

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ухтинский государственный технический университет»
(УГТУ)
филиал Ухтинского государственного технического университета
в г. Усинске
(УФ УГТУ)
(среднего профессионального образования)

УТВЕРЖДАЮ
И. о. директора филиала
_____ О. В. Филиппова
« ____ » _____ 20__ г.

КОМПЛЕКС ОЦЕНОЧНЫХ СРЕДСТВ
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
ПМ.01 Разработка, администрирование и защита баз данных
образовательной программы
среднего профессионального образования
По специальности 09.02.11 Разработка и управление программным
обеспечением

г. Усинск
2026

1. ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Область применения

Комплект оценочных средств (далее – КОС) предназначен для контроля и оценки результатов прохождения учебной дисциплины ПМ.07 «Сoadминистрирование баз данных и серверов», образовательной программы среднего профессионального образования (далее – ОП СПО) по специальности 09.02.11 Разработка и управление программным обеспечением.

1.2 Результаты освоения компетенции

В результате проведения промежуточной аттестации по дисциплине осуществляется комплексная оценка овладения следующими профессиональными и общими компетенциями:

Таблица 2.1

Код	Результат освоения компетенции
ПК 1.1.	Проектировать базы данных.
ПК 1.2.	Разрабатывать объекты баз данных в соответствии с результатами анализа предметной области.
ПК 1.3.	Реализовывать базу данных в конкретной системе управления базами данных.
ПК 1.4.	Администрировать базы данных.
ПК 1.5.	Защищать информацию в базе данных с использованием технологии защиты информации.
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках.

2. ФОРМЫ КОНТРОЛЯ И ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В соответствии с учебным планом и рабочей программой предусматривается текущий и промежуточный контроль результатов освоения.

Предметом оценки служат умения и знания, предусмотренные требованиями ФГОС по дисциплине ПМ.01 «Разработка, администрирование и защита баз данных», направленные на формирование общих и профессиональных компетенций, а также личностных результатов в рамках программы воспитания.

2.1 Критерии и нормы оценки знаний обучающихся.

Оценка «5» ставится в случае:

- знания, понимания, глубины усвоения обучающимися всего объёма программного материала;
- умения выделять главные положения в изученном материале, на основании фактов и примеров обобщать, делать выводы, устанавливать межпредметные и внутри предметные связи, творчески применять полученные знания в незнакомой ситуации;
- отсутствия ошибок и недочётов при воспроизведении изученного материала, при устных ответах устранения отдельных неточностей с помощью дополнительных вопросов учителя, соблюдения культуры письменной и устной речи, правил оформления письменных работ.

Оценка «4» ставится в случае:

- знания всего изученного программного материала;
- умения выделять главные положения в изученном материале, на основании фактов и примеров обобщать, делать выводы, устанавливать внутри предметные связи, применять полученные знания на практике;
- допущения незначительных (негрубых) ошибок, недочётов при воспроизведении изученного материала; соблюдения основных правил культуры письменной и устной речи, правил оформления письменных работ.

Оценка «3» ставится в случае:

- знания и усвоения материала на уровне минимальных требований программы, затруднения при самостоятельном воспроизведении, возникновения необходимости незначительной помощи преподавателя;
- умения работать на уровне воспроизведения, затруднения при ответах на видоизменённые вопросы;

- наличия грубой ошибки, нескольких грубых ошибок при воспроизведении изученного материала; незначительного несоблюдения основных правил культуры письменной и устной речи, правил оформления письменных работ.

Оценка «2» ставится в случае:

- знания и усвоения материала на уровне ниже минимальных требований программы; наличия отдельных представлений об изученном материале;
- отсутствия умения работать на уровне воспроизведения изученного материала, затруднения при ответе на стандартные вопросы;
- наличия нескольких грубых ошибок, большого числа негрубых при воспроизведении изученного материала, значительного несоблюдения основных правил культуры письменной и устной речи, правил оформления письменных работ.

2.2 Критерии оценки за тестирование

Оценка 5 «отлично» (85 % -100 %)

Оценка 4 «хорошо» (75 % - 84 %)

Оценка 3 «удовлетворительно» (55 % -74 %)

Оценка 2 «неудовлетворительно» (менее 54 %)

2.3 Формы и методы оценивания учебных дисциплин по модулю «Разработка, администрирование и защита баз данных»

Раздел, тема	Формы и методы контроля					
	Текущий контроль		Промежуточная аттестация		Итоговая аттестация	
	Формы контроля	Проверяе мые Знания, умения, ОК, ЛР	Формы контроля	Проверяемые знания, умения ОК, ЛР	Формы контроля	Проверяе мые ЗУН, ОК, ЛР
МДК. 01.01 Управлени е и автоматиза ция баз данных	Т, УО, ПР	ОК 7 ПК 7.1 - 7.3				
Тема 1. Принципы построения и администр ирования баз данных			ПРН№1 ПРН№2	ОК 7 ПК 7.1 -7.3		
Тема 2. Серверы баз данных			ПРН№3 ПРН№4 ПРН№5 ПРН№6 ПРН№7	ОК 7 ПК 7.1 -7.3		
Тема 3. Администр ирование баз данных и серверов			ПРН№1 ПРН№2 ПРН№3 ПРН№4 ПРН№5 ПРН№6 ПРН№7 ПРН№8	ОК 7 ПК 7.1 -7.3		
Экзамен			Т, ПР			
МДК.01.02 Сертифика ция информаци онных систем	Т, УО, ПР	ОК 7 ПК 7.1 - 7.3				
Тема 1. Защита и сохранност ь информаци			ПРН№1 ПРН№2 ПРН№3 ПРН№4	ОК 7 ПК 7.1 -7.3		

и баз данных						
Тема 2 Сертифика ция информаци онных систем			ПРН [№] 1 ПРН [№] 2 ПРН [№] 3	ОК 7 ПК 7.1 -7.3		
Экзамен			Т			

Кодификатор оценочных средств

Функциональный признак оценочного средства (тип контрольного задания)	Код оценочного средства
Устный опрос	УО
Практическая работа	ПР №
Самостоятельная работа	СР
Тестирование	Т
Другая форма контроля	ДФК
Экзамен	Эк

3. Контрольно-оценочные материалы для промежуточной и итоговой аттестации по модулю «Разработка, администрирование и защита баз данных»

3.1 Типовые задания для проведения текущего контроль

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.

Зачет 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) tempdb
- 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 экземпляры 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 пользователя 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 контейнер:

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

10. Для создания новой учетной записи можно воспользоваться следующей хранимой 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_helpprotect
- 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

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.

3.2 ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ПО

МДК. 01.01 УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ БАЗ ДАННЫХ И МДК.01.02 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

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.

Задание 1. Изучите:

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

Выполнение работы:

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» отобразить 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 (SACLs). 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 «Ок».

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.)

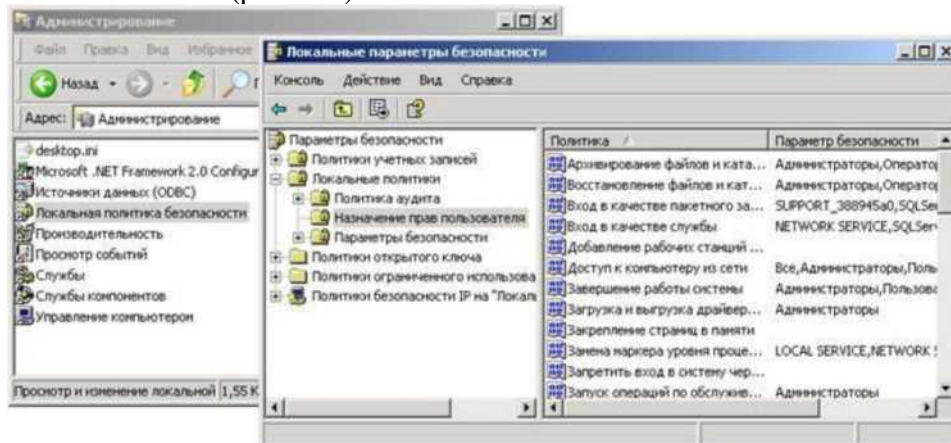


Рисунок 1.1 - Окно Локальные параметры безопасности

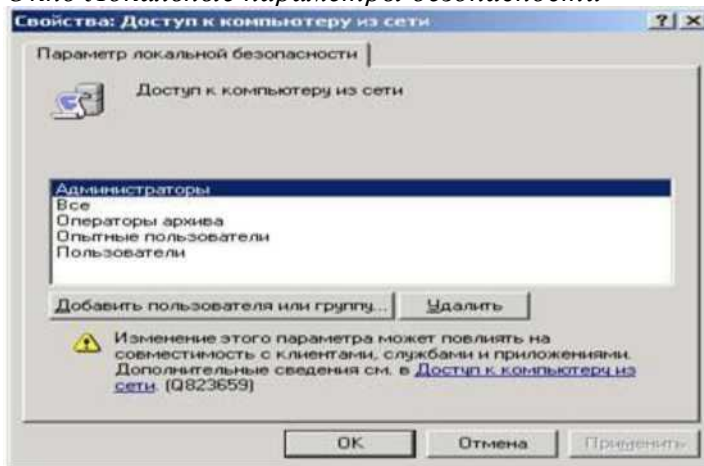


Рисунок 1.2 - Окно Параметр локальной безопасности

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.).

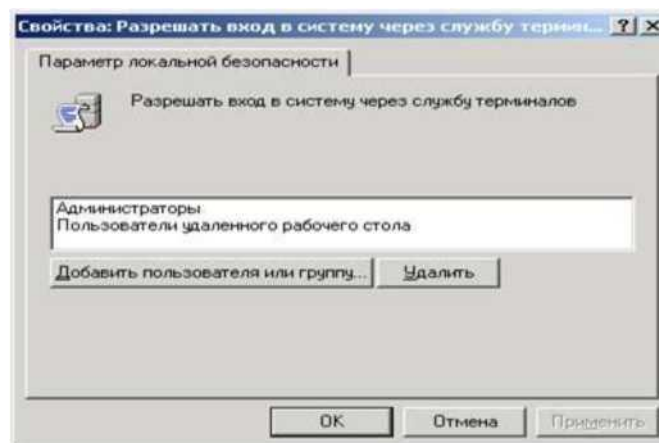


Рисунок 1.4 - Окно Разрешить вход в систему через службу терминалов

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.).

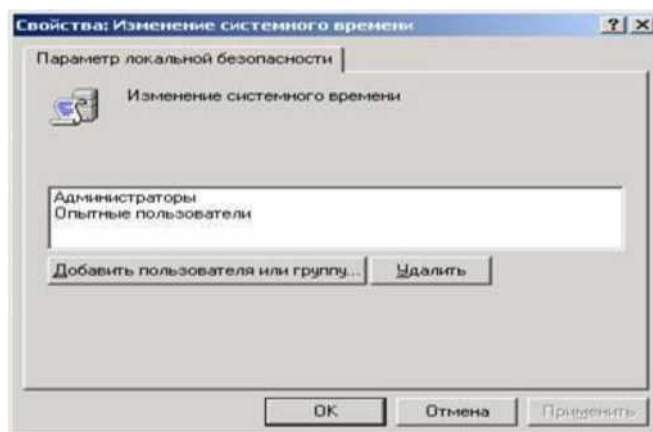


Рисунок 1.5 - Окно Изменение системного времени

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.).

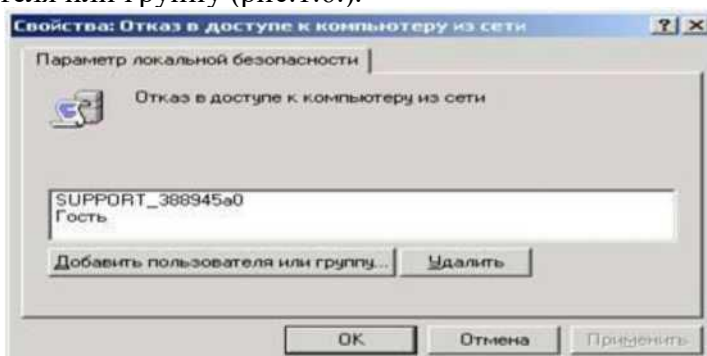


Рисунок 1.6 - Окно Отказ в доступе к компьютеру из сети

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.).

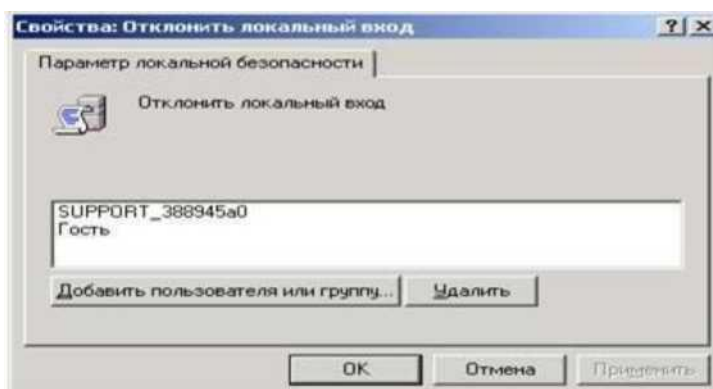


Рисунок 1.7 - Окно Отклонить локальный вход

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).

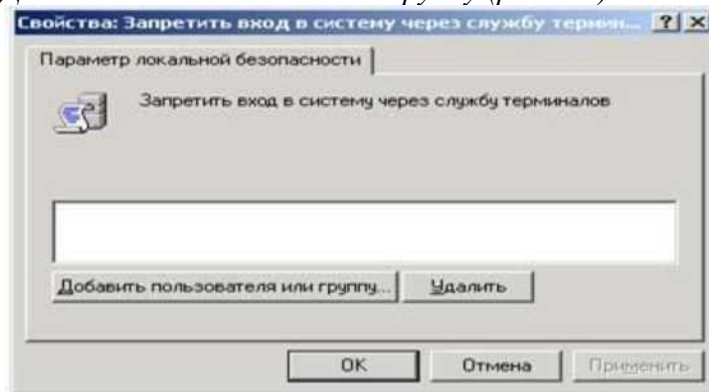
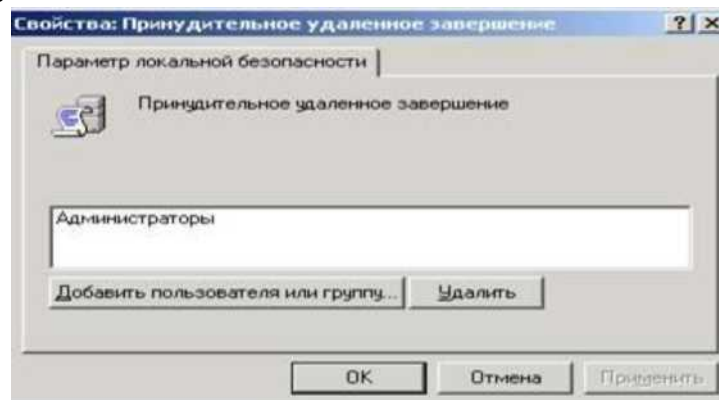


Рисунок 1.8 - Окно *Запретить вход в систему через службу терминалов*

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.)

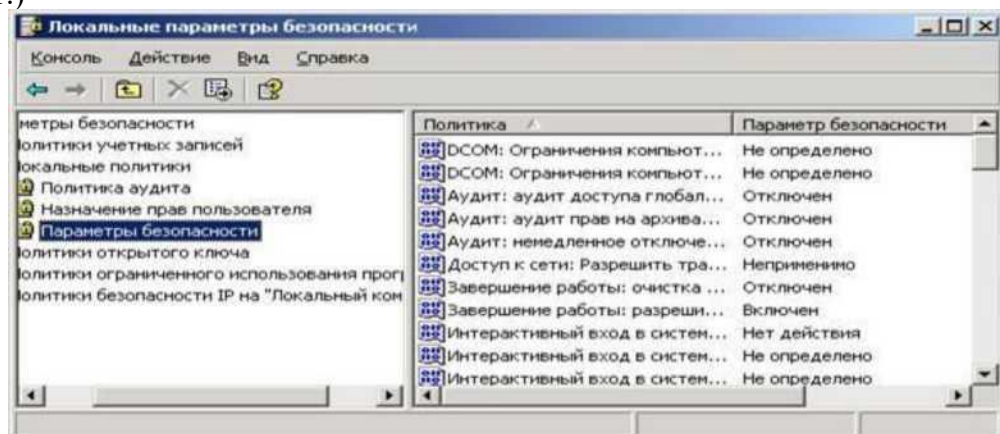


Рисунок 1.10 - Окно Параметры безопасности

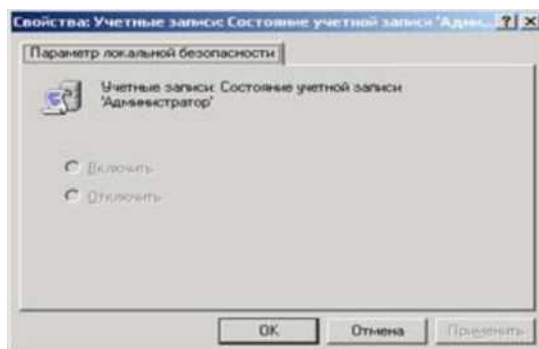


Рисунок 1.11 - Окно Состояние учетной записи 'Администратор'

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 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 отключен 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:

- Allow Wildcards - 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 выявляются ошибки и вносятся исправления 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

1. Если пользователь работает на домашнем компьютере, достаточно производить обновления системы раз в неделю. Если система является корпоративной или часто находится в Интернете, рекомендуется проводить ежедневное обновление, чтобы надежно защититься от сетевых взломщиков. Если система скачает обновления, и они будут готовы к установке, 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, but let 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't automatically download or install them опция позволяет операционной системе проверять наличие обновлений, но запрещает их непосредственное

скачивание или установку. Эта опция полезна, если пользователь сам устанавливает 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.

3.3 ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ПО УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Тема: «Команды Transact_SQL. Обеспечение безопасности в SQL Server»

Цель работы: отработать навыки использования команд языка Transact-SQL.

Задачи:

1. Создать БД и таблицы, используя запрос;
2. Заполнить таблицы БД информацией.

Практическое задание 1.

Создайте новую БД bookshop, в котором будут реализованы таблицы каталог, книги, пользователи, заказы:

Решение:

```
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 );

```

Практическое задание 2.

Заполните данными таблицу users, используя скрипт:

```

INSERT INTO users VALUES ('Александр','Валерьевич','Иванов','58-98-78',
'ivanov@email.ru', 'active'), ('Сергей','Иванович','1 Лосев','90-57-77', 'losev@email.ru', 'passive
1'), ('Игорь','Николаевич','Симонов','95-66-61', 'simonov@email.ru', 'active'),
('Максим','Петрович','Кузнецов',NULL, 'kuznetsov@email.ru', 'active'), ('Анатолий','1
Юрьевич','1 Петров', NULL, NULL, 'lock'), ('Александр','Александрович','Корнеев','89-78-
36', 'korneev@einail.ru', 'gold')

```

Решение:

```

INSERT INTO users (u_name, u_patronymic, u_surname, u_phone, u_email, u_status)
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@einail.ru', 'gold');

```

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ухтинский государственный технический университет»
(УГТУ)

филиал Ухтинского государственного технического университета
в г. Усинске
(УФ УГТУ)
(среднего профессионального образования)

УТВЕРЖДАЮ
И. о. директора филиала
О. В. Филиппова
« 20 » 2016 г.



**КОМПЛЕКС ОЦЕНОЧНЫХ СРЕДСТВ
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**

**ПМ.01 Разработка, администрирование и защита баз данных
образовательной программы
среднего профессионального образования**

По специальности 09.02.11 Разработка и управление программным
обеспечением

г. Усинск
2026

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ухтинский государственный технический университет»
(УГТУ)

**филиал Ухтинского государственного технического университета
в г. Усинске
(УФ УГТУ)
(среднего профессионального образования)**

УТВЕРЖДАЮ

И. о. директора филиала
О.В. Филиппова

« » 2006г.



КОМПЛЕКС ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

**ПМ.01.01(К) Экзамен по профессиональному модулю
ПМ.01 «Разработка, администрирование и защита баз данных»
образовательной программы
среднего профессионального образования
По специальности 09.02.11 Разработка и управление программным
обеспечением**

г. Усинск
2026

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ухтинский государственный технический университет»
(УГТУ)

филиал Ухтинского государственного технического университета
в г. Усинске
(УФ УГТУ)
(среднего профессионального образования)

УТВЕРЖДАЮ
И. о. директора филиала
О.В. Филиппова
« 20 » 2026 г.

(подпись) _____ (И. О. Фамилия)
« ____ » _____ 20 ____ г.

(подпись) _____ (И. О. Фамилия)
« ____ » _____ 20 ____ г.

РАБОЧАЯ ПРОГРАММА

Дисциплина: Разработка, администрирование и защита баз данных
Индекс: ПМ.01
Специальность: 09.02.11 Разработка и управление ПО
Форма очная
обучения:
Курс (ы) 3
Семестр (ы): 5, 6

г. Усинск
2026

Рабочая программа разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) 09.02.11 Разработка и управление программным обеспечением, утверждённым приказом Министерства образования и науки Российской Федерации 24 февраля 2025 г. № 138, зарегистрированным в Министерстве юстиции Российской Федерации 31 марта 2025 года, регистрационный № 81696, входящим в укрупнённую группу специальностей 09.00.00 Информатика и вычислительная техника.

Разработчик Лопешова М.А. преподаватель СПО УФ УГТУ.

Рассмотрено на заседании ученого совета УФ УГТУ (протокол от 26.05.2026 № 06).

СОГЛАСОВАНО

Заместитель директора УФ УГТУ
по учебной работе

О.В. Филиппова