку ***Таблицы****. Вы должны увидеть созданную таблицу для сохранения данных о всех дисциплинах. Эта таблица пока пустая с тремя столбцами* ***Kod_Discuplinu, name_Discuplinu, kol_chasov.***

Роль декана названа ***DEKAN****. Операторы назначения прав доступа для этой роли представлены ниже:*

GRANT DELETE, INSERT, UPDATE, SELECT ON Discuplinu TO DEKAN
GRANT EXECUTE TO DEKAN

Роль студента названа STUDENT. Операторы назначения прав доступа для этой роли представлены ниже:

GRANT SELECT ON Discuplinu TO STUDENT

Примените роли декана и студента к созданной таблице.

Создание пользователей с определенной ролью*Пример создания декана* ***Ivanov_Dek и присвоения ему роли:***

EXEC sp_addlogin 'Ivanov_Dek','Ivanov', 'University'use University

EXEC sp_adduser 'Ivanov_Dek','Ivanov_Dek' EXEC sp_addrolemember 'DEKAN', 'Ivanov_Dek'

Пример создания студент Petrov_Stud и присвоения роли:

EXEC sp_addlogin 'Petrov_Stud','Petrov', 'University'

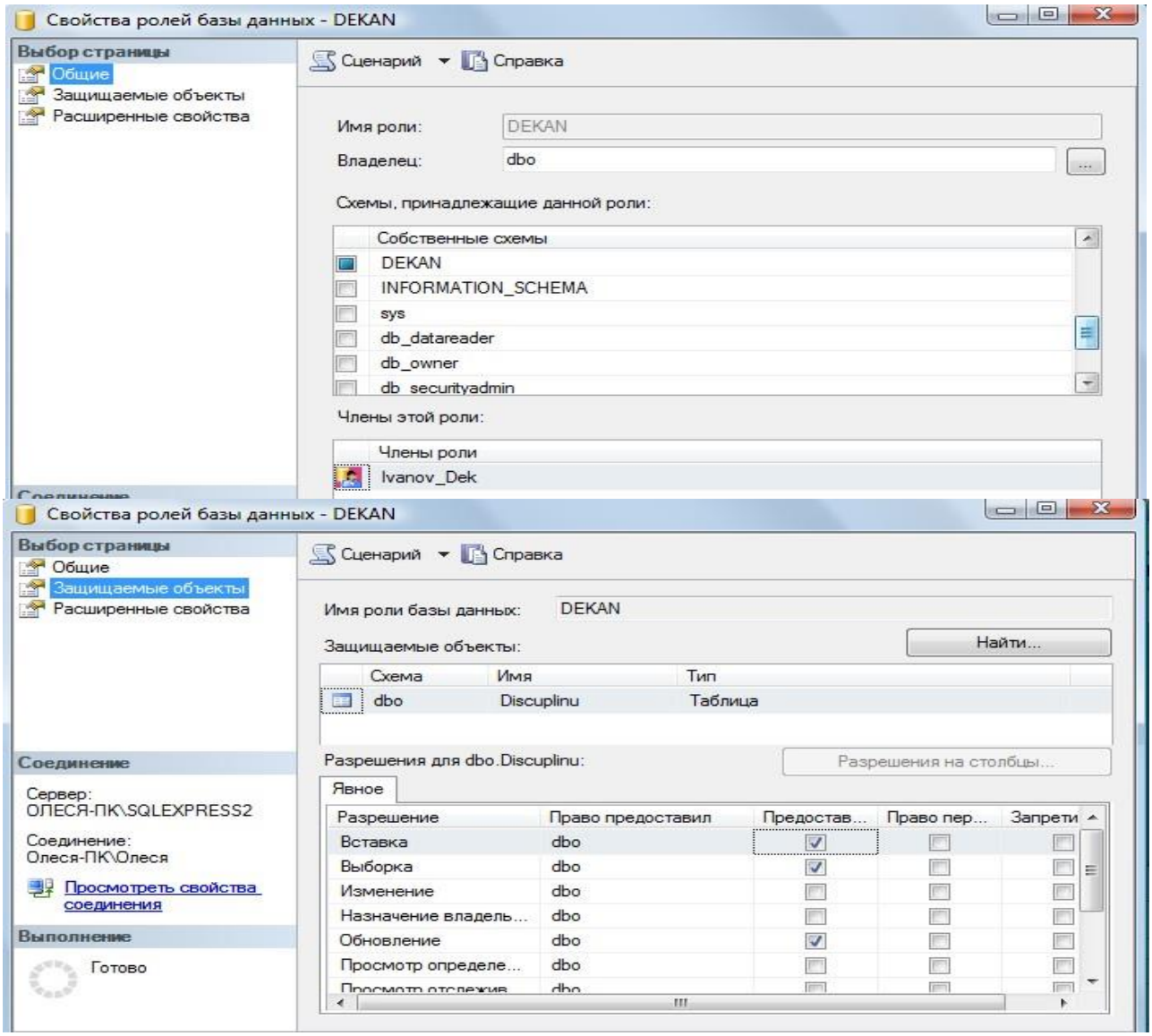
use University

EXEC sp_adduser 'Petrov_Stud','Petrov_Stud'

EXEC sp_addrolemember 'STUDENT', 'Petrov_Stud'

Выполните команды. Перейдите в окне Обозреватель объектов на ***Роли/Роли базы данных/Dekan*** *и просмотрите его свойства. Просмотрите назначенные общие свойства, защищаемые объекты и расширенные свойства.*

Самостоятельно *просмотрите свойства роли базы данных* ***Student.***
Просмотритеназначенные общие свойства, защищаемые объекты и расширенные свойства.



Оператор отмены привилегий

Синтаксис отмены привилегий:

REVOKE [with grant option]

< привилегии >,…ON < объект >,…

FROM <имя_пользователя>;

Предложение **with grant option** *сохраняет за пользователем перечисленные привилегии, но отменяет его право передавать их кому-либо другому.*

Пример:

REVOKE SELECT ON Discuplinu FROM STUDENT

Выполните команду.

Оператор изымания роли у пользователя

Revoke <список ролей> from <список пользователей>.

Пример:

use University

EXEC sp_droprolemember 'STUDENT', 'Petrov_Stud'

Выполните команду и просмотрите результат.