Приложение № 4 к ОПОП

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

Комплекс контрольно-оценочных средств

профессионального модуля

ПМ.07 СОАДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ И СЕРВЕРОВ

по специальности

09.02.07 Информационные системы и программирование базовой подготовки

2024 г.

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности СПО 09.02.07 «Информационные системы и программирование» базовой подготовки программы учебной дисциплины ПМ.07 Соадминистрирование баз данных и серверов.

Разработчик:

ГБПОУ «ККАТУ»	преподаватель	А.В. Атушкина
(место работы)	(занимаемая должность)	(инициалы, фамилия)

1. ПАСПОРТ КОМПЛЕКСА КОНТРОЛЬНО – ОЦЕНОЧНЫХ СРЕДСТВ

В результате освоения профессионального модуля ПМ.07 Соадминистрирование баз данных и серверов обучающийся должен обладать предусмотренными ФГОС по специальности 09.02.07 Информационные системы и программирование следующими умениями, знаниями, которые формируют общие и профессиональные компетенции. ПМ.07 состоит из междисциплинарных курсов:

МДК 07.01. Управление и автоматизация баз данных, МДК 07.02 Сертификация информационных
систем.

Формой аттестации МДК07.01 и МДК 07.02 является *экзамен*. В соответствии с требованиями ФГОС и рабочей программы для проведения текущего контроля успеваемости и промежуточной аттестации по междисциплинарным курсам МДК 07.01. Управление и автоматизация баз данных, МДК 07.02 Сертификация информационных систем разработан комплекс контрольно-оценочных средств (далее - КОС), являющийся частью учебно-методического комплекса настоящей дисциплины.

Комплекс контрольно-оценочных средств (КОС) включает:

1. Паспорт КОС;
2. КОС текущего контроля:
   - Типовые тестовые задания;
   - Типовые задания для контроля умений при проведении практических работ;

3. КОС промежуточной аттестации включает
   - типовые задания для проведения теоретической и практической частей экзамена;В КОС

по ПМ 07 представлены оценочные средства сформированности ОК и ПК.

Формы контроля и оценивания элементов профессионального модуля

Элемент модуля	**Форма контроля и оценивания**	
	Промежуточная аттестация	**Текущий контроль**
МДК.07.01	Экзамен (4 курс, 7 семестр),	*Контроль знаний в форме фронтального, индивидуального и тестового опросов по темам.* *Защита практических работ по темам*
МДК.07.02	Экзамен (4 курс, 7 семестр)	*Контроль знаний в форме фронтального, индивидуального и тестового опросов по темам.* *Защита практических работ по темам*
УП	Дифференцированный зачет (4 курс, 8 семестр)	*Наблюдение и экспертная оценка выполнения работ в ходе учебной практики.* *Оценка результатов учебной практики в форме отчета.*
ПП	Дифференцированный зачет (4 курс, 8 семестр)	*Наблюдение и экспертная оценка выполнения работ в ходе производственной практики.* *Оценка результатов производственной практики в форме отчета.*

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

2.1 Профессиональные и общие компетенции

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка профессиональных и общих компетенций, представленных в таблице 1.

Таблица 1 - Общие и профессиональные компетенции, подвергаемые проверке

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля результатов обучения**	**Оценка результатов обучения**
ПК 7.1	Выявляет технические проблемы, возникающие в процессе эксплуатации баз данных и серверов	Экзамен/зачет в форме собеседования: практическое задание по изменению содержания таблиц базы данных и выполнению запросов к базе данных. По изменению структуры базы данных Защита отчетов по практическим и лабораторным работам Экспертное наблюдение за выполнением	Оценка «**отлично**» - проанализирована структура БД и сделан вывод о поддержании целостности БД; внесены указанные изменения в БД и проконтролировано сохранение этих изменений; созданы указанные запросы к БД. Выполнены запросы на указанное изменение структуры БД и проверена их корректность Оценка «**хорошо**» - проанализирована структура БД; внесены указанные изменения в БД и проконтролировано сохранение этих изменений; созданы указанные запросы к БД. Выполнены запросы на указанное изменение структуры БД и проверена их корректность Оценка «**удовлетворительно**» - проанализирована структура БД; внесены указанные изменения в БД; созданы указанные запросы к БД. Выполнены запросы на указанное изменение структуры БД
ПК 7.2	Осуществляет администрирование отдельных компонент серверов		Оценка «**отлично**» - предложенные функции администратора выполнены в полном объеме с пояснениями, демонстрирующими знание технологий. Оценка «**хорошо**» - предложенные функции администратора выполнены в достаточном объеме с некоторыми пояснениями, демонстрирующими знание технологий Оценка «**удовлетворительно**» - предложенные функции администратора выполнены в удовлетворительном объеме с некоторыми пояснениями

ПК 7.3	Формирует требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов	различных видов работ во время учебной/ производственной практики	Оценка «**отлично**» - проанализированы условия эксплуатации, требуемый уровень безопасности и необходимые возможности аппаратных средств для реализации поставленной задачи; сформированы требования к конфигурации компьютерных сетей и серверного оборудования для реализации, поставленной задачи в нескольких вариантах. Оценка «**хорошо**» - проанализированы условия эксплуатации, требуемый уровень безопасности, указано возможное оборудование; сформированы требования к конфигурации компьютерных сетей и серверного оборудования для реализации поставленной задачи. Оценка «**удовлетворительно**» - проанализированы условия эксплуатации; сформированы типовые требования к конфигурации компьютерных сетей и серверного оборудования для реализации поставленной задачи.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля результатов обучения**	**Оценка результатов обучения**
ОК 07	Планирует информационный поиск из широкого набора источников, необходимого для выполнения профессиональных задач; Проводит анализ полученной информации, выделяет в ней главные аспекты; структурирует отобранную информацию в соответствии параметрами поиска. Интерпретирует полученную информацию в контексте профессиональной деятельности.	- эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности.	Экспертное наблюдение за выполнением работ

Результаты	Основные показатели оценки результата	Формы и методы контроля результатов обучения	Оценка результатов обучения
ТФ А/01.4	Собирает данные для выявления требований к типовой ИС в соответствии с	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: -на практических занятиях; - при выполнении работ на различных этапах учебной практики;	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.
ТФ А/09.4	Устанавливает и настраивает системное и прикладное ПО, необходимое для функционирования ИС в соответствии с трудовым заданием		

3. ОЦЕНКА ОСВОЕНИЯ КУРСА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Формы и методы оценивания образовательных достижений студентов при текущем контроле и промежуточной аттестации

Предметом оценки служат умения и знания, предусмотренные ФГОС по МДК.07.01 и МДК 07.02, направленные на формирование общих и профессиональных компетенций.

Занятия представлены следующими видами работы: лекции, практические занятия. На всех видах занятий предусматривается проведение текущего контроля в различных формах. Промежуточная аттестация студентов по МДК проводится в соответствии с локальными актами и является обязательной.

Текущий контроль по МДК осуществляется преподавателем и проводится в форме контрольных мероприятий по оцениванию фактических результатов обучения студентов: защиты выполненных практических работ, решения задач, выполнения и защиты рефератов, домашних заданий, оценки устных ответов студентов.

Объектами оценивания выступают:

- общие и профессиональные компетенции (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по дисциплине);
- степень усвоения теоретических знаний;
- уровень овладения практическими умениями и навыками по всем видам учебной работы;
- результаты самостоятельной работы.

Промежуточная аттестация студентов по МДК 07.01 и МДК 07.02 проводится в соответствии с локальными актами. Промежуточная аттестация студентов является обязательной.

Промежуточная аттестация в форме экзамена проводится, в соответствии с рабочими учебными планами специальности.

Экзамен по МДК 07.01. Управление и автоматизация баз данных проводится в 2 этапа – тестирование и практическое задание.

Экзамен по МДК.07.02 Сертификация информационных систем проводится в виде тестирования.

В каждом экзаменационном задании содержатся задания, позволяющие осуществить контроль усвоения знаний и умений, приобретенных в процессе изучения МДК.

Контроль знаний и умений осуществляется в соответствии с требованиями ФГОС специальности и рабочей программы профессионального модуля.

4. ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МДК 07.01. УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ БАЗ ДАННЫХ И МДК.07.02 СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

4.1 Типовые задания для проведения промежуточной аттестации

Контрольно-измерительные материалы (КИМ) охватывает наиболее актуальные разделы и темы программы и содержат экзаменационные задания. Экзаменационные материалы целостно отражают объем проверяемых теоретических знаний и практических умений.

Экзамен по МДК 07.01. Управление и автоматизация баз данных состоит из 2 частей – тест и практическое задание.

Экзамен по МДК.07.02 Сертификация информационных систем проводится в форме тестирования.

Типовые задания для проведения промежуточной аттестации:

Пример экзаменационного теста:

Структура теста

1. Какая системная БД, используется SQL Server при восстановлении данных?

a) tempbd

b) model

c) msdb

d) pubs

2. Для получения списка файлов данных и журналов транзакций, входящих в набор резервных копий, используется следующий оператор Transact-SQL

a) RESTORE FILELISTONLY FROM

b) RESTORE HEADONLY FROM

c) RESTORE LABELONLY FROM

d) RESTORE DATA FROM

3. Возможно ли восстановление данных БД на другом сервере?

a) возможно, если предварительно создать экземпляр БД

b) возможно, если только сервер имеет такое же имя, что и исходный

c) невозможно, данные могут быть перенесены только путем импорта данных

d) невозможно, данные могут быть только реплицированы

4. При использовании проверки аутентификации SQL Server, информацию о логине пользователе и его пароле хранится в системной таблице БД master:

a) sysusers

b) sysmembers

c) sysxlogins d) хранится отдельно

5. Участник роли Serveradmin имеет следующие права на уровне экземпляра SQL Server:

a) может выполнять любую задачу в любой БД SQL Server.

b) устанавливать и изменять параметры конфигурации удаленных и связанных сервисов и параметры репликации.

c) конфигурировать SQL Server с помощью системной хранимой процедуры sp_configure и перезапускать службы SQL Server

d) выполнять все операции, связанные с защитой, контроль над учетными записями сервера и чтение журнала ошибок SQL Server

6. Участник роли ddladmin имеет следующие права на уровне базы данных:

a) может добавлять в БД и удалять из нее пользователей

b) может добавлять, изменять и удалять объекты

c) может управлять разрешениями, ролями, записями участников ролей

d) может выполнять команды DBCC, инициировать процессы фиксации транзакций, создавать резервные копии

7. Участник роли Db_securityadmin имеет следующие права на уровне базы данных:

a) может добавлять в БД и удалять из нее пользователей

b) может добавлять, изменять и удалять объекты

c) может управлять разрешениями, ролями, записями участников ролей

d) может выполнять команды DBCC, инициировать процессы фиксации транзакций, создавать резервные копии

8. Участник роли Sysadmin на уровне экземпляра SQL Server при создании новой БД автоматически становится участником следующей роли на уровне БД:

a) Db_accessadmin

b) Db_securityadmin

c) Db_owner

d) Db_ddladmin

9. Для управления учетными записями в Enterprise Manager используется контей-

нер:

a) Security
b) Users
c) Managment
d) Support Services

10. Для создания новой учетной записи можно воспользоваться следующей храниой процедурой:

a) Sp_addlogin
b) Sp_adduser
c) Sp_revokelogin
d) Sp_createuser

11. Для просмотра информации об участниках заданной роли можно воспользоваться следующей системной процедурой:

a) Sp_helpuser
b) Sp_helpntgroup
c) Sp_helprolemember
d) Sp_helplogins

12. Для задания разрешения на создание объектов БД можно воспользоваться следующим оператором Tranact-SQL:

a) REVOKE
b) DENY
c) GRANT
d) ALLOW

13. Для просмотра информации о разрешениях, заданных для объекта используется следующая системная процедура:

a) Sp_helprotect
b) Sp_helpgrant
c) Sp_viewproperties
d) Sp_permission

14. При автоматизации задач администрирования SQL Server оператор (operator) является пользователем, который имеет права:

a) может создавать новые задания
b) может получать оповещения о выполняемых операциях
c) может управлять разрешениями на выполнение заданий
d) может создавать и редактировать оповещения

15. SQL Server позволяет организовать рассылку сообщений с помощью:

a) электронной почты, сообщений по локальной сети, программ-пейджеров
b) только электронной почты
c) электронной почты и записи в журнал событий компьютера администратора
d) электронной почты, записи в журнал событий, программы пейджера

16 Документ, созданный в субд access, имеет расширение

а) *.doc б) *.exe в) *.com г) *.mdb, *.accdb

17 Основной объект БД, где хранятся данные

а) Мои документы б) Таблицы в) Корзина г) Мой компьютер

18 Поле, которое является очевидным кандидатом для создания связей между таблицами

а) Связующее б) Табличное в) Логическое г) Ключевое

19 База данных, имеющая связанные двумерные таблицы называется

а) реляционная б) иерархическая в) интегрированная г) сетевая

20 Связи между таблицами в СУБД отображаются в …

а) окне базы данных
б) окне “Схема данных”
в) окне Microsoft Access
г) режиме конструктора таблиц

21 Большинство БД имеют структуру:
а) Плоскую б) Табличную в) Базовую г) Иерархическую
22 Объект СУБД, предназначенный для подготовки и отправки данных на печать
а) Принтер б)Формы в) Отчеты г)Таблицы

Примеры практических заданий:

Восстановите базу данных из скрипта.
Для восстановления таблиц в созданную базы данных воспользуйтесь предоставленным скриптом.

Заказчик системы предоставил файлы с данными (с пометкой import в ресурсах) для переноса в новую систему. Подготовьте данные файлов для импорта и загрузите в разработанную базу данных.

4.2. Защита практического задания

4.2.1. Проверяемые результаты обучения:
Проверяемые результаты обучения: ПК 7.1, 7.2, ПК 7.3, ОК 07.

4.2.2. Критерии оценки:
Критерии оценки профессиональных и общих компетенций при защите практического задания

Оценка экзамена	Требования к знаниям	Требования к умениям	Требования к освоению ОК и ПК
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий Было верно выполнено 90-100 % теста	Правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения заданий, применяет знания в комплексе, проводит анализ полученных результатов	Реализует творческий подход и инициативу в овладении профессией. Демонстрирует высокий уровень анализа информации, проявляет инициативу. Студент демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос Было верно выполнено 80-89 % теста	Правильно применяет теоретические положения при решении задач, владеет необходимыми навыками и приемами их выполнения, испытывает незначительные затруднения при анализе полученных результатов	Ответственен и активен в изучении профессии. Самостоятельно анализирует и оценивает информацию. Студент демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4

«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания толькоосновного материала, но неусвоил его деталей, допускает неточности, недостаточно правильные формулировки, Нарушения логической последовательности в изложении программного материала Было верно выполнено 7 0 - 7 9 % теста	Испытывает затруднения при решении задач, слабо аргументирует принятые решения, не в полной мере интерпретирует полученные результаты	Имеет общее представление о сущности профессии, малоинициативен. Требуется помощьпреподавателя при анализе и оценке информации. Студент демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий поМДК. Было верно выполнено менее 7 0 % теста	Неуверенно, с большими затруднениями решает задачи, неправильно использует необходимые формулы, не может сформулировать выводов по результатам решения задачи	Имеет низкое представление о сущности профессии, малоинициативен. Требуется помощь преподавателя при анализе и оценке информации. Студент не демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4

4. 3 Система оценки решения задач, ответов на вопросы, выполнения заданий

При выполнении 70% и более содержания заданий задание считается выполненным, при этом в ведомость (оценочный/аттестационный лист) выставляется положительная оценка (1).

В случае менее 70% правильных ответов контрольное задание считается не выполненным, при этом в ведомость (оценочный/аттестационный лист) выставляется отрицательная оценка (0).

4.4. Организация проведения промежуточной аттестации

4.1.1 Условия проведения экзамена. Подготовка к проведению экзамена

Экзамен проводится в период экзаменационной сессии, установленной календарным графиком учебного процесса рабочего учебного плана. С формами проведения промежуточной аттестации обучающиеся знакомятся в течение двух месяцев с начала обучения.

Количество вопросов и практических задач в перечне для подготовки к промежуточной аттестации превышает количество вопросов и практических задач, необходимых для составления контрольно-измерительных материалов.

На основе разработанного и объявленного обучающимся перечня вопросов и практических задач, рекомендуемых для подготовки к экзамену, составлены задания, содержание которых до обучающихся не доводится. Вопросы и практические задачи носят равноценный характер. Формулировки вопросов билетов четкие, краткие, понятные, исключают двойное толкование.

4.1.2 Проведение экзамена

Студенты для сдачи экзамена распределяются по времени. На выполнение экзаменационного задания студенту отводится не более одного академического часа.

Оценка, полученная на экзамене, заносится преподавателем в зачетную книжку студента (кроме неудовлетворительной) и экзаменационную ведомость (в том числе и неудовлетворительные).

5.2. ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ПО МДК. 07.01 УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ БАЗ ДАННЫХ И МДК.07.02 СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Текущий контроль осуществляется после изучения раздела/темы в ходе освоения МДК.
Формами текущего контроля могут быть:

- тестирование;
- опрос;
- разноуровневые задачи и задания.

Например:

Тестовые задания.

Инструкция: *Внимательно прочитайте вопросы в тесте. В зависимости от постановки вопроса дать правильный ответ.*

Критерии оценки: *«5» - 37-30 баллов*
«4» - 29-25 баллов
«3» - 24-20 баллов
«2» - менее 20 баллов

1. ***Выберите один правильный вариант ответа***

База данных - это:

A. Специальным образом организованная и хранящаяся на внешнем носителе совокупность взаимосвязанных данных о некотором объекте;
B. Произвольный набор информации;
C. Совокупность программ для хранения и обработки больших массивов информации;
D. Интерфейс, поддерживающий наполнение и манипулирование данными;
E. Компьютерная программа, позволяющая в некоторой предметной области делать выводы, сопоставимые с выводами человека-эксперта.

2. *Выберите один правильный вариант ответа*
Перечислите преимущества централизованного подхода к хранению и управлению данными.

A. Возможность общего доступа к данным
B. Поддержка целостности данных
C. Соглашение избыточности
D. Сокращение противоречивости

3. *…*

Ключ: 1- A, 2 – B…

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 пользователя длиной 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.)

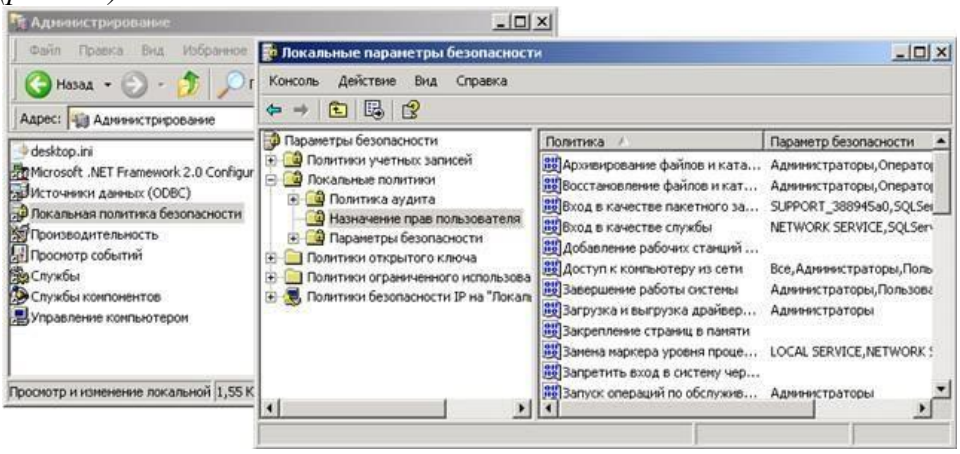


Рисунок 1.1 - Окно Локальные параметры безопасности

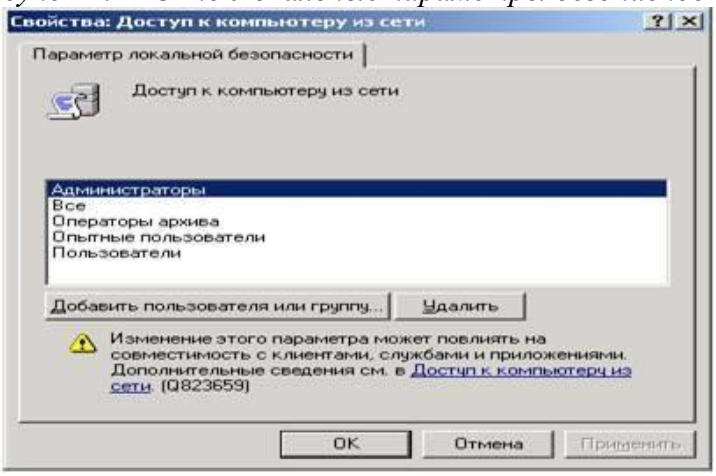


Рисунок 1.2 - Окно Параметр локальной безопасности

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 и клавиши 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.*

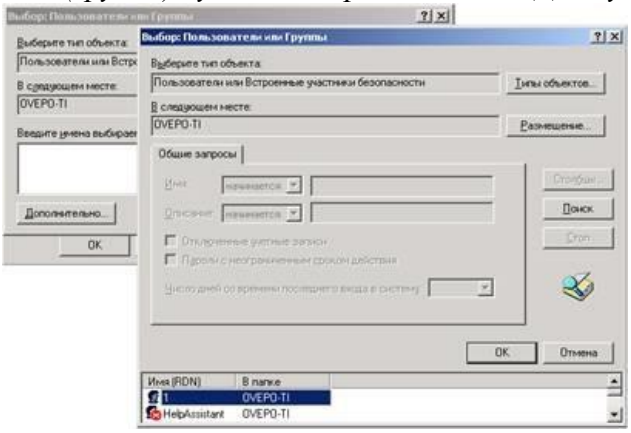


Рисунок 1.3 - Добавление пользователей или групп

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.).*

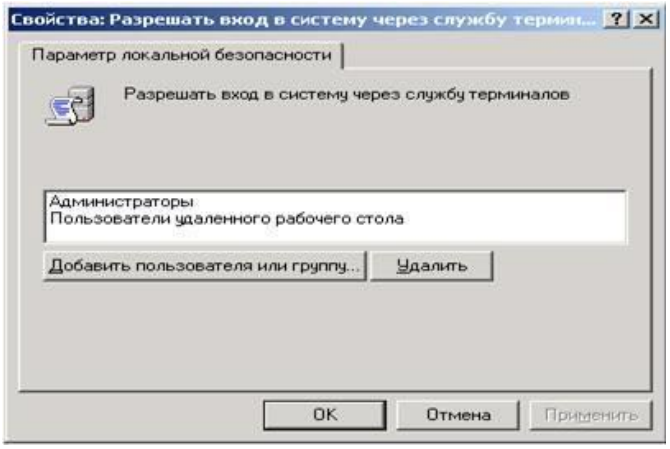


Рисунок 1.4 - Окно Разрешить вход в систему через службу терминалов

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.).*

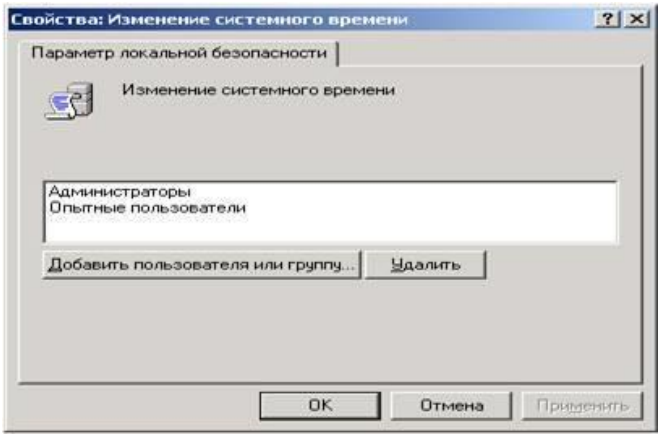


Рисунок 1.5 - Окно Изменение системного времени

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.).*

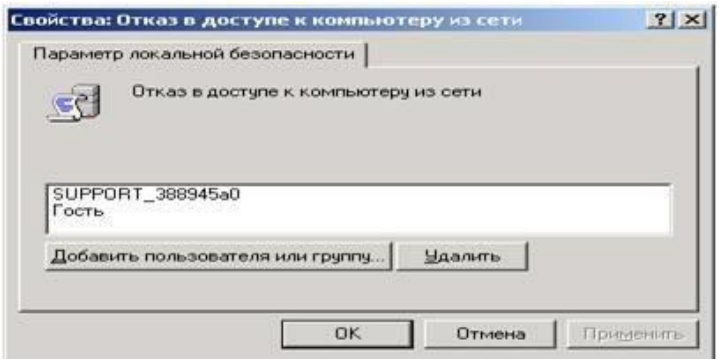


Рисунок 1.6 - Окно Отказ в доступе к компьютеру из сети

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.).*

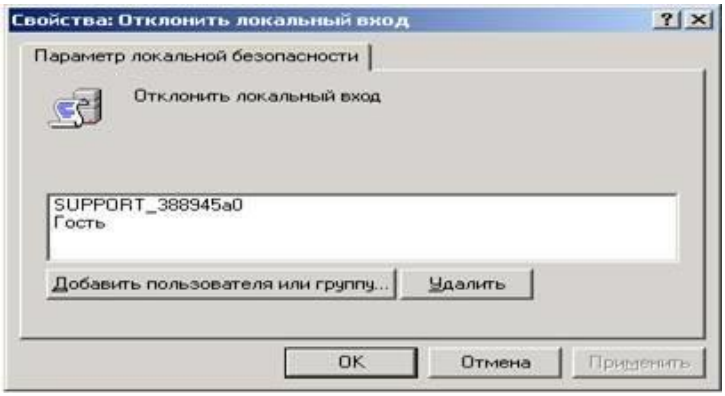


Рисунок 1.7 - Окно Отлонить локальный вход

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.).*

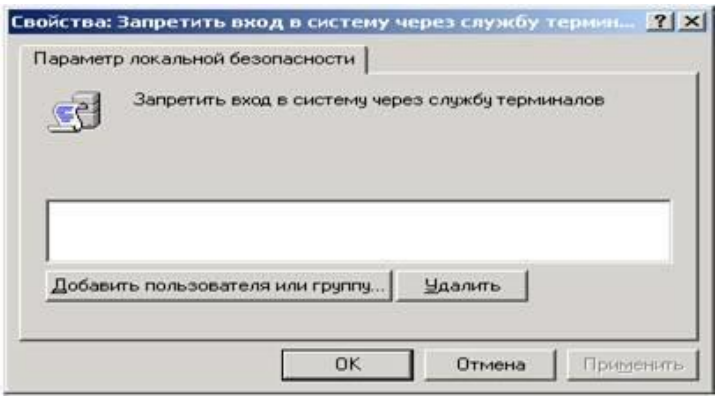
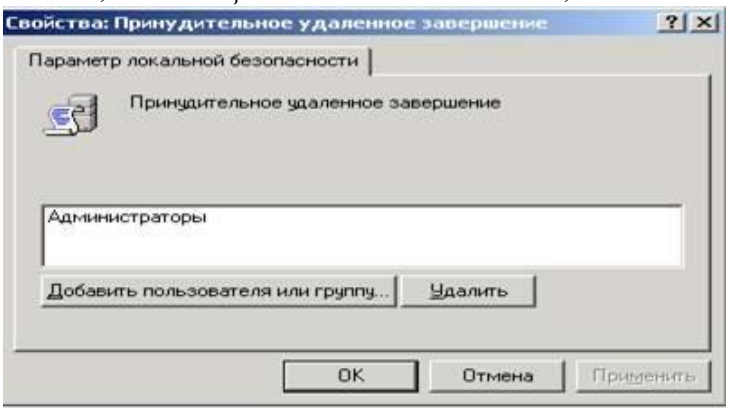


Рисунок 1.8 - Окно Запретить вход в систему через службу терминалов

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 пользователей может 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.)

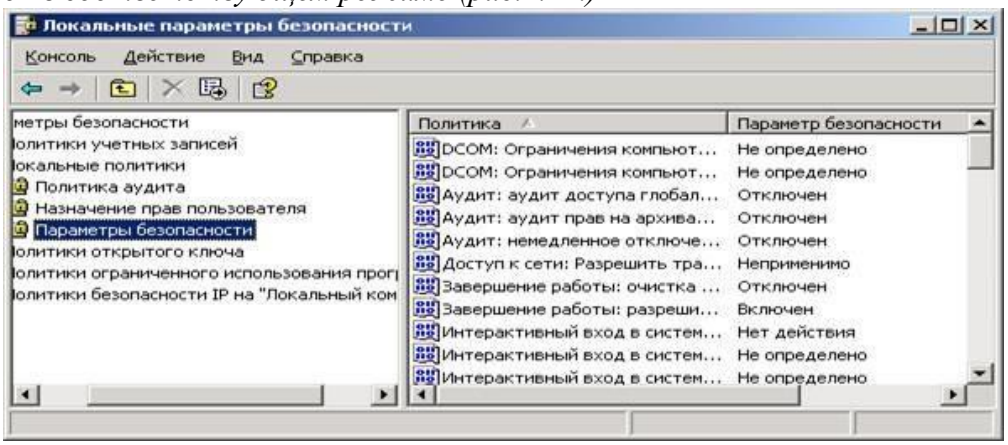


Рисунок 1.10 - Окно Параметры безопасности

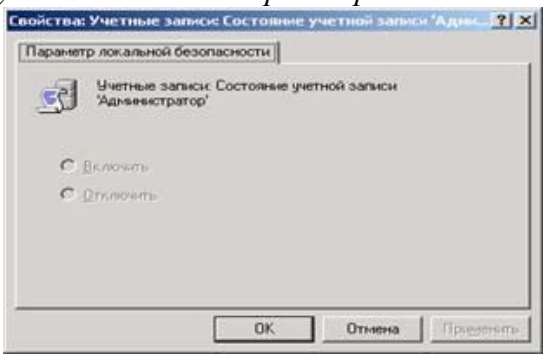


Рисунок 1.11 - Окно Состояние учетной записи 'Администратор'

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 невыдается;

- 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 управлениях 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 через службу 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 локальной сети?*
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 ресурсам предоставляет шифрующая файловая система?*

Критерии оценивания практических работ:

Оценка экзамена	**Требования к знаниям**	**Требования к умениям**	**Требования к освоению ОК и ПК**
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий Было верно выполнено 90-100 % теста	Правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения заданий, применяет знания в комплексе, проводит анализ полученных результатов	Реализует творческий подход и инициативу в овладении профессией. Демонстрирует высокий уровень анализа информации, проявляет инициативу. Студент демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос Было верно выполнено 80-89 % теста	Правильно применяет теоретические положения при решении задач, владеет необходимыми навыками и приемами их выполнения, испытывает незначительные затруднения при анализе полученных результатов	Ответственен и активен в изучении профессии. Самостоятельно анализирует и оценивает информацию. Студент демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4

«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания толькоосновного материала, но неусвоил его деталей, допускает неточности, недостаточно правильные формулировки, Нарушения логической последовательности в изложении программного материала Было верно выполнено 7 0 - 7 9 % теста	Испытывает затруднения при решении задач, слабо аргументирует принятые решения, не в полной мере интерпретирует полученные результаты	Имеет общее представление о сущности профессии, малоинициативен. Требуется помощ ьпреподавателя при анализе и оценке информации. Студент демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий поМДК. Было верно выполнено менее 7 0 % теста	Неуверенно, с большими затруднениями решает задачи, неправильно использует необходимые формулы, не может сформулировать выводов по результатам решения задачи	Имеет низкое представление о сущности профессии, малоинициативен. Требуется помощь преподавателя при анализе и оценке информации. Студент не демонстрирует ОК 7, ПК 7.1, 7.2, 7.3 А 01/4, 09/4

5.3.ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ПО УП 07

Тема: «Команды Transact_SQL. Обеспечение безопасности в SOL Server»
Цель работы: отработать навыки использования команд языка Transact-SQL.
Задачи:

- ✓ *Создать БД и таблицы, используя запрос*
- ✓ *Заполнить таблицы БД информацией*
- ✓ *Создать запросы с использованием различных операторов и функций языка T-SQL*

Задание 1. *Для созданной базы данных, согласно номеру варианта, самостоятельно создайте на языке Transact-SQL запросы с отбором строк по условию:*

- *запрос с использованием операторов сравнения;*
- *запросы с использованием логических операторов AND, OR и NOT;*
- *запрос на использование выражений над столбцами;*
- *запрос с проверкой на принадлежность диапазону значений;*
- *запрос с проверкой на неопределенное значение.*

Задание 2. *Для созданной базы данных, согласно номеру варианта, самостоятельно создайте на языке Transact-SQL многотабличные запросы:*

- *запрос с использованием функции **COUNT**;*
- *запрос с использованием функции **SUM**;*

- *запрос с использованием группировки по одному столбцу;*
- *запрос с использованием сортировки по столбцу;*
- *запрос на добавление новых данных в таблицу;*
- *запрос на обновление существующих данных в таблице;*
- *запрос на удаление существующих данных.*

Задание 3. *Создайте новую БД:*

```
 CREATE DATABASE bookshop2;
GO
USE bookshop2;
CREATE TABLE catalogs
(
cat_ID INT PRIMARY KEY IDENTITY,
cat_name NVARCHAR (50) NOT NULL,
);
CREATE TABLE books (
book_ID INT NOT NULL IDENTITY,
b_name NVARCHAR(200) NOT NULL,
b_author NVARCHAR(200) NOT NULL,
b_year INT NOT NULL,
b_price DECIMAL(7,2) NULL default '0.00',
b_count INT NULL DEFAULT '0',
b_cat_ID INT NOT NULL DEFAULT '0',
PRIMARY KEY (book_ID),
FOREIGN KEY (b_cat_ID) REFERENCES catalogs (cat_ID) ON UPDATE CASCADE ON DELETE
CASCADE
);
CREATE TABLE users (
user_ID INT NOT NULL IDENTITY,
u_name NVARCHAR(50) NOT NULL,
u_patronymic NVARCHAR(50) NOT NULL,
u_surname NVARCHAR(50) NOT NULL,
u_phone NVARCHAR(12) NULL,
u_email NVARCHAR(50) NULL,
u_status   NVARCHAR(10)   CHECK   (u_status='active'or   u_status='passive'   or
u_status='lock' or u_status='gold') DEFAULT 'passive',
PRIMARY KEY (user_ID)
);
CREATE TABLE orders (
order_ID INT NOT NULL IDENTITY,
o_user_ID INT NOT NULL,
o_book_ID INT NOT NULL,
o_time DATETIME NOT NULL DEFAULT '0000-00-00 00:00:00',
o_number INT NOT NULL DEFAULT '0',
PRIMARY KEY (order_ID),
FOREIGN KEY (o_book_ID) REFERENCES books(book_ID) ON DELETE CASCADE ON UPDATE
CASCADE,
FOREIGN KEY (o_user_ID) REFERENCES users(user_ID) ON DELETE CASCADE ON UPDATE
CASCADE
);
```

Задание 4. Добавьте в нее таблицу Products с данными

cat_ID	cat_name
1	Программирование
2	Интернет
3	Базы данных
4	Сети
5	Мультимедиа

Задание 5. Заполните данными таблицу users, используя скрипт:

```
INSERT INTO users VALUES ('Александр','Валерьевич','Иванов','58-98-78',
'ivanov@email.ru', 'active'),
('Сергей','Иванович','Лосев','90-57-77', 'losev@email.ru', 'passive'),
('Игорь','Николаевич','Симонов','95-66-61', 'simonov@email.ru', 'active'),
('Максим','Петрович','Кузнецов',NULL, 'kuznetsov@email.ru', 'active'),
('Анатолий','Юрьевич','Петров', NULL, NULL, 'lock'),
('Александр','Александрович','Корнеев','89-78-36', 'korneev@email.ru', 'gold')
```

Убедитесь, что таблица заполнена корректными значениями.

Задание 6. Заполните следующими данными таблицу books:

book_ID	b_name	b_author	b_year	b_price	b_count	b_cat_ID
1	JavaScript в кармане	Рева О.Н.	2008	42.00	10	1
2	Visual FoxPro 9.0	Клепинин В.Б.	2007	660.00	2	1
3	C++ Как он есть	Тимофеев В.В.	2009	218.00	4	1
4	Создание приложений с помощью C#	Фаронов В.В.	2008	169.00	1	1
5	Delphi. Народные советы	Шкрыль А.А.	2007	243.00	6	1
6	Delphi. Полное руководство	Сухарев М.	2008	500.00	6	1
7	Профессиональное программирование на PHP	Шлосснейгл Дж.	2006	309.00	5	1
8	Совершенный код	Макконнелл С.	2007	771.00	1	1
9	Практика программирования	Керниган Б.	2004	214.00	12	1
10	Принципы маршрутизации в Internet	Хелеби С.	2001	428.00	4	2
11	Поиск в Internet	Гусев В.С.	2004	107.00	2	2
12	Web-конструирование	Дуванов А.А.	2003	177.00	6	2
13	Самоучитель Интернет	Константинов Ю.П.	2009	121.00	4	2
14	Популярные интернет-браузеры	Маринин С.А.	2007	82.00	6	2
15	Общение в Интернете	Экслер А.	2006	85.00	5	2
16	Базы данных	Малыхина М.П.	2006	326.00	2	3
17	Базы данных. Разработка приложений	Рудикова Л.В.	2006	189.00	6	3
18	Раскрытие тайн SQL	Оппель Э.	2007	200.00	3	3
19	Практикум по Access	Золотова С.И.	2007	87.00	6	3
20	Компьютерные сети	Танненбаум Э.	2007	630.00	6	4
21	Сети. Поиск неисправностей	Бигелоу С.	2005	434.00	4	4
22	Безопасность сетей	Брегг Р.	2006	462.00	5	4
23	Анализ и диагностика компьютерных сетей	Хогдал Дж.	2001	344.00	3	4
24	Локальные вычислительные сети	Епанешников А.	2005	82.00	8	4
25	Цифровая фотография	Надеждин Н.	2004	149.00	20	5
26	Музыкальный компьютер для гитариста	Петелин Р.Ю.	2004	217.00	15	5
27	Видео на ПК	Федорова А.	2003	231.00	10	5
28	Мультипликация во Flash	Киркпатрик Г.	2006	211.00	20	5
29	Запись CD и DVD	Гультяев А.К.	2003	167.00	12	5
30	Запись и обработка звука на компьютере	Лоянич А.А.	2008	51.00	8	5

Задание 7. Заполните следующими данными таблицу orders

order_ID	o_user_ID	o_book_ID	o_time	o_number
1	3	8	2009-04-01 10:39:38	1
2	6	10	2009-10-02 09:40:29	2
3	1	20	2009-18-02 13:41:05	4
4	4	20	2009-10-03 18:20:00	1
5	3	20	2009-17-03 19:15:36	1

Задание 7. Создайте таблицу Products, *используя запрос:*

```
CREATE TABLE Products
(
    Id INT IDENTITY PRIMARY KEY,
    ProductName NVARCHAR(30) NOT NULL,
    Manufacturer NVARCHAR(20) NOT NULL,
    ProductCount INT DEFAULT 0,
    Price MONEY NOT NULL
);
INSERT INTO Products
VALUES
('iPhone 6', 'Apple', 3, 36000),
('iPhone 6S', 'Apple', 2, 41000),
('iPhone 7', 'Apple', 5, 52000),
('Galaxy S8', 'Samsung', 2, 46000),
('Galaxy S8 Plus', 'Samsung', 1, 56000),
('Mi6', 'Xiaomi', 5, 28000),
('OnePlus 5', 'OnePlus', 6, 38000)
```

Задание 8. *Для выше созданной БД создать запросы:*

- *Получите все записи из всех полей таблицы users.*
- *Отсортируйте таблицу users по полю u_name по возрастанию и получите первые три записи.*
- *Отсортируйте таблицу users по полю u_name по возрастанию и получите последние три записи.*
- *Создайте простой запрос на выборку к таблице books, который содержит поля b_name, b_year, b_price и b_count.*
- *Создайте простой запрос на выборку к таблице books, который содержит поля b_name, b_year, b_price и b_count. Запрос должен вывести только книги из категории под номером три.*
- *Создайте простой запрос на выборку к таблице books, который содержит поля b_name, b_year, b_price, b_count и поле b_summ, поле b_summ содержит суммарную стоимость всех экземпляров данной книги, его значение является произведением значений полей b_price и b_count.*
- *Создайте запрос с использованием агрегатных функций к таблице books, который содержит поля b_cat_ID и b_cat_summ, которое содержит суммарную стоимость всех книг в данной категории.*
- *Создайте запрос с использованием агрегатных функций к таблице books, который содержит поля b_cat_ID и b_cat_summ, поле b_cat_summ содержит суммарную стоимость всех книг в данной категории. Выборка должна быть отсортирована по возрастанию по полю b_cat_summ и содержать только значения более 10 000.*

Задание 9. *Рефлексия*
Сформировать вывод по пройденному занятию.

Лист согласования. Дополнения и изменения к комплексу КОС на учебный год

Дополнения и изменения к комплекту КОС на_____учебный год по МДК. 07.01 Управление и автоматизация баз данных
В комплект КИМ внесены следующие изменения:
_____
_____
_____
_____
Дополнения и изменения в комплекте КОС обсуждены на заседании ЦК
_____
«_____»_____20_____г. (протокол №_____).
Председатель ЦК_____/_____/

Лист согласования. Дополнения и изменения к комплексу КОС на учебный год

Дополнения и изменения к комплекту КОС на_____учебный год по МДК.07.02 Сертификация информационных систем

В комплект КИМ внесены следующие изменения:

_____
_____
_____
_____

Дополнения и изменения в комплекте КОС обсуждены на заседании ЦК

_____

«_____»_____20_____г. (протокол №_____).

Председатель ЦК_____/_____/