ЦБИ-сервис

Система управления базами данных Microsoft® SQL Server™ 2005

Руководство по безопасной настройке и контролю сертифицированной версии

Версия 1.0

2007

СОДЕРЖАНИЕ

Перечень сокращений

ACL – Access Control List

GPC – Group Policy Container

GPT – Group Policy Template

HKLM – H_KEY_LOCAL_MACHINE

NTFS – NT File System

SAM – Security Account Manager

SDDL – Security Descriptor Definition Language

SID – Security Identifier

SP – Service Pack

SQL – Structured Query Language

БД – база данных

ОГП – объект групповой политики

ОП – организационное подразделение

ОС – операционная система

СУБД – система управления базами данных

1 Введение

Настоящий документ содержит рекомендации по настройке и контролю механизмов защиты систем управления базами данных Microsoft® SQL Server™ 2005 при организации обработки конфиденциальной информации на объекте информатизации. Представленные рекомендации применимы для сертифицированных по требованиям безопасности систем управления базами данных Microsoft® SQL Server™ 2005 Standard Edition и Microsoft® SQL Server™ 2005 Enterprise Edition (далее, СУБД Microsoft® SQL Server™ 2005).

Руководство предназначено для настройки механизмов защиты системы управления базами данных Microsoft® SQL Server™ 2005 в соответствии с той конфигурацией безопасности, в которой данное изделие было сертифицировано, а также подготовки объекта информатизации к аттестации на соответствие требованиям безопасности при обработке конфиденциальной информации.

Система управления базами данных Microsoft® SQL Server™ 2005 может функционировать как на автономном компьютере (сервере баз данных), так и на компьютере (сервере баз данных) в составе локальной вычислительной сети. В свою очередь в локальной вычислительной сети может быть развернута инфраструктура службы каталогов Microsoft® Active Directory™ на базе серверных операционных систем семейства Microsoft® Windows® Server 2003. В этом случае компьютер (сервер БД), функционирующий под управлением операционной системы семейства Microsoft® Windows® Server 2003, может быть включен в состав домена Active Directory, либо не входить в него, но иметь возможность взаимодействовать с другими компьютерами. Взаимодействие компьютера в данной конфигурации с остальными будет эквивалентно взаимодействию компьютеров в составе рабочей группы (Workgroup).

Таким образом, исходя из вариантов расположения СУБД Microsoft® SQL Server™ 2005 и клиентских приложений (СУБД и клиентские приложения могут быть расположены либо на одном, либо на разных компьютерах), а также возможных вариантов среды функционирования СУБД Microsoft® SQL Server™ 2005 (либо на автономном компьютере, либо на компьютере в составе локальной вычислительной сети, включенном в домен Active Directory™), можно выделить следующие варианты функционирования СУБД Microsoft® SQL Server™ 2005 (см. таблицу 1.1).

Таблица 1.1 – Варианты функционирования СУБД Microsoft® SQL Server™ 2005

№ п/п	Варианты функционирования системы управления базами данных
Варианты функционирования СУБД Microsoft® SQL Server™ 2005 при включении компьютера в домен Active Directory™	
1.	СУБД Microsoft® SQL Server™ 2005 установлена на компьютере, одновременно являющимся контроллером домена Active Directory™ и сервером БД. Клиентские приложения установлены на входящие в состав домена Active Directory™ клиентские рабочие станции, функционирующие под управлением клиентской ОС Microsoft® Windows® XP Professional SP2.
2.	СУБД Microsoft® SQL Server™ 2005 установлена на компьютере, функционирующем под управлением серверной операционной системы семейства Microsoft® Windows® Server 2003, но не являющимся контроллером домена Active Directory™. Клиентские приложения также установлены на данном компьютере.
3.	СУБД Microsoft® SQL Server™ 2005 установлена на компьютере, функционирующем под управлением серверной операционной системы семейства Microsoft® Windows® Server 2003, но не являющимся контроллером домена Active Directory™. Клиентские приложения установлены на входящие в состав домена Active Directory™ клиентские рабочие станции, функционирующие под управлением клиентской ОС Microsoft® Windows® XP Professional SP2.
Варианты функционирования СУБД Microsoft® SQL Server™ 2005 в случае, когда компьютер не входит в домен Active Directory™ (конфигурация Stand-Alone)	
4.	СУБД Microsoft® SQL Server™ 2005 установлена на автономном компьютере, функционирующим под управлением серверной операционной системы семейства Microsoft® Windows® Server 2005. Клиентские приложения также установлены на данном компьютере.
5.	СУБД Microsoft® SQL Server™ 2005 установлена на автономном компьютере, функционирующим под управлением серверной операционной системы семейства Microsoft® Windows® Server 2003. Клиентские приложения установлены на клиентские рабочие станции, функционирующие под управлением клиентской ОС Microsoft® Windows® XP Professional SP2.

2 Последовательность действий по настройке сертифицированной версии СУБД Microsoft® SQL Server™ 2005

Администратором эксплуатирующей организации для приведения СУБД Microsoft® SQL Server™ 2005 в конфигурацию, в которой данное ИТ-изделие было сертифицировано, необходимо выполнить как настройку самой СУБД, так и сертифицированной версии операционной системы семейства Microsoft® Windows Server™ 2003, под управлением которой она функционирует.

2.1 Процедуры прединсталляционной настройки операционной системы

Процедуры прединсталляционной настройки описывают последовательность предшествующих установке СУБД Microsoft® SQL Server™ 2005 действий, выполняемых администратором по конфигурированию операционной системы семейства Microsoft® Windows Server™ 2003, под управлением которой данная СУБД функционирует.

Процедуры прединсталляционной настройки операционной системы подразумевают выполнение администратором эксплуатирующей организации следующих действий:

1. Создание доменной или локальной учетной записи (в зависимости от варианта функционирования СУБД), используемой для запуска служб SQL Server и SQL Server Agent. При этом для данной учетной записи должен быть установлен пароль, удовлетворяющий требованиям сложности, а ее описание с целью исключения возможных ассоциаций с ее предназначением изменено. Кроме того, при создании учетной записи следует выбрать опцию «`Срок действия пароля неограничен`», свидетельствующую об отсутствии необходимости дальнейшей смены пароля, используемой учетной записью.

2. Создание глобальной группы безопасности и включение в состав ее участников учетной записи, используемой для запуска служб SQL Server и SQL Server Agent. Членство в данной группе безопасности следует контролировать с использованием механизма групп с ограниченным доступом через групповую политику.

3. Исключение учетной записи, используемой для запуска служб SQL Server и SQL Server Agent, из состава группы безопасности «Пользователи домена», в которую она включается по умолчанию при создании. Данный шаг позволит предотвратить использование данной учетной записью привилегий, назначаемых группе «Пользователи домена» по умолчанию.

4. Задание ограничения на возможность входа в систему с использованием созданной учетной записи только на заданных компьютерах, выступающих в роли серверов

БД под управлением СУБД Microsoft® SQL Server™ 2005 (см. рисунок 2.1). Задание данного вида ограничения для учетной записи выполняется с использованием оснастки консоли управления «Active Directory – пользователи и компьютеры» и возможно только для доменных учетных записей.

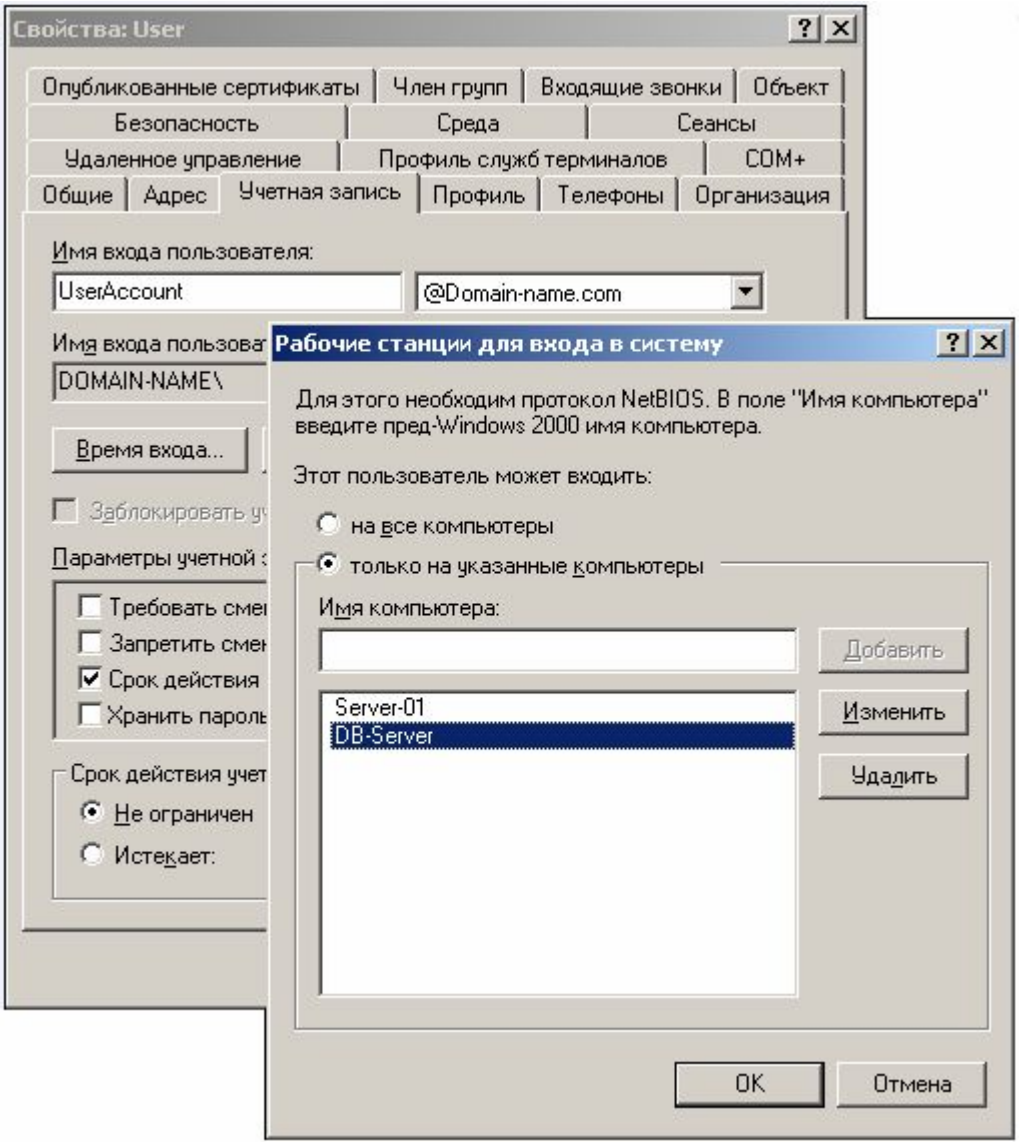

Рисунок 2.1

5. Назначение указанной учетной записи следующего минимального набора прав и привилегий (см. рисунок 2.2):

- работа в режиме операционной системы;
- обход перекрестной проверки;
- настройка квот памяти для процесса;
- отклонить локальный вход;
- закрепление страниц в памяти;

– вход в качестве службы;

– вход в качестве пакетного задания;

– замена маркера уровня процесса.

Детальное описание назначаемых прав доступа представлено в Приложении А настоящего Руководства.

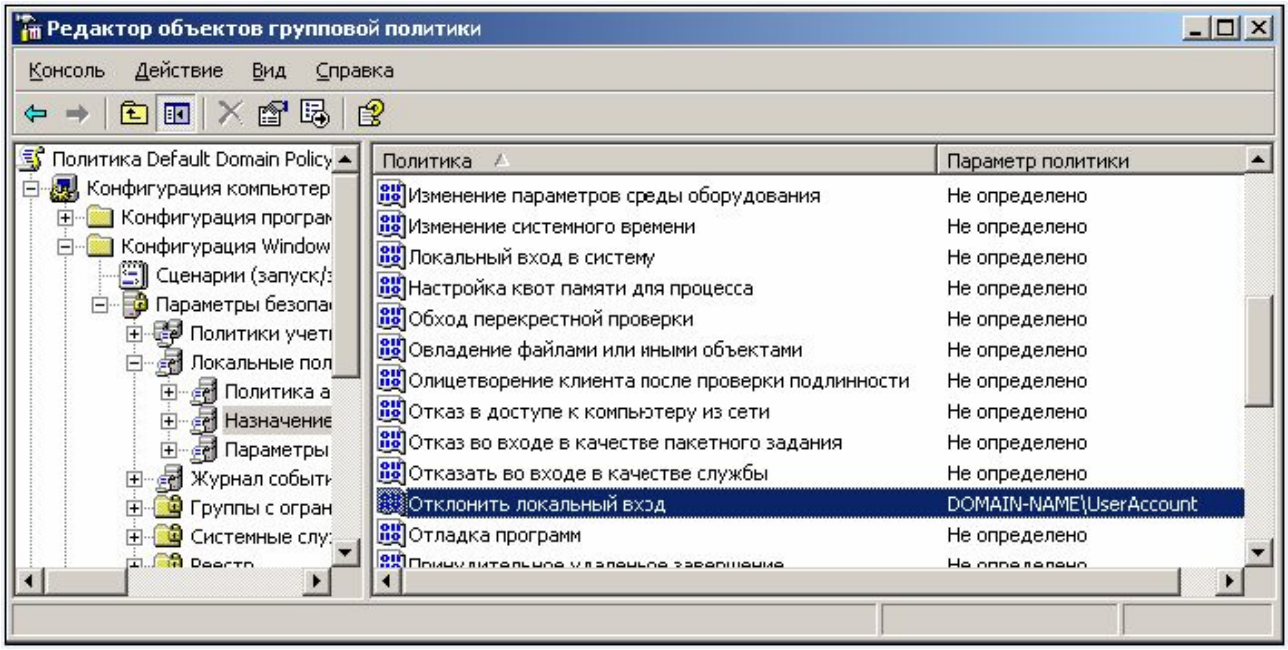

Рисунок 2.2

6. Изменение предустановленных параметров безопасности, касающихся в первую очередь встроенной локальной учетной записи администратора и его пароля. В частности для встроенной локальной учетной записи «Администратор» должен быть установлен пароль, удовлетворяющий требованиям сложности, а сама учетная запись, так же как и её стандартное описание, изменено.

7. Осуществление запрета учетной записи «Гость» (Guest), позволяющей осуществлять анонимный доступ к сетевым ресурсам сервера БД.

8. Осуществление настройки ряда служб операционной системы семейства Microsoft® Windows Server™ 2003 в части запрета их запуска. Описание рекомендуемых к запрету служб операционной системы представлено в Приложении А.

Назначение прав учетной записи, используемой для запуска служб СУБД Microsoft® SQL Server™ 2005, переименование учетной записи администратора, определение состояния учетной записи «Гость» и настройка режима запуска служб операционной системы семейства Microsoft® Windows Server™ 2003 может реализовываться с использованием механизма групповой политики и осуществляться как вручную, так и путем применения

шаблона безопасности к соответствующему объекту групповой политики. Использование групповой политики позволяет обеспечить централизованное управление и применение единых параметров безопасности для всех серверов БД под управлением СУБД Microsoft® SQL Server™ 2005. Описание порядка настройки и применения групповой политики представлено в пп.2.3 настоящего Руководства.

2.2 Процедуры безопасной установки сертифицированной версии СУБД Microsoft® SQL Server™ 2005

В данном разделе процедуры безопасной установки сертифицированной версии СУБД Microsoft® SQL Server™ 2005 будут рассмотрены на примере СУБД Microsoft® SQL Server™ 2005 Standard Edition.

Для установки СУБД Microsoft® SQL Server™ 2005 должны быть выбраны соответствующие аппаратные средства, удовлетворяющие минимальным системным требованиям, предъявляемым к данной версии системы управления базами данных, и учитывающие вопросы оптимизации производительности СУБД Microsoft® SQL Server™ 2005 и решаемые задачи.

Установка СУБД Microsoft® SQL Server™ 2005 должна осуществляться пользователем, обладающим административными полномочиями в операционной системе семейства Microsoft® Windows Server™ 2003, под управлением которой функционирует СУБД, в следующей последовательности:

1. Осуществить вызов программы установки СУБД Microsoft® SQL Server™ 2005 одним из следующих способов:
   - вставить компакт-диск с дистрибутивом СУБД Microsoft® SQL Server™ 2005 в привод CD-ROM и дважды щелкнуть `splash.hta` в каталоге `\Servers\`, расположенном на компакт-диске. В появившемся диалоговом окне щелкнуть на “`Server components, tools, Book Online and samples`” (см. рисунок 2.3);
   - дважды щелкнуть файл `setup.exe` в каталоге `\Servers\`, расположенном на компакт-диске с дистрибутивом СУБД Microsoft® SQL Server™ 2005.

Рисунок 2.3

2. Ознакомится с лицензионным соглашением и в случае согласия нажать `Next>` (Далее) (см. рисунок 2.4).

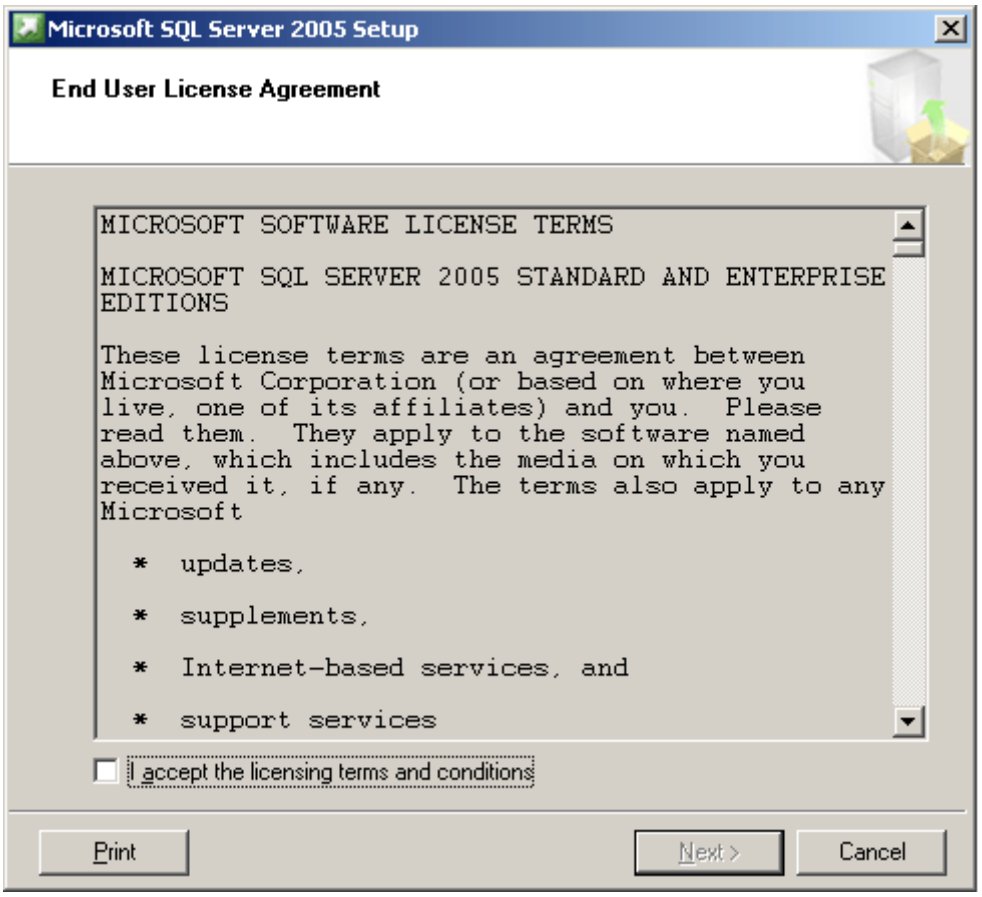

Рисунок 2.4

3. Нажать `Install>` (Инсталляция) для продолжения установки.

4. Подождать, пока инсталлятор протестирует компьютер на соответствие системным требованиям и, в случае успешного завершения операции, нажать `Next>` (Далее) (см. рисунок 2.5).

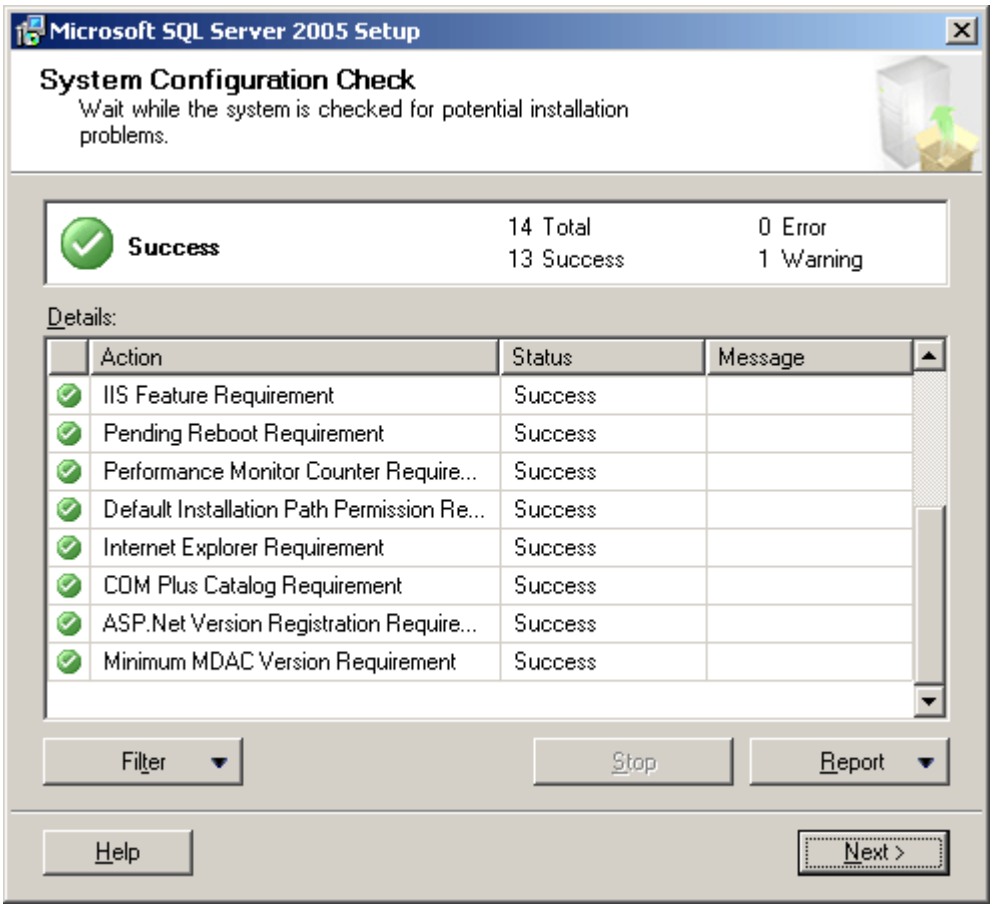

Рисунок 2.5

5. Ввести имя пользователя, название компании (необязательно) и серийный номер продукта. Нажать `Next>` (Далее) (см. рисунок 2.6).

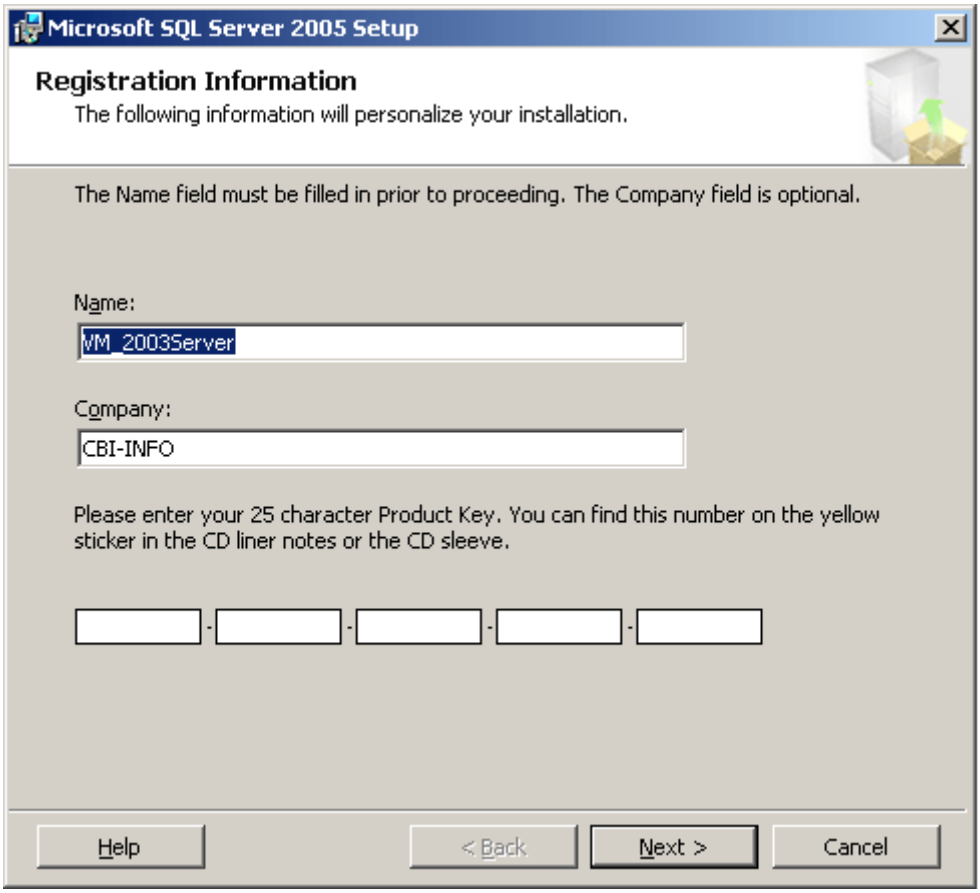

Рисунок 2.6

6. В окне выбора компонент вручную выбрать необходимые для работы компоненты СУБД Microsoft® SQL Server™ 2005 (см. рисунок 2.7). Нажать `Next>` (Далее).

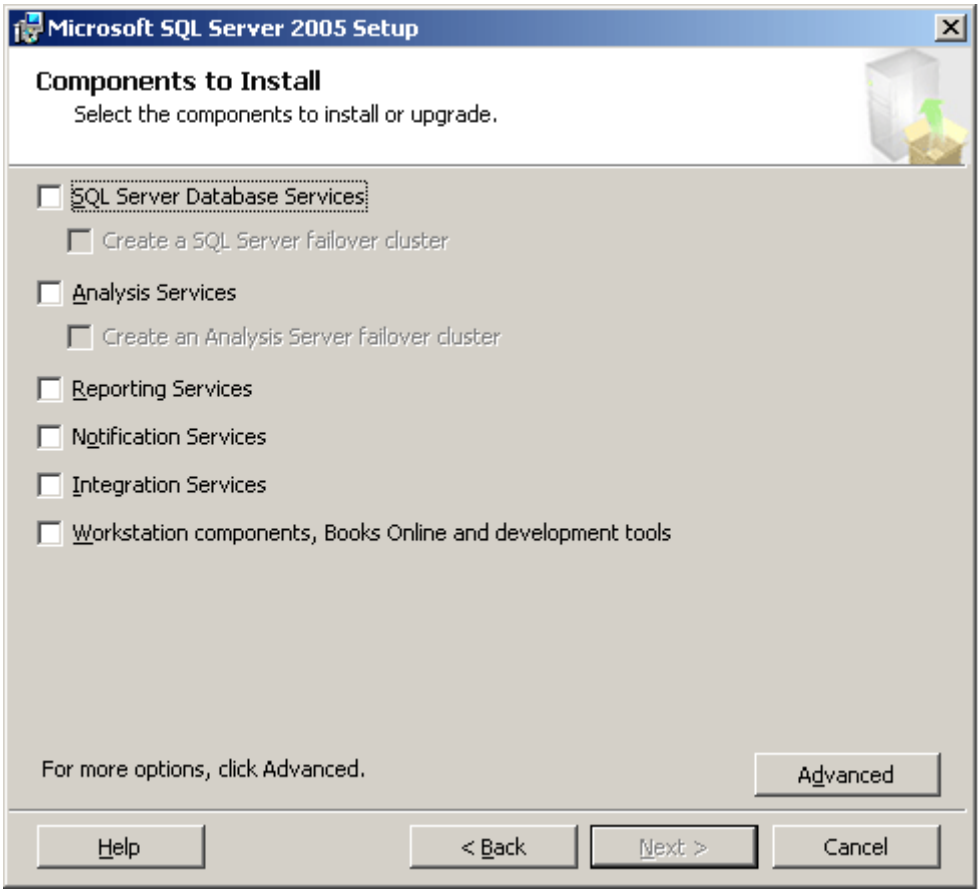

Рисунок 2.7

7. Ввести имя устанавливаемого экземпляра СУБД Microsoft® SQL Server™ 2005 (см. рисунок 2.8). При этом устанавливаемый экземпляр можно сделать экземпляром по умолчанию (выбрав опцию `Default instance`) или именованным экземпляром (`Named instance`). На одном сервере БД может быть установлено несколько именованных экземпляров, обращение к которым будет осуществляться по именам, и только один экземпляр по умолчанию.

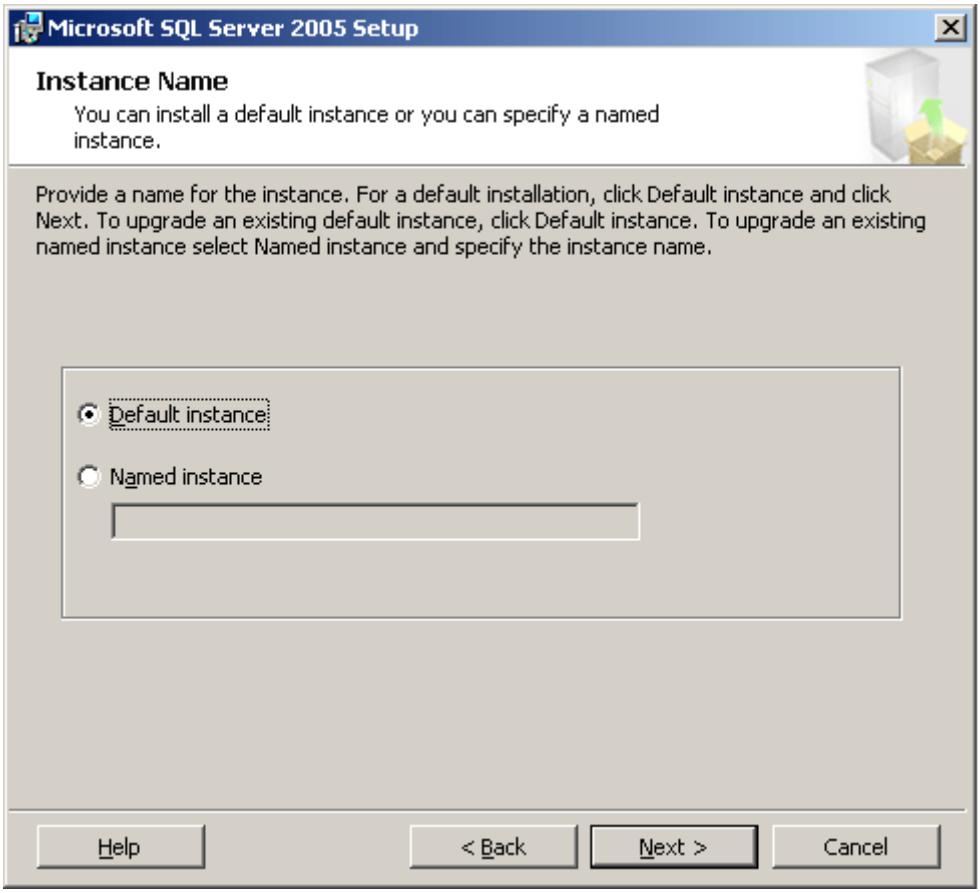

Рисунок 2.8

8. Осуществить ввод имени локальной или доменной учетной записи, используемой для запуска служб SQL Server и каждого из компонентов (см. рисунок 2.9). При этом для запуска служб не рекомендуется использовать системные учетные записи. Выбрать компоненты, которые будут запущены непосредственно после установки СУБД Microsoft® SQL Server™ 2005. Нажать `Next>` (Далее).

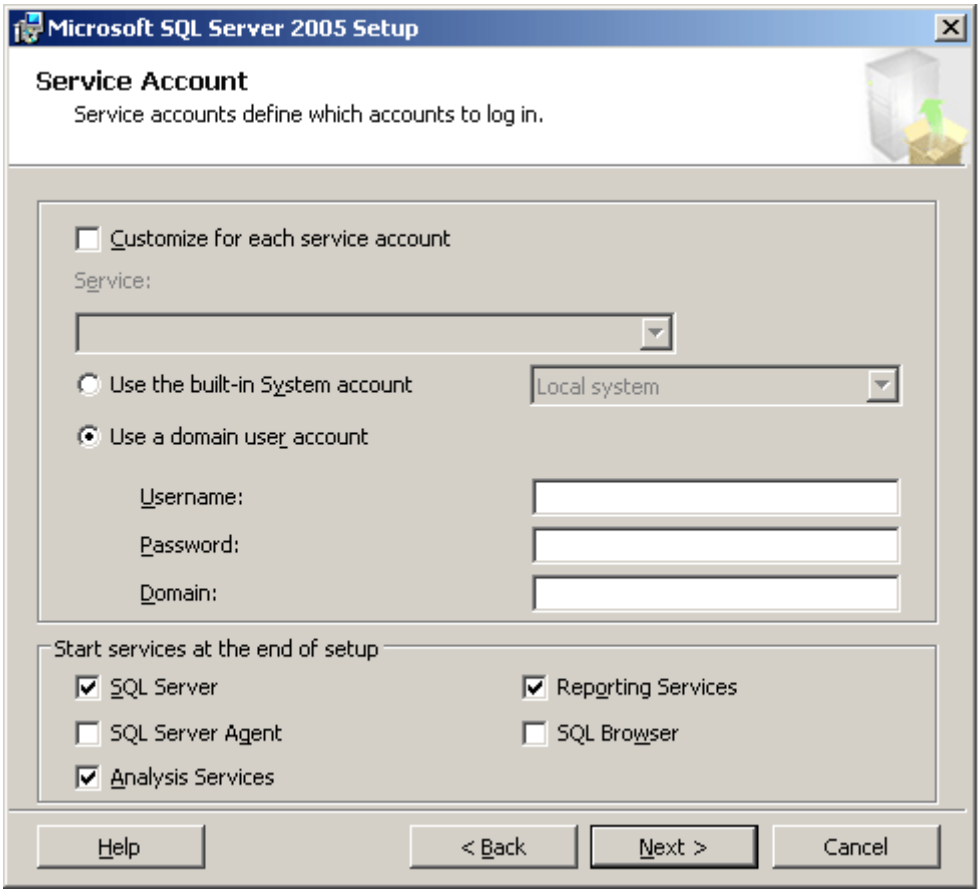

Рисунок 2.9

9. Выбрать режим проверки подлинности пользователей. При этом рекомендуемым является режим «Windows Authentication Mode» - режим проверки подлинности Windows (см. рисунок 2.10). Использование смешанного режима проверки подлинности (Mixed Mode) должно быть запрещено, поскольку он обладает рядом недостатков и не позволяет обеспечить адекватную защиту СУБД Microsoft® SQL Server™ 2005 от попыток нарушения безопасности даже нарушителями с низким потенциалом нападения. Нажать Next> (Далее).

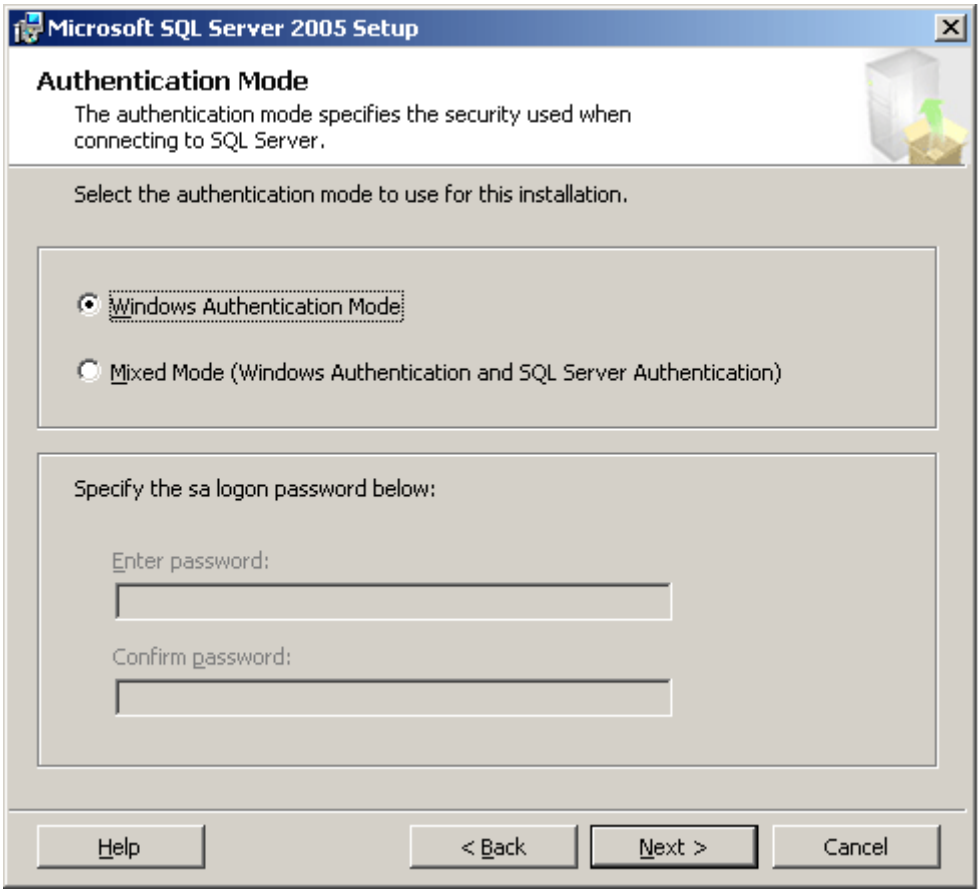

Рисунок 2.10

10. Настроить параметры сортировки данных СУБД Microsoft® SQL Server™ 2005 (см. рисунок 2.11). Рекомендуется оставить настройки по умолчанию. Нажать `Next>` (Далее).

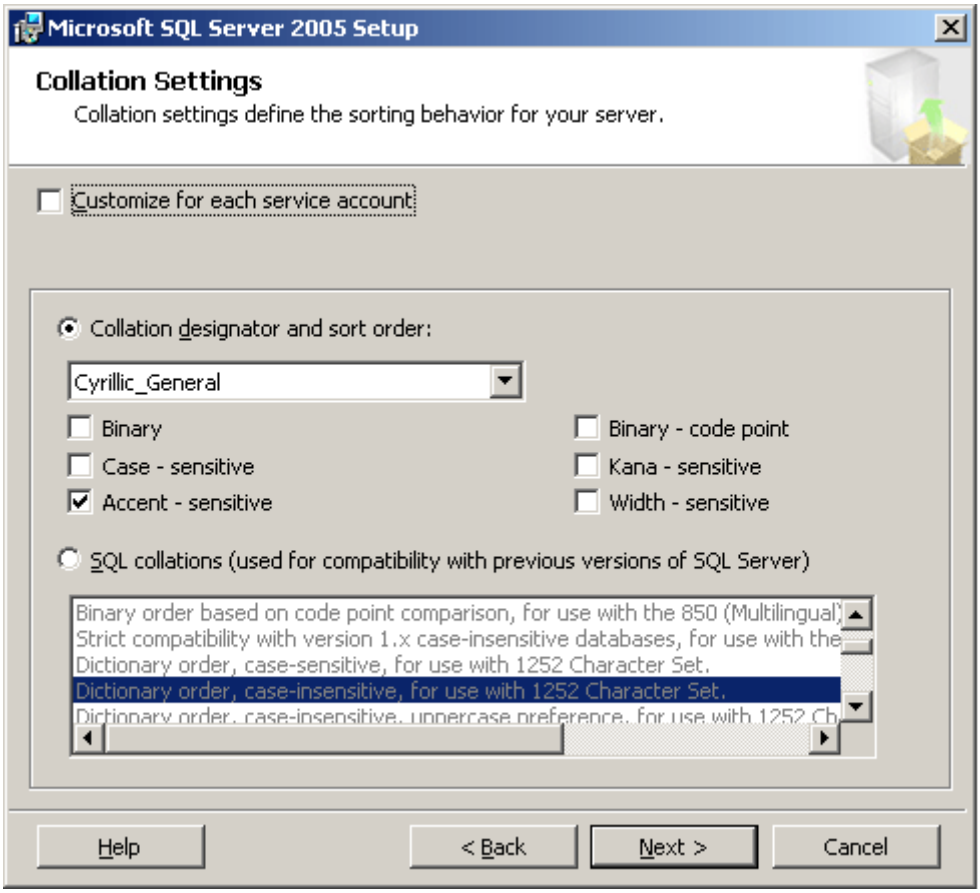

Рисунок 2.11

11. Выбрать действие, которое будет совершаться при возникновении критических ошибок (необязательно) (см. рисунок 2.12). Нажать `Next>` (Далее).

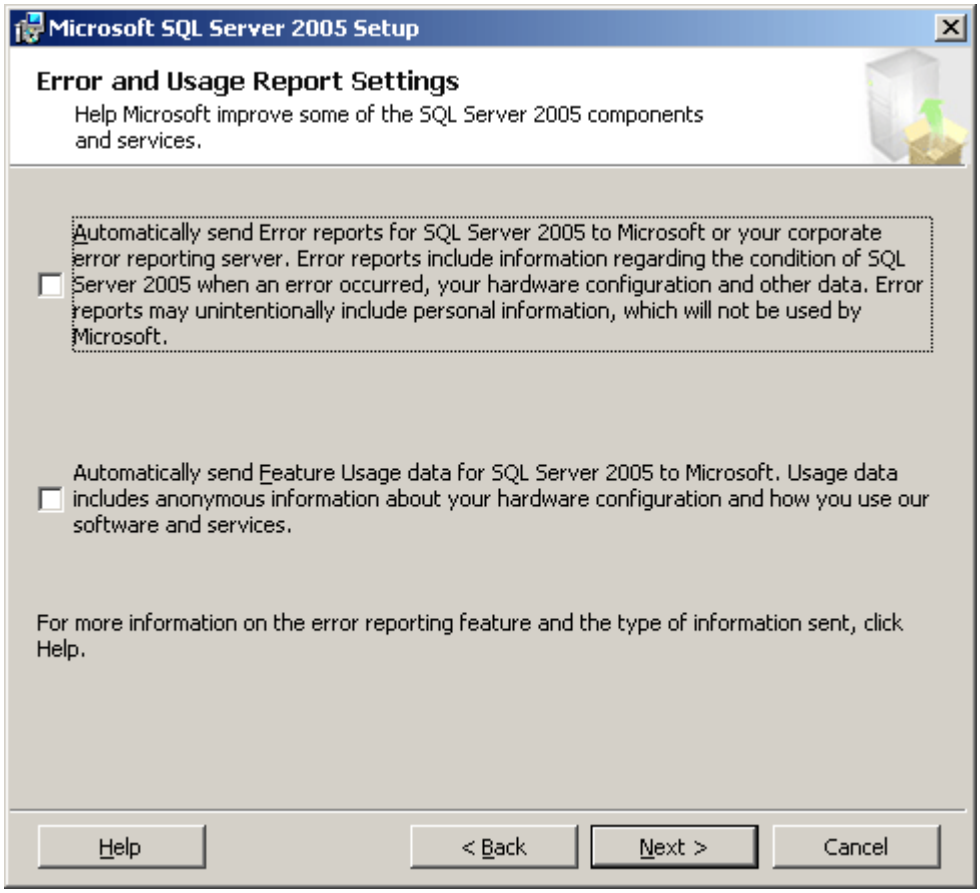

Рисунок 2.12

12. Для продолжения установки нажать `Install>` (Установка) (см. рисунок 2.13).

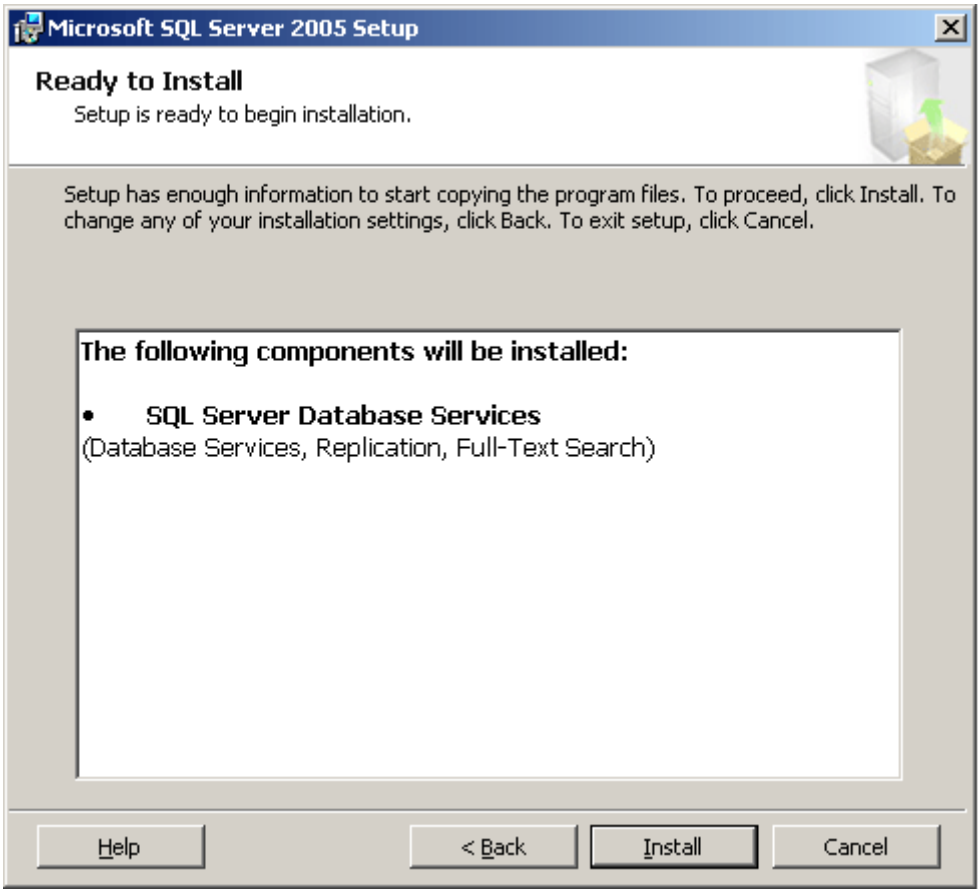

Рисунок 2.13

13. Для завершения установки СУБД Microsoft® SQL Server™ 2005 нажать `Finish>` (Закончить) и мастер завершит свою работу (см. рисунок 2.14).

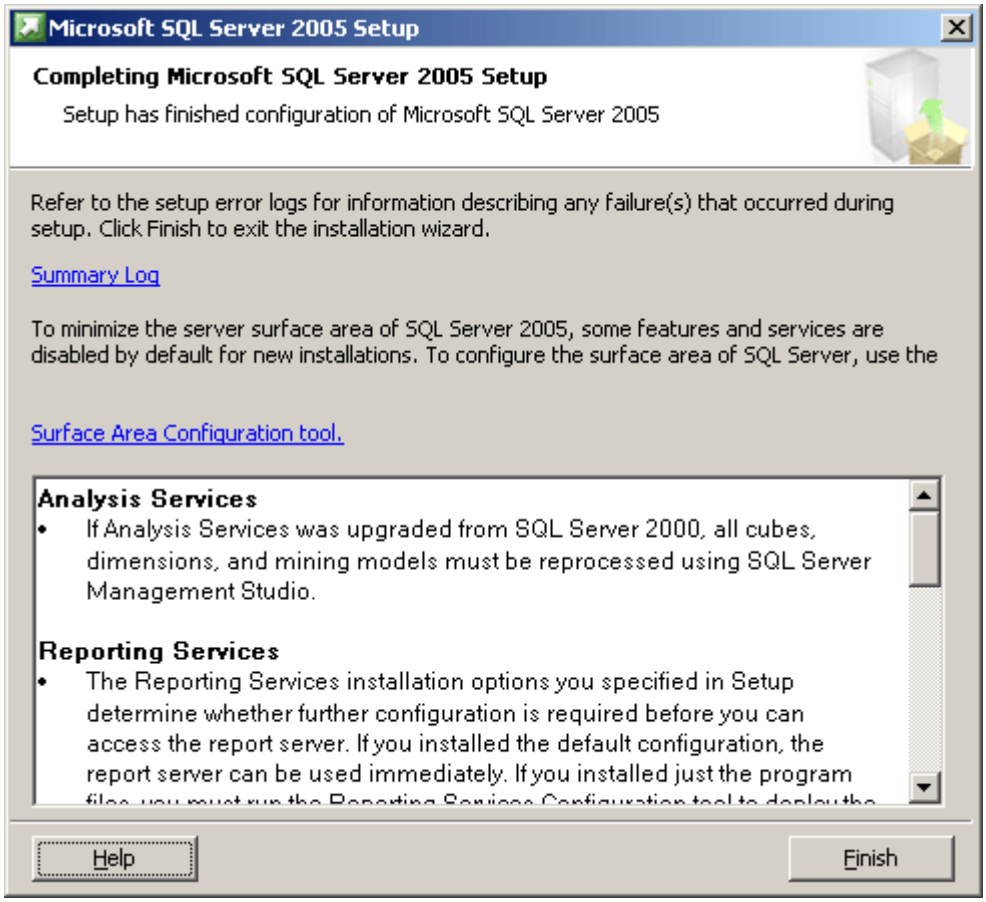

Рисунок 2.14

14. По окончании процесса установки СУБД Microsoft® SQL Server™ 2005 проанализировать журнал регистрации ошибок (`%windir%\Setup.log`) и журнал «Приложение» операционной системы на предмет возможных ошибок, которые могли возникнуть на этапе установки СУБД.

2.3 Настройка параметров безопасности сертифицированной версии операционной системы семейства Microsoft® Windows Server™ 2003

2.3.1 Общие указания

Для реализации политики безопасности, соответствующей оцененной на этапе сертификационных испытаний конфигурации СУБД Microsoft® SQL Server™ 2005, администратор эксплуатирующей организации может настроить параметры безопасности сертифицированной версии ОС семейства Microsoft® Windows Server™ 2003 самостоятельно, либо (что является более предпочтительным) использовать предопределенные значения параметров безопасности, представленные в файле шаблона безопасности, размещенного на компакт-диске, входящем в комплект поставки сертифицированной версии системы

управления базами данных Microsoft® SQL Server™ 2005. Использование шаблонов безопасности позволяет упростить выполнение задач администрирования, поскольку обеспечивает централизованное приведение к единой конфигурации безопасности заданного множества компьютеров в рамках одного домена, выступающих в роли серверов БД.

По умолчанию, на компьютерах для хранения шаблонов безопасности используется папка `%SystemRoot%\security\templates`. Данная папка не реплицируется между контроллерами домена. Таким образом, во избежание возникновения проблем с управлением версиями шаблона безопасности, должно быть определено место для организации централизованного хранения оригинала шаблона (как правило, для этой цели используется какой-либо из контроллеров домена или выделенный файловый сервер). Оптимальной является практика, когда изменения всегда вносятся в одну и ту же копию шаблона безопасности. Оригинальную копию шаблонов безопасности необходимо хранить в защищенном от несанкционированного доступа месте, доступ к которому предоставляется только администраторам.

Настройку параметров безопасности компьютера, выполняющего роль сервера БД под управлением СУБД Microsoft® SQL Server™ 2005 и включенного в состав домена Active Directory, необходимо осуществлять через использование групповых политик, применяемых на уровне организационных подразделений (контейнеров, содержащих учетные записи компьютеров – серверов БД), что позволит всем компьютерам, на которые распространяется групповая политика, автоматически применить единую конфигурацию безопасности, описанную с помощью соответствующих шаблонов безопасности.

Альтернативой централизованному применению групповой политики является настройка каждого компьютера вручную с использованием локальной политики безопасности.

Таким образом, в зависимости от режимов функционирования компьютера (в автономном режиме или в составе домена Active Directory) шаблоны безопасности необходимо применять либо непосредственно на компьютере (к локальному объекту групповой политики), либо на контроллере домена (к объектам групповой политики, базируемым на Active Directory).

2.3.2 Порядок применения групповой политики для компьютеров, являющихся членами домена Active Directory

Порядок применения объектов групповой политики строго иерархичен и по умолчанию предусматривает наследование от структурных объектов Active Directory

высокого уровня к объектам более низкого уровня. Групповые политики применяются в следующем порядке:

1. **Local group policy** – локальная политика безопасности;
2. **Site-level group policies** – групповые политики, применяемые на уровне сайта (область вычислительной сети, обеспечивающей объединение контроллеров домена высокоскоростными и надежными каналами связи);
3. **Domain-level group policies** - групповые политики, применяемые на уровне домена Active Directory;
4. **OU-level group policies** – групповые политики уровня организационного подразделения (ОП - это контейнер, используемый для объединения объектов домена в логические административные группы).

Применению групповой политики, содержащей параметры безопасности, соответствующие сертифицированной конфигурации СУБД Microsoft® SQL Server™ 2005 должно предшествовать выполнение ряда подготовительных операций, а именно:

- создание организационного подразделения, содержащего учетные записи компьютеров под управлением операционной системы семейства Microsoft® Windows Server™ 2003 с установленной СУБД Microsoft® SQL Server™ 2005;
- создание объекта групповой политики (ОГП);
- осуществление привязки созданного ОГП к организационному подразделению;
- импортирование в объект групповой политики шаблона безопасности, содержащего установленные значения параметров безопасности для сертифицированной конфигурации, учитывающие особенности, связанные с выполнением компьютером роли сервера БД (см. рисунок 2.15).

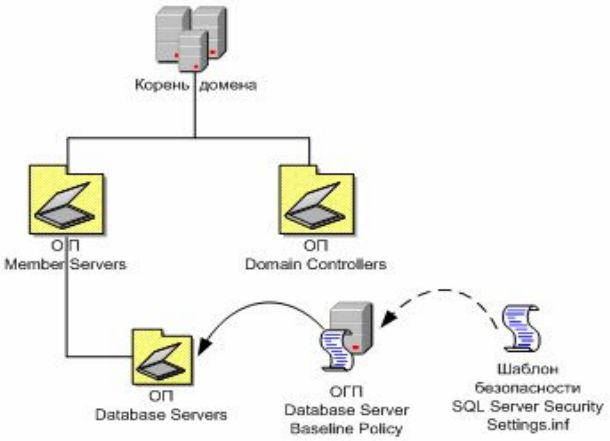

Рисунок 2.15 – Иерархия ОП и применяемых ОГП

2.3.3 Настройка сервера БД под управлением СУБД Microsoft® SQL Server™ 2005, включенного в состав домена Active Directory

Используемые шаблоны безопасности

Для автоматической настройки параметров политики безопасности, учитывающей особенности, связанные с выполнением компьютером роли сервера БД под управлением СУБД Microsoft® SQL Server™ 2005, следует импортировать шаблон безопасности `SQL Server Security Settings.inf` в объект групповой политики, определяемый на уровне отдельного организационного подразделения, содержащего учетные записи компьютеров, реализующих данную роль.

Порядок применения шаблонов безопасности

Импорт шаблона безопасности `SQL Server Security Settings.inf` необходимо осуществлять с использованием редактора объекта групповой политики, определяемого на уровне организационного подразделения ОП, содержащего учетные записи серверов БД под управлением СУБД Microsoft® SQL Server™ 2005. Чтобы импортировать шаблон безопасности в объект групповой политики необходимо выполнить следующие действия:

1. Нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `dsa.msc` и нажать «ОК».

2. В появившемся окне оснастки консоли управления «Active Directory – пользователи и компьютеры» выделить имя организационного подразделения (например, `Database Servers`) и посредством пункта «Свойства» контекстного меню получить доступ к диалоговому окну свойств указанного ОП. Далее, перейти на вкладку «Групповая политика».

3. В случае если на уровне организационного подразделения групповая политика не определена, необходимо создать новый объект групповой политики и привязать его к соответствующему организационному подразделению. Для этого в окне свойств соответствующего организационного подразделения на вкладке «Групповая политика» нажать «Создать» и ввести имя нового объекта групповой политики (см. рисунок 2.16).

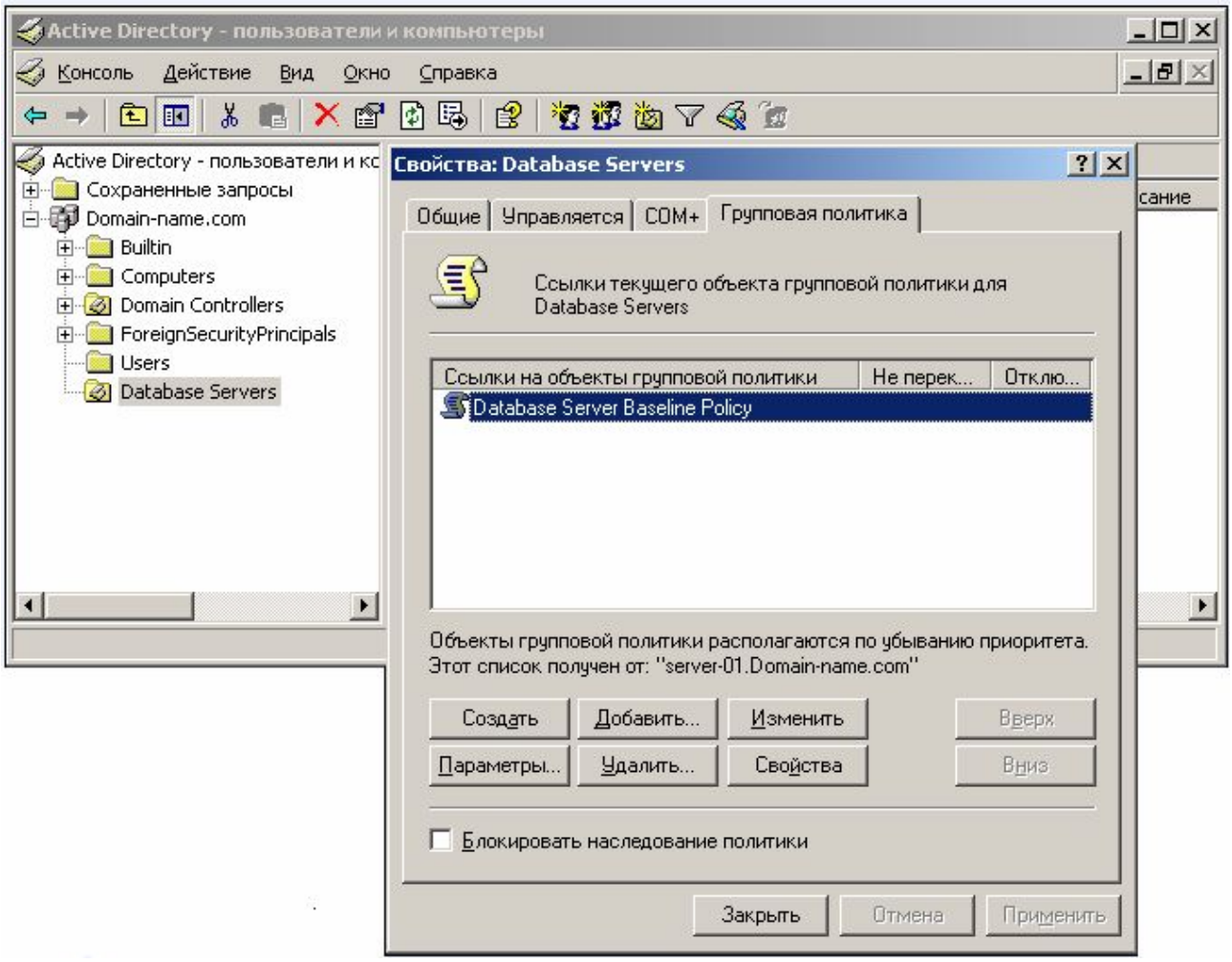

Рисунок 2.16

Для указанного объекта групповой политики должен быть применен параметр принудительного наследования «Не перекрывать: другие объекты групповой политики не могут перекрывать параметры этой политики», что не позволит ОГП, определяемых на более низких уровнях иерархии ОП, переопределять заданные данной групповой политикой параметры безопасности.

4. Вызвать редактор объектов групповой политики (Group Policy Object Editor). Для этого необходимо выделить требуемый объект групповой политики (в частности, «Database Server Baseline Policy») и нажать «Изменить».

5. В окне редактора объектов групповой политики выбрать узел «Конфигурация компьютера» и перейти к разделу «Конфигурация Windows».

6. Выделить папку «Параметры безопасности».

7. Посредством контекстного меню выбрать пункт «Импорт политики».

8. В появившемся диалоговом окне импорта политики выбрать шаблон безопасности SQL Server Security Settings.inf и нажать «Открыть». После чего

параметры безопасности импортируются из выбранного файла в текущий объект групповой политики (см. рисунок 2.17).

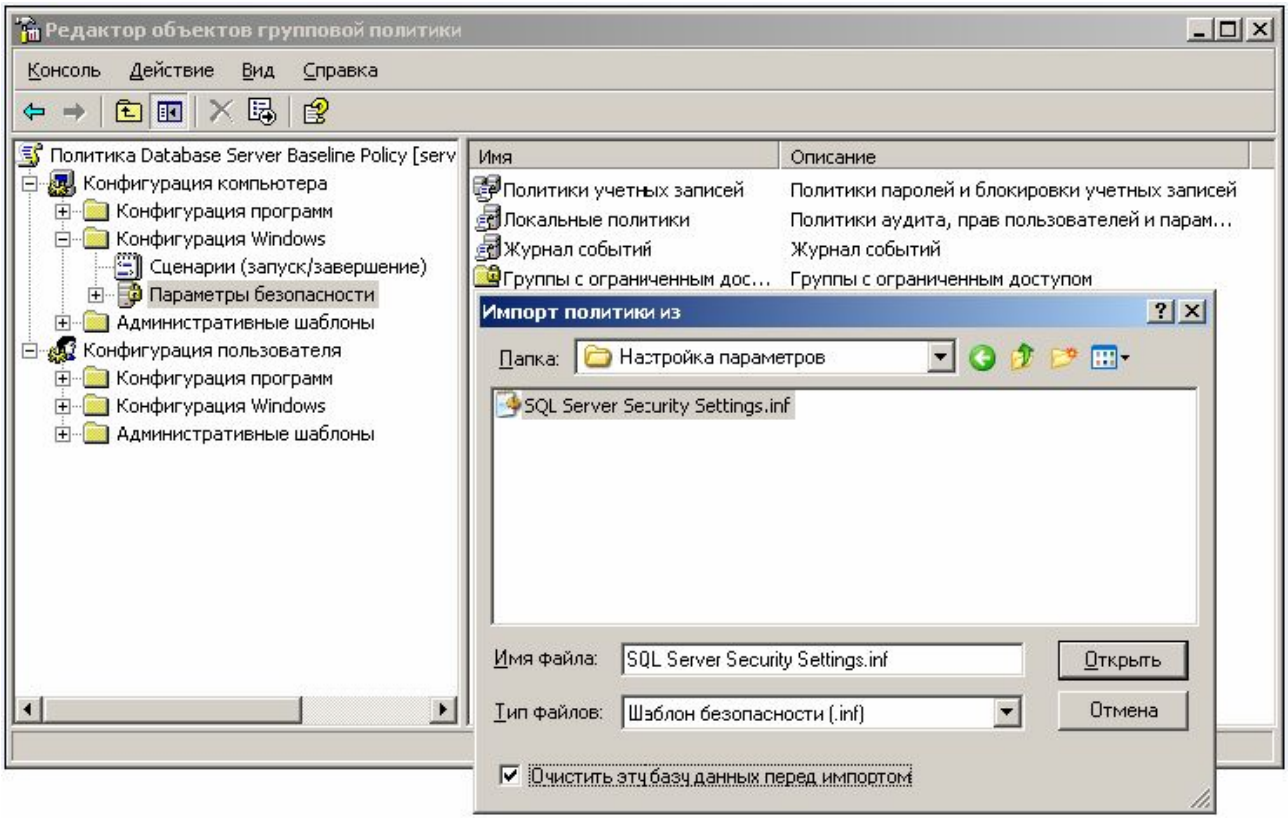

Рисунок 2.17

9. Закрыть редактор групповой политики.

10. В командной строке выполнить команду `gpudate.exe /force`, позволяющую осуществить принудительную репликацию и обновление измененной политики безопасности (см. рисунок 2.18).

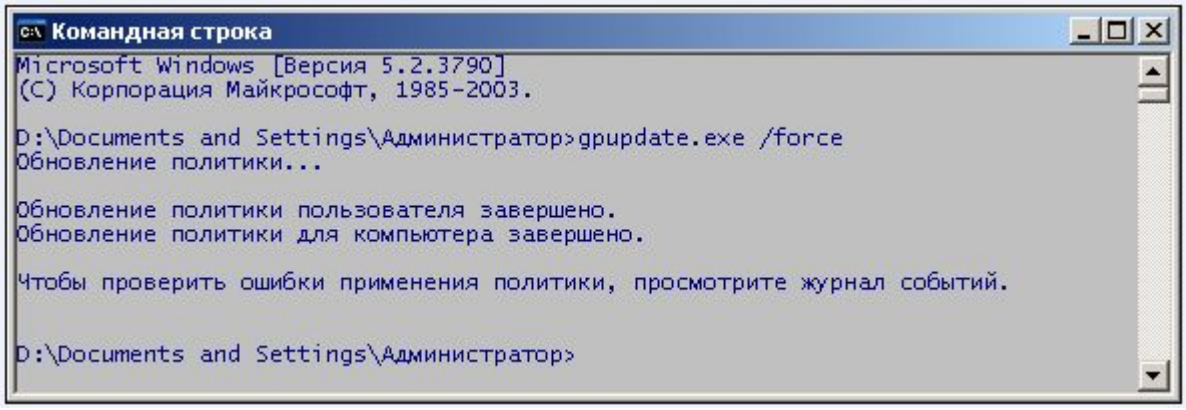

Рисунок 2.18

11. Проанализировать журнал регистрации событий «Приложение» операционной системы на предмет наличия ошибок, которые могли возникнуть на этапе репликации или

обновления политики безопасности. В случае успешного применения политики безопасности в объекте групповой политики в журнале «Приложение» должно быть зарегистрировано событие с кодом `ID:1704` (см. рисунок 2.19).

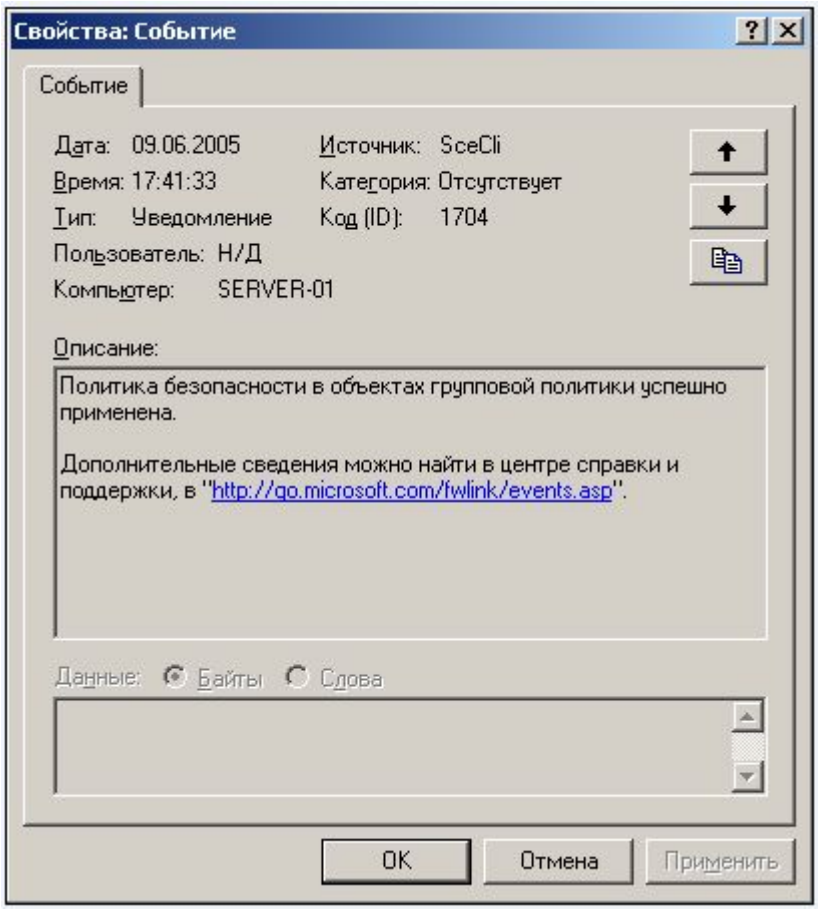

Рисунок 2.19

При назначении политики на уровне организационного подразделения необходимо убедиться, что в списке управления доступом ACL соответствующего объекта групповой политики для пользователей и компьютеров домена, выступающих в роли серверов БД, определены разрешения «Чтение» и «Применение групповой политики». Если в списке управления доступом не будут определены требуемые значения, политика безопасности к указанным субъектам применена не будет.

2.3.4 Настройка автономного сервера БД под управлением СУБД Microsoft® SQL Server™ 2005

Используемые шаблоны безопасности

С целью обеспечения требуемого уровня безопасности, необходимого для обработки конфиденциальной информации, автономные компьютеры, выполняющие роль серверов БД

под управлением СУБД Microsoft® SQL Server™ 2005 должны быть настроены в соответствии с требуемой конфигурацией безопасности. Для приведения указанных компьютеров в соответствующую конфигурацию, администратор должен обеспечить применение параметров безопасности, определенных в шаблоне `SQL Server Security Settings.inf`, к локальной политике безопасности.

Таким образом, для настройки параметров безопасности автономного компьютера, выступающего в роли сервера БД, необходимо выполнить импорт шаблона безопасности `SQL Server Security Settings.inf` в локальный объект групповой политики.

Порядок применения шаблонов безопасности

Импорт шаблона безопасности `SQL Server Security Settings.inf` можно осуществлять как с использованием графического интерфейса Windows (оснастки консоли управления «Анализ и настройка безопасности»), так и с использованием инструментального средства командной строки `Secedit.exe`.

Импорт шаблона безопасности с использованием графического интерфейса Windows

Для импортирования шаблона безопасности `SQL Server Security Settings.inf` необходимо выполнить следующие действия:

1. Открыть оснастку консоли управления «Анализ и настройка безопасности». Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `mmc` и нажать «ОК». В окне консоли управления MMC (Microsoft Management Console) посредством пункта меню «Добавить или удалить оснастку…» добавить изолированную оснастку «Анализ и настройка безопасности» (см. рисунок 2.20).

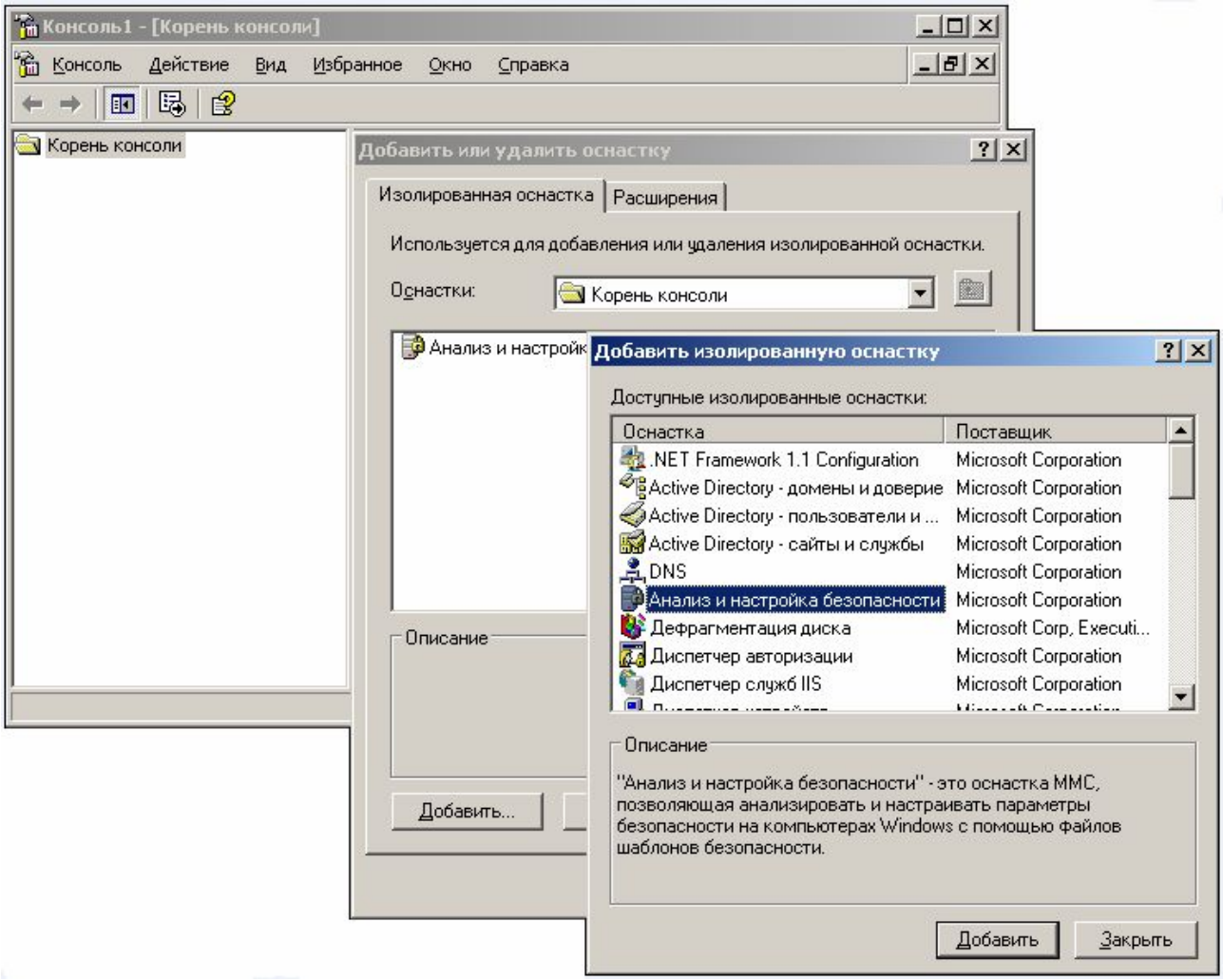

Рисунок 2.20

2. В дереве имен консоли посредством нажатия правой кнопкой мыши узла «Анализ и настройка безопасности» выбрать команду «Открыть базу данных».

3. В диалоговом окне «Открыть базу данных» выполнить одно из следующих действий (см. рисунок 2.21):

– создать новую базу данных анализа. Для этого необходимо ввести новое имя в поле «Имя файла» и нажать «Открыть». При открытии новой базы данных в диалоговом окне «Импорт шаблона» выбрать импортируемый шаблон безопасности `SQL Server Security Settings.inf` и нажать «Открыть»;
– открыть существующую базу данных анализа. Для этого необходимо выделить имя базы данных и нажать «Открыть».

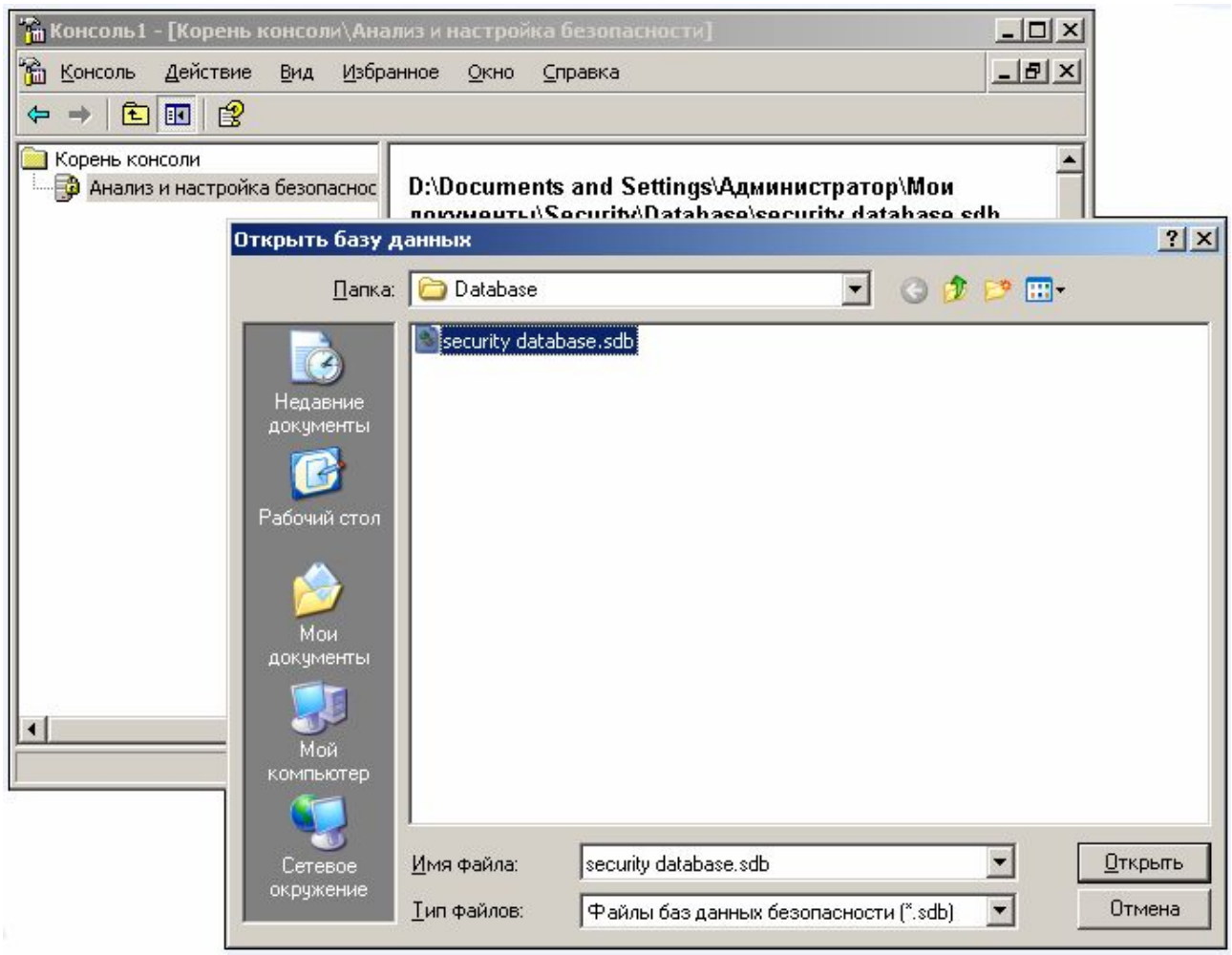

Рисунок 2.21

4. Импортировать шаблон безопасности `SQL Server Security Settings.inf`, определяющий требуемые параметры политики безопасности. Для этого в диалоговом окне консоли «Анализ и настройка безопасности» выбрать пункт меню «Действие» и далее «Импорт шаблона». При импортировании шаблона безопасности администратором должны быть учтены следующие аспекты:

– в случае использования существующей базы данных анализа, при импортировании в нее нового шаблона безопасности в диалоговом окне «Импорт шаблона» необходимо выбрать опцию «`Очистить эту базу данных перед импортом`», что приведет к перезаписи всех шаблонов, хранящихся в базе данных, импортируемым шаблоном. Если данная опция снята, импортируемый шаблон безопасности будет объединен с сохраненными шаблонами, и в базе данных будет храниться составной шаблон безопасности (см. рисунок 2.22);

– в случае использования новой базы данных при импортировании шаблона безопасности опция «Очистить эту базу данных перед импортом» может быть отключена.

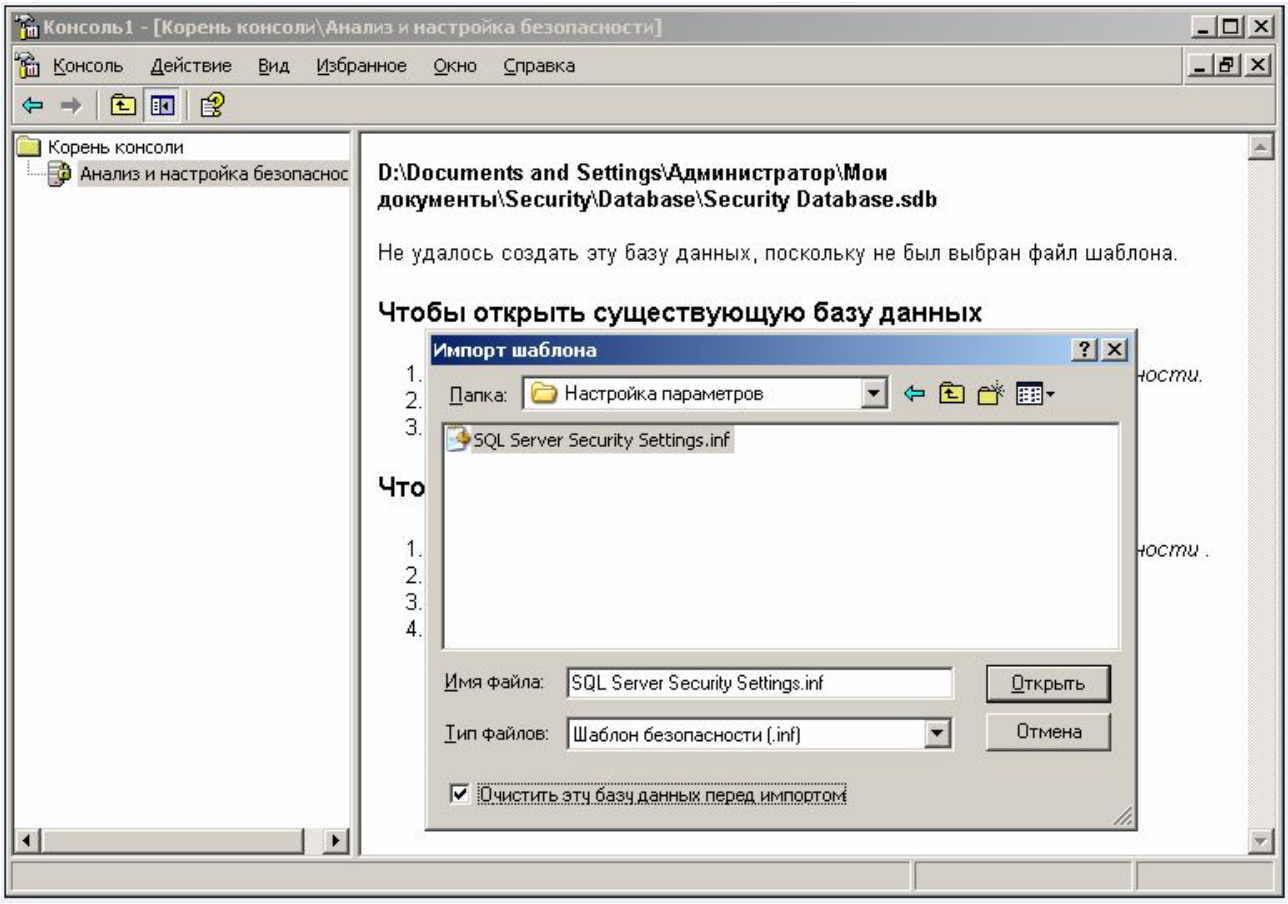

Рисунок 2.22

5. Посредством нажатия правой кнопкой мыши узла «Анализ и настройка безопасности» выбрать команду «Настроить компьютер» (см. рисунок 2.23).

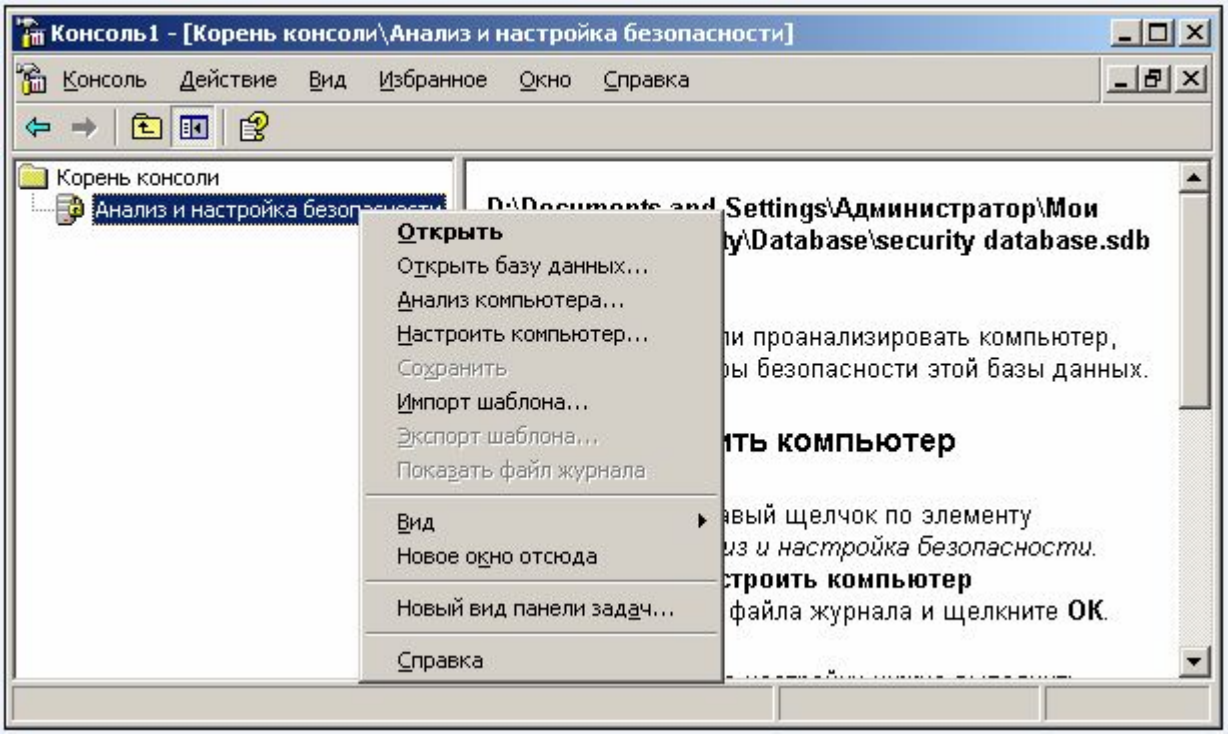

Рисунок 2.23

6. Выполнить одно из следующих действий:
   - при использовании стандартного журнала ошибок в группе «Путь файла журнала ошибок» нажать «ОК» (см. рисунок 2.24);
   - для выбора другого журнала ввести в поле «Путь файла журнала ошибок» допустимый путь и имя файла.

Рисунок 2.24

7. Проанализировать содержимое журнала регистрации событий на предмет наличия ошибок, возникших на этапе применение шаблона безопасности к локальной политики безопасности.

8. Закрыть оснастку «Анализ и настройка безопасности».

Импорт шаблона безопасности с использованием командной строки

Администратор имеет возможность настроить параметры безопасности в соответствии с требуемой конфигурацией, запустив файл командного сценария, входящего в комплект поставки сертифицированной версии СУБД Microsoft® SQL Server™ 2005.

Для автоматической настройки параметров безопасности сертифицированной версии операционной системы семейства Microsoft® Windows Server™ 2003 необходимо осуществить запуск файла командного сценария `Configure Stand-Alone SQL Server.cmd`, осуществляющего импорт шаблона безопасности `SQL Server Security Settings.inf` и применение его к локальному объекту групповой политики.

2.3.5 Настройка разрешений доступа файловой системы NTFS и параметров безопасности реестра

По окончании установки сертифицированной версии СУБД Microsoft® SQL Server™ 2005 администратором эксплуатирующей организации должны быть выполнена дополнительная настройка сертифицированной версии ОС семейства Microsoft® Windows Server™ 2003 в части определения рекомендуемых значений разрешений доступа к программным файлам и файлам БД и параметров безопасности реестра.

Рекомендуемые к установке разрешения доступа к программным файлам и файлам БД системы управления базами данных Microsoft® SQL Server™ 2005 представлены в таблице 2.2.

Таблица 2.2 - Параметры безопасности файловой системы

Папка или файл	Группа пользователей	Разрешения	Область применения
Каталог, содержащий программные файлы СУБД (например, c:\Program Files\ Microsoft SQL Server)	Администраторы	Полный доступ	Папка, ее подпапки и файлы
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Полный доступ	Папка, ее подпапки и файлы

Папка или файл	Группа пользователей	Разрешения	Область применения
%SystemDrive% (Диск, на котором установлена операционная система)	Администраторы	Полный доступ	Папка, ее подпапки и файлы
	Создатель-владелец	Полный доступ	Только подпапки и файлы
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы
Каталог, содержащий файлы данных БД (например, d:\ MSSQL\Data)	Администраторы	Полный доступ	Папка, ее подпапки и файлы
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Полный доступ	Папка, ее подпапки и файлы
%SystemRoot%\ System32	Администраторы	Полный доступ	Папка, ее подпапки и файлы
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы
	Прошедшие проверку	Чтение и выполнение	Папка, ее подпапки и файлы

В общем случае настройка разграничения доступа пользователей и обслуживающего персонала к информационным ресурсам системы осуществляется в следующей последовательности:

– посредством контекстного меню необходимо получить доступ к диалоговому окну свойств защищаемого информационного ресурса (файла или папки) и перейти на вкладку «Безопасность» (см. рисунок 2.25);

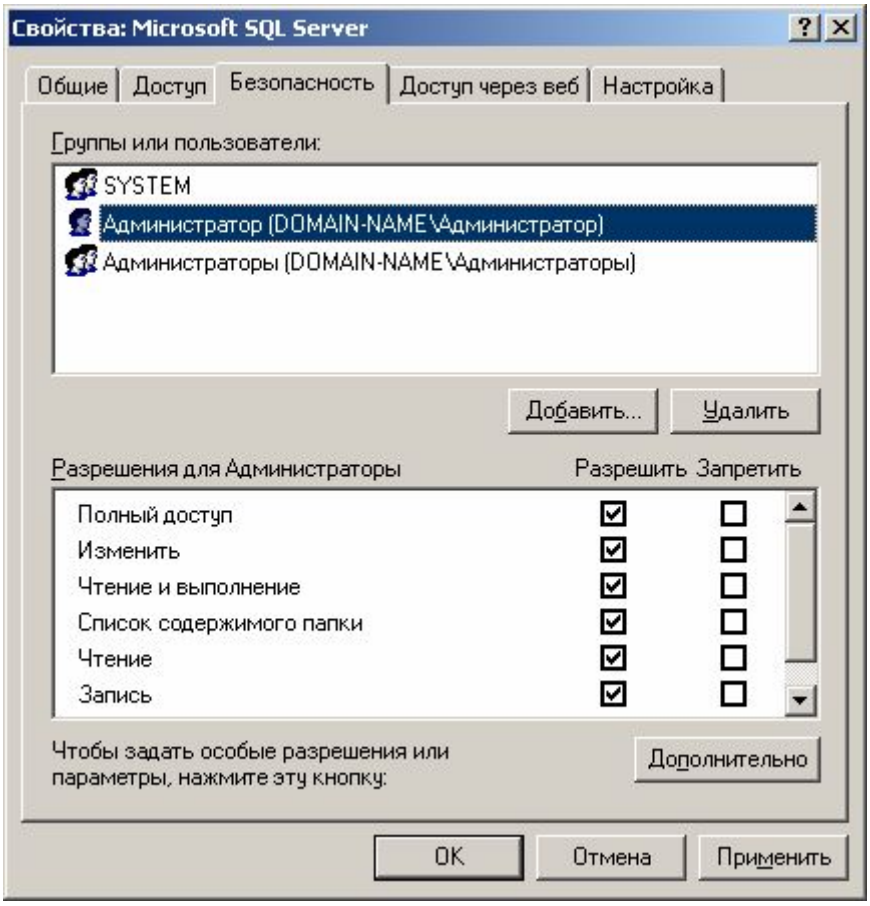

Рисунок 2.25

– через кнопку «Добавить…» выбрать пользователей или группы пользователей (субъектов доступа), которым необходимо запретить или предоставить разрешения на доступ к данному ресурсу (объекту доступа) (см. рисунок 2.26):

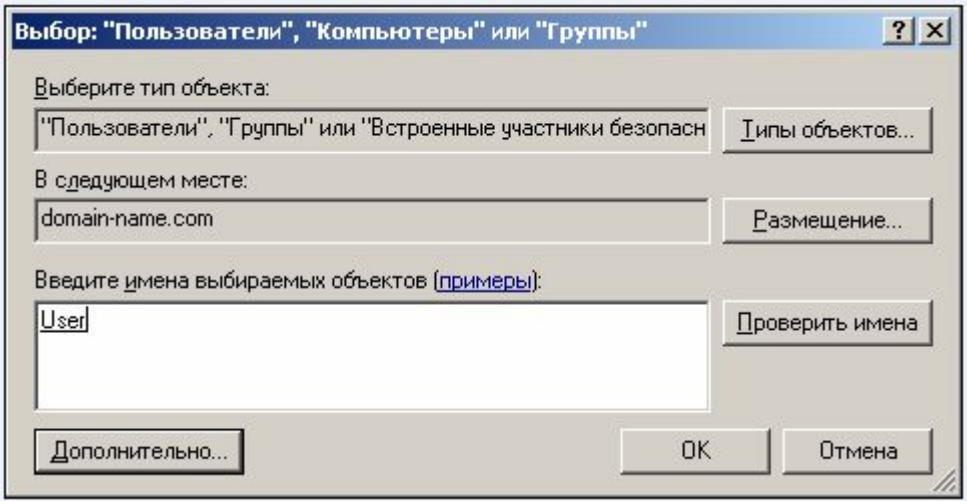

Рисунок 2.26

– в окне списка разрешений, установить или снять соответствующий флажок, чтобы явно разрешить или запретить доступ к ресурсу выбранным

пользователям или группам пользователей. С целью более гибкой настройки разрешений на доступ к контролируемому ресурсу через кнопку «Дополнительно» окна свойств файла или каталога получить доступ к окну настройки дополнительных параметров безопасности (см. рисунок 2.27). Через кнопку «Изменить…» получить доступ к диалоговому окну «Элемент разрешений для…» и установить требуемые разрешения доступа для выбранных субъектов (см. рисунок 2.28).

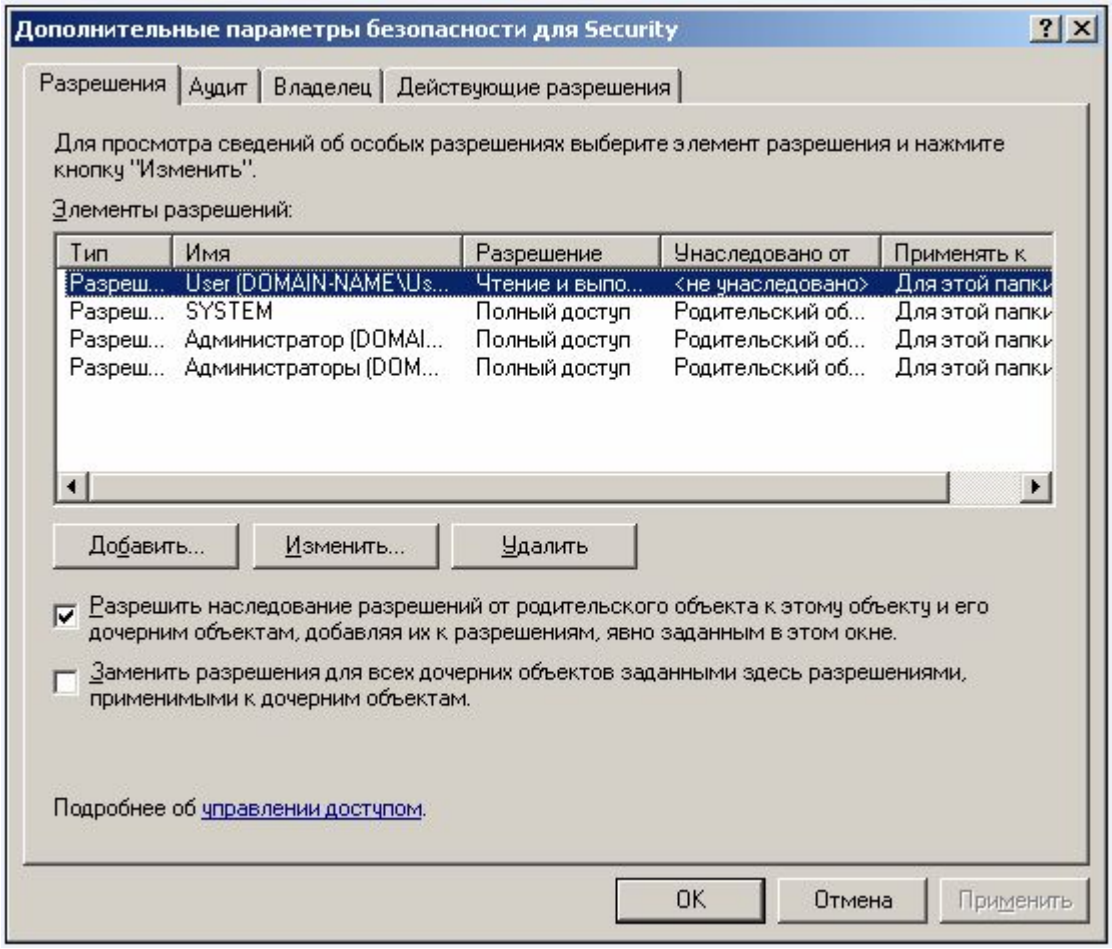

Рисунок 2.27

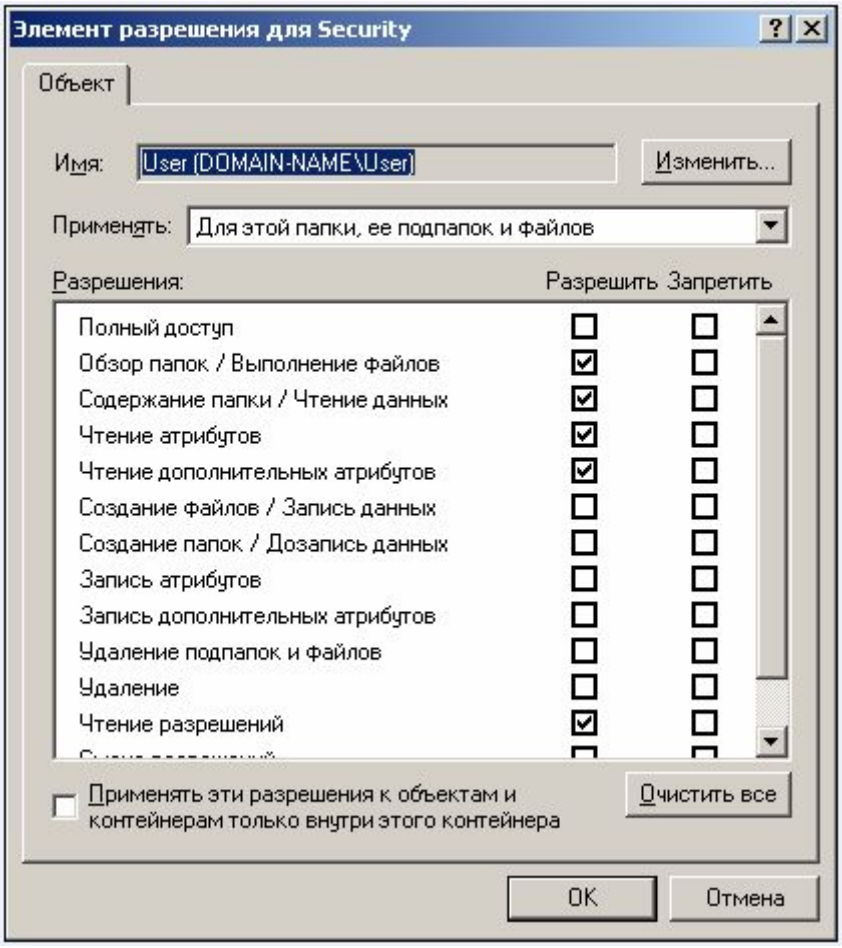

Рисунок 2.28

Рекомендуемые значения параметров безопасности разделов реестра сертифицированной версии операционной системы семейства Microsoft® Windows® Server 2003™, относящихся к сертифицированной версии СУБД Microsoft® SQL Server™ 2005, представлены в таблице 2.3.

Таблица 2.3 – Параметры безопасности разделов реестра

Раздел реестра	Группа пользователей	Разрешения доступа
HKLM\Software\Microsoft\ MSSQLServer	SYSTEM	Полный доступ
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Запрос значения Задание значения Создание подраздела Перечисление подразделов Уведомление Чтение разрешений

Раздел реестра	Группа пользователей	Разрешения доступа
HKLM \Software\Microsoft\ WindowsNT\CurrentVersion\Perflib	SYSTEM	Полный доступ
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Запрос значения Задание значения Создание подраздела Перечисление подразделов Уведомление Чтение разрешений
HKLM\Software\Microsoft\ Microsoft SQL Server\ $Instance-Name (где $InstanceName – имя экземпляра SQL Server)	SYSTEM	Полный доступ
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Запрос значения Перечисление подразделов Уведомление Чтение разрешений
HKLM\System\CurrentControlSet\ Services\SQLSERVERAGENT	SYSTEM	Полный доступ
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Запрос значения Перечисление подразделов Уведомление Чтение разрешений
HKLM\System\CurrentControlSet\ Services\SQLAgent$InstanceName (где $InstanceName – имя экземпляра SQL Server)	SYSTEM	Полный доступ
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Запрос значения Перечисление подразделов Уведомление Чтение разрешений
HKLM\System\CurrentControlSet\ Services\MSSQLServer	SYSTEM	Полный доступ
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Запрос значения Перечисление подразделов Уведомление Чтение разрешений

Раздел реестра	Группа пользователей	Разрешения доступа
HKLM\System\CurrentControlSet\Services\MSSQL\$InstanceName (где $InstanceName – имя экземпляра SQL Server)	SYSTEM	Полный доступ
	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent	Запрос значения Перечисление подразделов Уведомление Чтение разрешений

В общем случае порядок настройки разрешений доступа пользователей к защищаемым разделам реестра эквивалентен порядку определения разрешений доступа к объектам файловой системе NTFS (файлам и папкам).

2.4 Общие указания по настройке параметров безопасности сертифицированной версии СУБД Microsoft® SQL Server™ 2005

По окончании настройки параметров безопасности сертифицированной версии операционной системы семейства Microsoft® Windows Server™ 2003, под управлением которой функционирует сервер баз данных, администратором должна быть выполнена настройка параметров безопасности непосредственно самой СУБД Microsoft® SQL Server™ 2005, а именно:

- режима проверки подлинности пользователей;
- уровня аудита событий доступа к SQL Server;
- порядка использования хранимых процедур.

Определение режима проверки подлинности пользователей и уровня аудита событий доступа к SQL Server может осуществляться с использованием графического интерфейса администрирования СУБД или встроенной хранимой процедуры `xp_instance_regwrite`.

Для определение режима проверки подлинности пользователей средствами Windows и аудита всех (успешных и неудачных) событий доступа с использованием графического интерфейса администрирования необходимо выполнить следующие действия:

- вызвать графическую утилиту администрирования «SQL Server Management Studio». Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Все программы», «Microsoft SQL Server 2005» и далее оснастку консоли управления «SQL Server Management Studio»;

– в окне консоли «SQL Server Management Studio» выделить требуемый экземпляр СУБД Microsoft® SQL Server™ 2005 и посредством пункта «Properties» (Свойства) контекстного меню вызвать диалоговое окно его свойств;
– в левой части окна выбрать страницу (Select a page) Security (Безопасность);
– в разделе Server authentication (Режим проверки подлинности) выбрать опцию Windows Authentication mode;
– в разделе Login auditing (Уровень аудита) выбрать опцию Both failed and successful logins, определяющую необходимость регистрации в журнале аудита операционной системы (журнале «Приложение») всех (успешных и неудачных) событий доступа (см. рисунок 2.29);

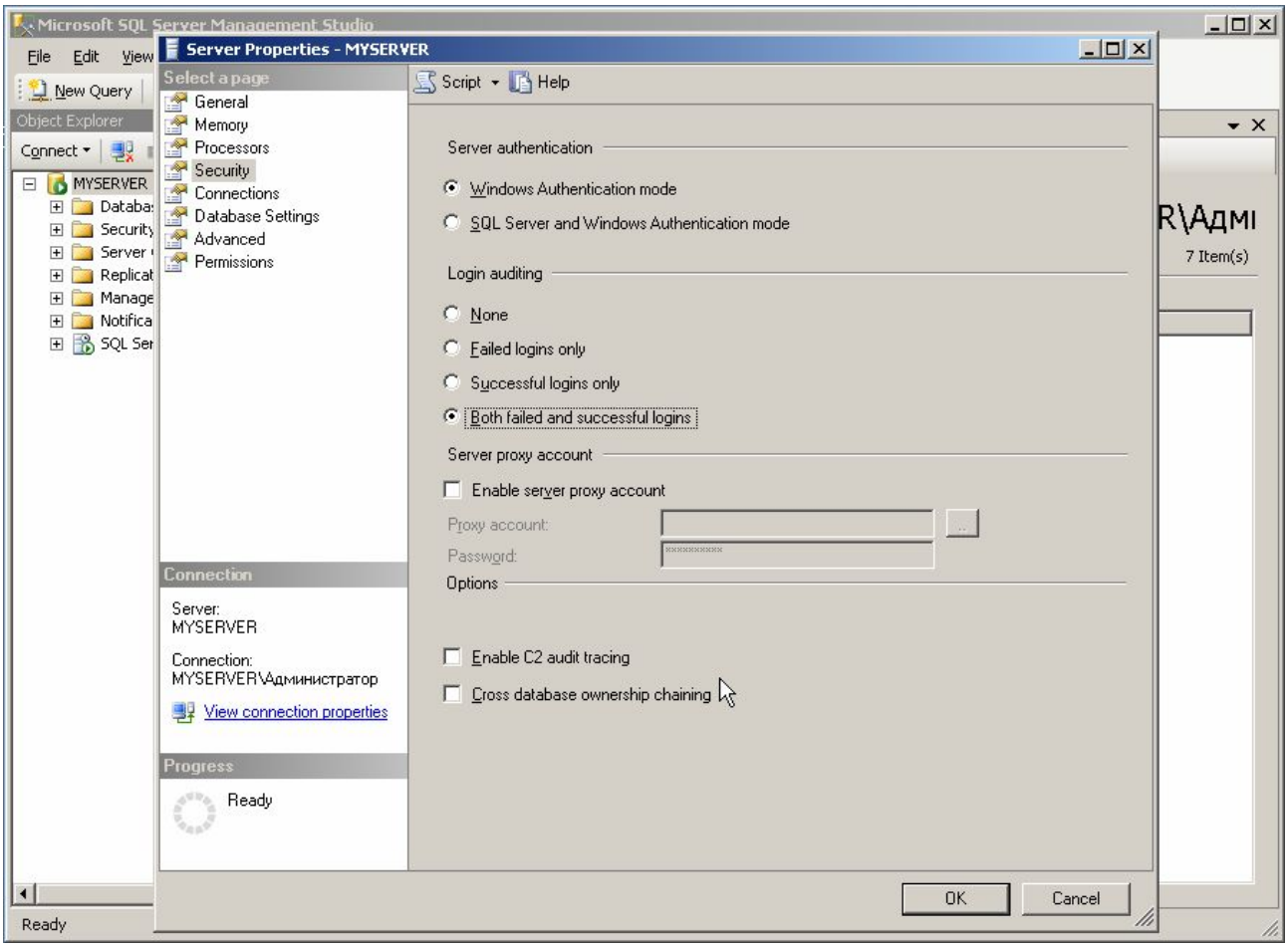

Рисунок 2.29

– нажать кнопку «OK» с целью вступления сделанных изменений в силу. При этом служба SQL Server перезапустится.

Для определение режима проверки подлинности пользователей и аудита всех (успешных и неудачных) событий доступа с использованием расширенной хранимой

процедуры `xp_instance_regwrite` необходимо выполнить следующие действия (представленные SQL-запросы продемонстрированы на примере экземпляра Microsoft® SQL Server™ 2005 Standard Edition по умолчанию. В случае использования именованных экземпляров их необходимо изменить):

- в уже открытом окне консоли «SQL Server Management Studio» выбрать пункт меню «`File/New/Query with current connection`;
- с целью задания режима проверки подлинности пользователей только средствами Windows (Windows only) в появившемся поле редактора запросов создать и выполнить следующий запрос:

  `Master..xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer',N'LoginMode', REG_DWORD,1`
- с целью задания требования аудита всех событий доступа в поле редактора запросов создать и выполнить следующий запрос:

  `Master..xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer',N'AuditLevel', REG_DWORD,3`
- для вступления сделанных изменений в силу выполнить останов и последующий старт службы SQL Server.

Хранимые процедуры представляют собой набор команд SQL, скомпилированных в один план выполнения и хранимых на сервере БД. Таким образом, вместо того, чтобы хранить часто используемый запрос, клиенты получают возможность ссылаться на соответствующую хранимую процедуру. Это позволяет обеспечить лучшую производительность, поскольку данный запрос будет анализироваться только однажды, и уменьшить трафик между клиентом и сервером БД.

Хранимые процедуру используются для работы с таблицами, оптимизации производительности, получения системной информации, регулирования прав доступа и выполнения задач по администрированию БД.

Преимущество использования хранимых процедур заключается в том, что пользователю для доступа к данным и их модификации необходимы только разрешения на выполнение хранимой процедуры и не нужны права доступа к таблицам и представлениям, к которым осуществляется обращение из данной хранимой процедуры. Такой подход позволяет обеспечить разграничение доступа пользователей к таблицам и представлениям, к

которым происходит обращение из хранимой процедуры, без непосредственного определения для них прав доступа.

Наряду с очевидными преимуществами, связанными с применением хранимых процедур, существует ряд недостатков, заключающихся в возможной, или точнее существующей вероятности, некорректной реализации самих процедур и ошибок программирования, что создает предпосылки к реализации злоумышленником атак типа «внедрение SQL-кода» (injecting SQL code).

Помимо хранимых процедур СУБД Microsoft® SQL Server™ 2005 включает ряд расширенных хранимых процедур, которые используют внешние динамически подключаемые библиотеки и предназначены для расширения функциональности СУБД Microsoft® SQL Server™ 2005 и повышения эффективности администрирования. Их применение также связано с потенциальной опасностью атак типа «внедрение SQL-кода».

Таким образом, администратором эксплуатирующей организации должны быть проанализированы все хранимые процедуры на предмет необходимости их использования. Те процедуры, в которых нет необходимости, должны быть удалены или, если это невозможно, запрещены к использованию.

Ниже представлен перечень хранимых процедур, которые рекомендуется удалить или запретить к использованию:

- sp_OACreate
- sp_OADestroy
- sp_OAGetErrorInfo
- sp_OAGetProperty
- sp_OAMethod
- sp_OASetProperty
- sp_OAStop
- xp_regaddmultistring
- xp_regdeletekey
- xp_regdeletevalue
- xp_regenumvalues
- xp_regremovemultistring
- sp_bindsession
- sp_cursor
- sp_cursorclose
- sp_replflush
- sp_replstatus
- sp_repltrans
- sp_sdidebug
- xp_availablemedia
- xp_cmdshell
- xp_deletemail
- xp_dirtree
- xp_dropwebtask
- xp_dsninfo
- xp_enumdsn
- xp_enumerrorlogs
- xp_enumgroups
- xp_enumqueuedtasks
- xp_eventlog
- xp_msver
- xp_perfend
- xp_perfmonitor
- xp_perfsample
- xp_perfstart
- xp_readerrorlog
- xp_readmail
- xp_revokelogin
- xp_runwebtask
- xp_schedulersignal
- xp_sendmail
- xp_servicecontrol
- xp_snmp_getstate
- xp_snmp_raisetrap
- xp_sprintf

- sp_cursorfetch
- sp_cursoropen
- sp_cursoroption
- sp_getbindtoken
- sp_GetMBCSCharLen
- sp_IsMBCSLeadByte
- sp_replcmds
- sp_replcounters
- sp_repldone
- xp_findnextmsg
- xp_fixeddrives
- xp_getfiledetails
- xp_getnetname
- xp_grantlogin
- xp_logevent
- xp_loginconfig
- xp_logininfo
- xp_makewebtask
- xp_sqlinventory
- xp_sqlregister
- xp_sqltrace
- xp_sscanf
- xp-startmail
- xp_stopmail
- xp_subdirs
- xp_unc_to_drive

3 Последовательность действий по контролю сертифицированной версии СУБД Microsoft® SQL Server™ 2005

3.1 Контроль маркирования сертифицированной версии СУБД Microsoft® SQL Server™ 2005

В данном разделе контроль маркирования сертифицированной версии СУБД Microsoft® SQL Server™ 2005 рассматривается на примере СУБД Microsoft® SQL Server™ 2005 Standard Edition.

Контроль маркирования сертифицированной версии системы управления базами данных Microsoft® SQL Server™ 2005 Standard Edition в совокупности с контролем исходного состояния, основанном на контрольном суммировании, направлен на получение удостоверения в том, что на компьютере установлена сертифицированная версия СУБД Microsoft® SQL Server™ 2005 Standard Edition.

Контроль маркирования проводится следующим образом:

1. Удостовериться, что на упаковочной коробке дистрибутива системы управления базами данных, установленной на компьютере, присутствует надпись «Microsoft® SQL Server™ 2005 Standard Edition».
2. Удостовериться, что упаковочная коробка дистрибутива системы управления базами данных, установленной на компьютере, маркирована знаком соответствия сертифицированной продукции.
3. Удостовериться, что на оптическом носителе дистрибутива системы управления базами данных, установленной на компьютере, присутствует надпись «Microsoft® SQL Server™ 2005 Standard Edition».

3.2 Порядок проверки соответствия текущих значений параметров безопасности значениям, установленным в шаблонах безопасности

Для проверки соответствия текущих параметров безопасности групповой политики параметрам безопасности, определенным в соответствующем шаблоне (соответствующих шаблонах) безопасности, необходимо выполнить анализ безопасности операционной системы семейства Microsoft® Windows Server™ 2003, под управлением которой функционирует СУБД Microsoft® SQL Server™ 2005. Анализ может осуществляться как с использованием графического интерфейса Windows (оснастки консоли управления «Анализ

и настройка безопасности»), так и с использованием инструментального средства командной строки `Secedit.exe`.

Анализ безопасности с использованием графического интерфейса Windows

Для анализа безопасности системы необходимо выполнить следующие действия:

1. Открыть оснастку консоли управления «Анализ и настройка безопасности». Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `mmc` и нажать «ОК». В окне консоли управления ММС посредством пункта меню «Добавить/удалить оснастку…» добавить изолированную оснастку «Анализ и настройка безопасности».

2. В дереве консоли посредством нажатия правой кнопкой мыши узла «Анализ и настройка безопасности» выбрать команду «Открыть базу данных».

3. В диалоговом окне «Открыть базу данных» выполнить одно из следующих действий:

   – создать новую базу данных анализа. Для этого необходимо ввести новое имя в поле «Имя файла» и нажать «Открыть». При открытии новой базы данных в диалоговом окне «Импорт шаблона» выбрать один из необходимых шаблонов безопасности и нажать кнопку «Открыть»;
   – открыть существующую базу данных анализа. Для этого необходимо выделить имя базы данных и нажать «Открыть».

4. Импортировать шаблон безопасности `SQL Server Security Settings.inf`, определяющий параметры политики безопасности ОС семейства Microsoft® Windows Server™ 2003. Для этого в диалоговом окне консоли управления «Анализ и настройка безопасности» выбрать пункт меню «Действие» и далее «Импорт шаблона». При импортировании шаблона безопасности администратором должны быть учтены следующие аспекты:

   – в случае использования существующей базы данных и последующим импортированием в нее нового шаблона безопасности в диалоговом окне «Импорт шаблона» необходимо выбрать опцию «`Очистить эту базу данных перед импортом`», что приведет к перезаписи всех шаблонов, хранящихся в базе данных, импортируемым шаблоном;
   – в случае использования новой базы данных при импортировании шаблона безопасности `SQL Server Security Settings.inf` опция «`Очистить эту базу данных перед импортом`» может быть снята.

5. Выбрать пункт меню «Действие» диалогового окна консоли управления «Анализ и настройка безопасности» и далее команду «Анализ компьютера» (см. рисунок 3.1).

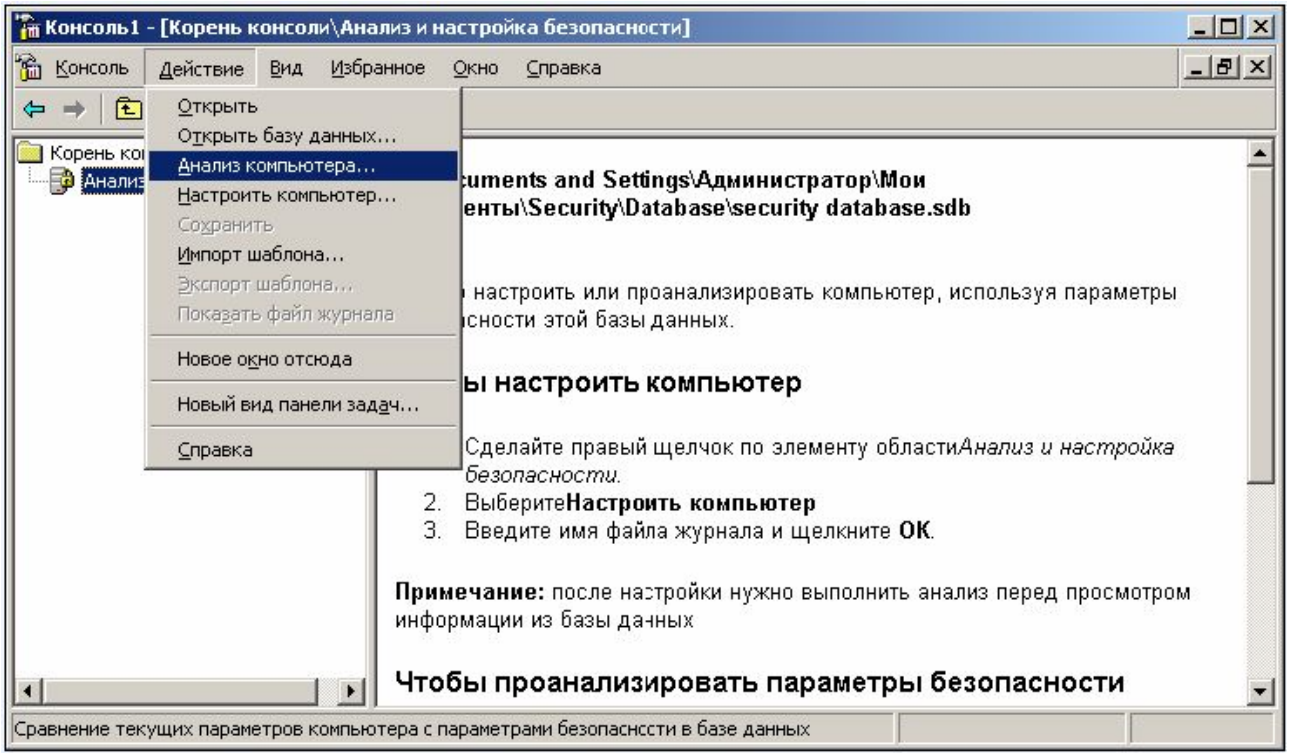

Рисунок 3.1

6. Выполнить одно из следующих действий:
   - при использовании стандартного журнала ошибок в группе «Путь файла журнала ошибок» нажать «ОК»;
   - для выбора другого журнала ввести в поле «Путь файла журнала ошибок» допустимый путь и имя файла.

7. По завершении анализа безопасности компьютера просмотреть журнал ошибок (для просмотра журнала ошибок необходимо правой кнопкой мыши нажать на узел «Анализ и настройка безопасности» и выбрать команду «`Показать файл журнала`») или результаты анализа безопасности на предмет соответствия текущих параметров безопасности системы эталонным значениям. Если элемент определен в шаблоне безопасности и в системе, однако значения параметров безопасности не совпадают, то в файле журнала данный элемент будет отмечен строкой «`Не соответствует` – `<`*`Наименование_параметра`*`>` (см. рисунок 3.2), а в результатах анализа помечен знаком (см. рисунок 3.3).

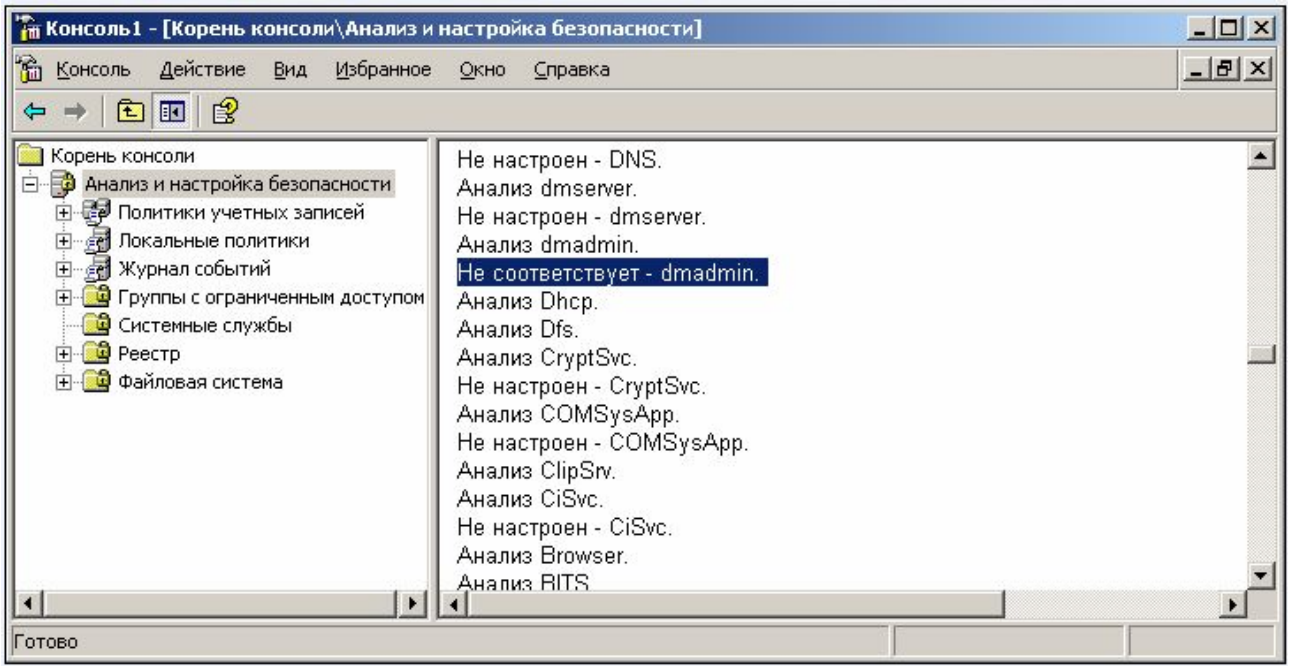

Рисунок 3.2

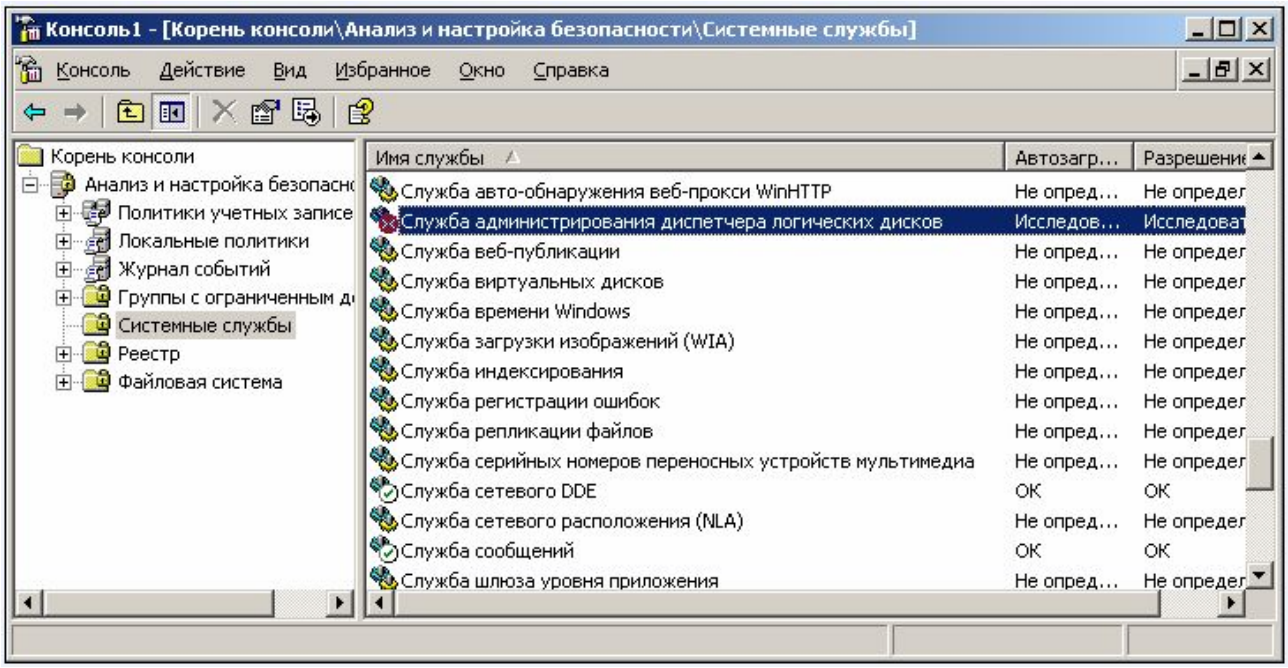

Рисунок 3.3

8. Закрыть оснастку «Анализ и настройка безопасности».

Анализ безопасности системы с использованием командной строки

Для анализа параметров безопасности системы запустить из пакетного файла с помощью планировщика задания или с использованием окна командной сроки утилиту `Secedit.exe` со следующими параметрами (см. таблицу 3.1):

```
Secedit /analyze /db <имя_файла_базы данных>
        [/cfg <имя_файла_шаблона_безопасности>] [/override]
        [/log <путь_к_файлу_журнала>] [/quiet]
```

Таблица 3.1 – Описание аргументов команды `Secedit.exe` для анализа безопасности

Аргумент	Описание
`/db` *<имя_файла_базы_данных>*	Обязательный аргумент. Путь к базе данных, содержащей сохраненную эталонную конфигурацию безопасности, по которой будет производиться анализ. Если значение *имя_файла_базы_данных* соответствует новой базе данных, необходимо указать аргумент `/cfg` *<имя_файла_шаблона_безопасности>*.
`/cfg` *<имя_файла_шаблона_безопасности>*	Данный аргумент может использоваться только совместно с опцией `/db` и указывает путь к шаблону безопасности, который будет импортироваться в базу данных для анализа. Если данный аргумент не указан, буден использоваться шаблон, хранящийся в базе данных.
`/log` *<путь_к_файлу_журнала>*	Путь к файлу журнала ошибок. Если данный аргумент не указан будет использоваться файл журнала ошибок по умолчанию (путь `%windir%\Security\Logs\Scesrv.log`).
`/quiet`	Параметр, указывающий, что процесс анализа безопасности системы должен выполняться без запроса подтверждения пользователя.

3.3 Указания по контролю настроек безопасности в процессе администрирования СУБД Microsoft® SQL Server™ 2005

Определенные в Приложении А настоящего руководства параметры, включенные в шаблоны безопасности, являются базовыми параметрами безопасности, определяющими общий уровень безопасности операционной системы семейства Microsoft® Windows Server™ 2003, под управлением которой функционирует СУБД Microsoft® SQL Server™ 2005.

Администратор имеет возможность изменять значения параметров безопасности, не включенных в соответствующие шаблоны. При изменении параметров безопасности администратор должен контролировать неизменность параметров примененных шаблонов

безопасности. Контроль неизменности параметров безопасности системы может осуществляться как с использованием оснастки консоли управления «Анализ и настройка безопасности» (порядок применения указанного средства представлен выше), так и с использованием инструментального средства командной строки `Secedit.exe`, запуск которого осуществляется из соответствующего файла командного сценария, размещенного на компакт-диске, входящем в комплект поставки сертифицированной версии СУБД Microsoft® SQL Server™ 2005.

Для контроля неизменности параметров примененного шаблона безопасности `SQL Server Security Settings.inf` необходимо осуществить запуск файла командного сценария `Analyze SQL Server.cmd`. Проанализировав полученный журнал регистрации `SecurityLog.log`, необходимо убедиться в отсутствии в нем строк следующего характера: «`Не соответствует - <`*`Наименование_анализируемого_параметра`*`>`», свидетельствующих, что контролируемые параметры безопасности были изменены.

В случае необходимости изменения значений каких-либо параметров примененного шаблона безопасности, администратор должен представить соответствующее обоснование. Это обоснование учитывается при оформлении аттестата соответствия.

3.4 Автоматизированный контроль сертифицированной версии СУБД Microsoft® SQL Server™ 2005

В данном разделе автоматизированный контроль сертифицированной версии СУБД Microsoft® SQL Server™ 2005 рассматривается на примере СУБД Microsoft® SQL Server™ 2005 Standard Edition.

Для контроля версии и настроек СУБД Microsoft® SQL Server™ 2005 Standard Edition, а также требуемых настроек безопасности операционной системы семейства Microsoft® Windows Server™ 2003, может использоваться «`Программа контроля сертифицированной версии СУБД Microsoft® SQL Server™ 2005`», поставляемая дополнительно к дистрибутиву на компакт-диске. Установка программы осуществляется путем копирования каталога, содержащего дистрибутив программы, на жесткий магнитный диск компьютера.

Запуск программы на исполнение осуществляется путем выбора исполняемого файла `SQLchk2005SE.exe` и двойного щелчка левой кнопкой мыши на его пиктограмме и должен выполняться пользователем, обладающим административными полномочиями в операционной системе и имеющим доступ к БД `master` контролируемого экземпляра СУБД

Microsoft® SQL Server™ 2005 Standard Edition. После запуска программы контроля сертифицированной версии СУБД Microsoft® SQL Server™ 2005 Standard Edition на экране должно появиться диалоговое окно, представленное на рисунке 3.4.

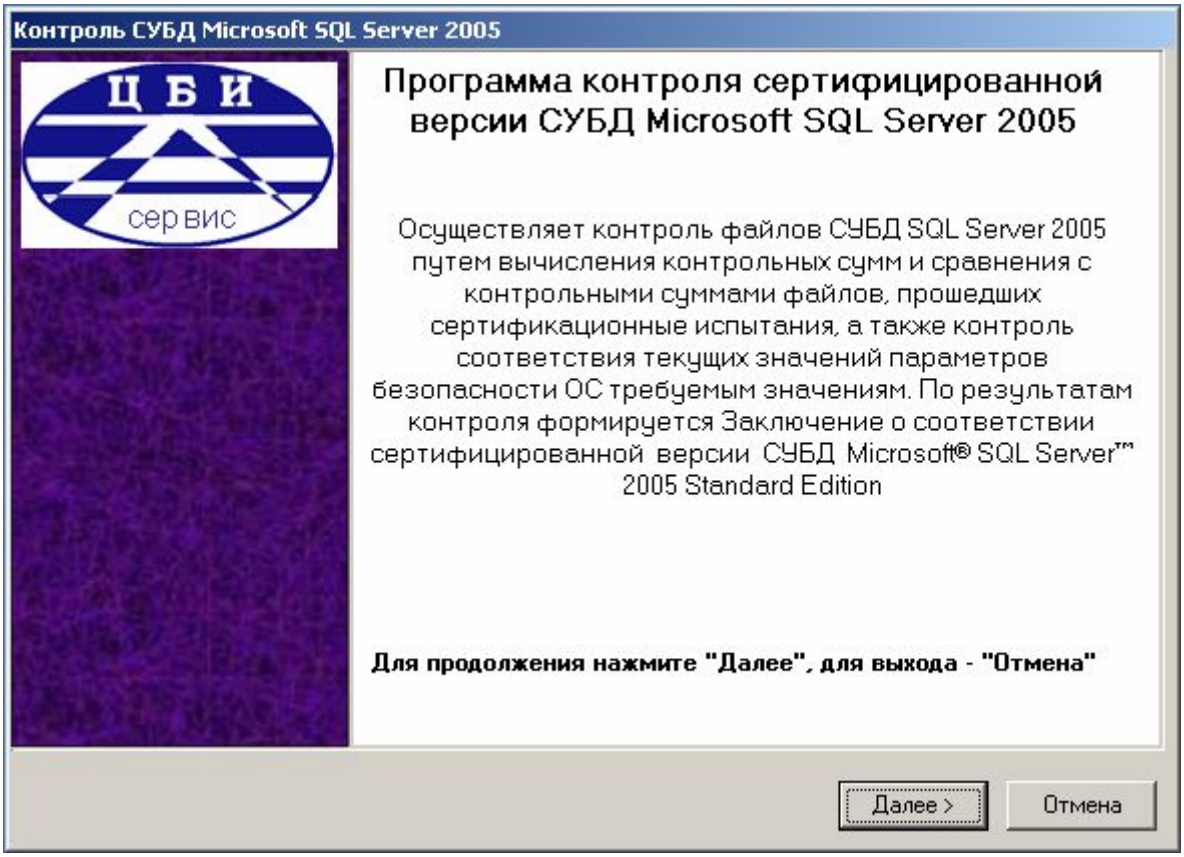

Рисунок 3.4 – Вид окна программы контроля сертифицированной версии СУБД Microsoft® SQL Server™ 2005 Standard Edition

В появившемся после запуска диалоговом окне необходимо нажать кнопку «Далее». После этого появляется диалоговое окно выбора экземпляра СУБД Microsoft® SQL Server™ 2005, для которого необходимо осуществить контроль файлов и проверить соответствие текущих параметров безопасности сертифицированным значениям (см. рисунок 3.5). Администратор может выбрать один из именованных экземпляров СУБД Microsoft® SQL Server™ 2005, установленных на компьютере. Имя экземпляра СУБД Microsoft® SQL Server™ 2005, установленного по умолчанию (`Default Instance`) `MSSQLSERVER`.

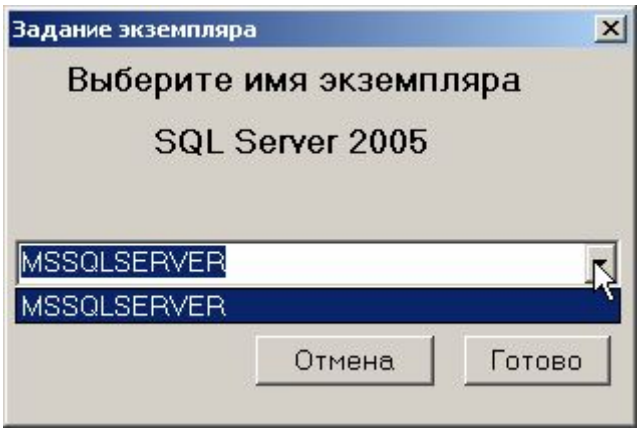

Рисунок 3.5 – Окно выбора контролируемого экземпляра СУБД Microsoft® SQL Server™ 2005

После выбора экземпляра СУБД Microsoft® SQL Server™ 2005 инициируется процесс контроля ее версии и редакции. В случае если версия и редакция системы управления базами данных, установленной на компьютере, не соответствует сертифицированной, в окне программы, представленном на рисунке 3.6, будет выведена надпись «Соответствие версии сертифицированной СУБД не установлено».

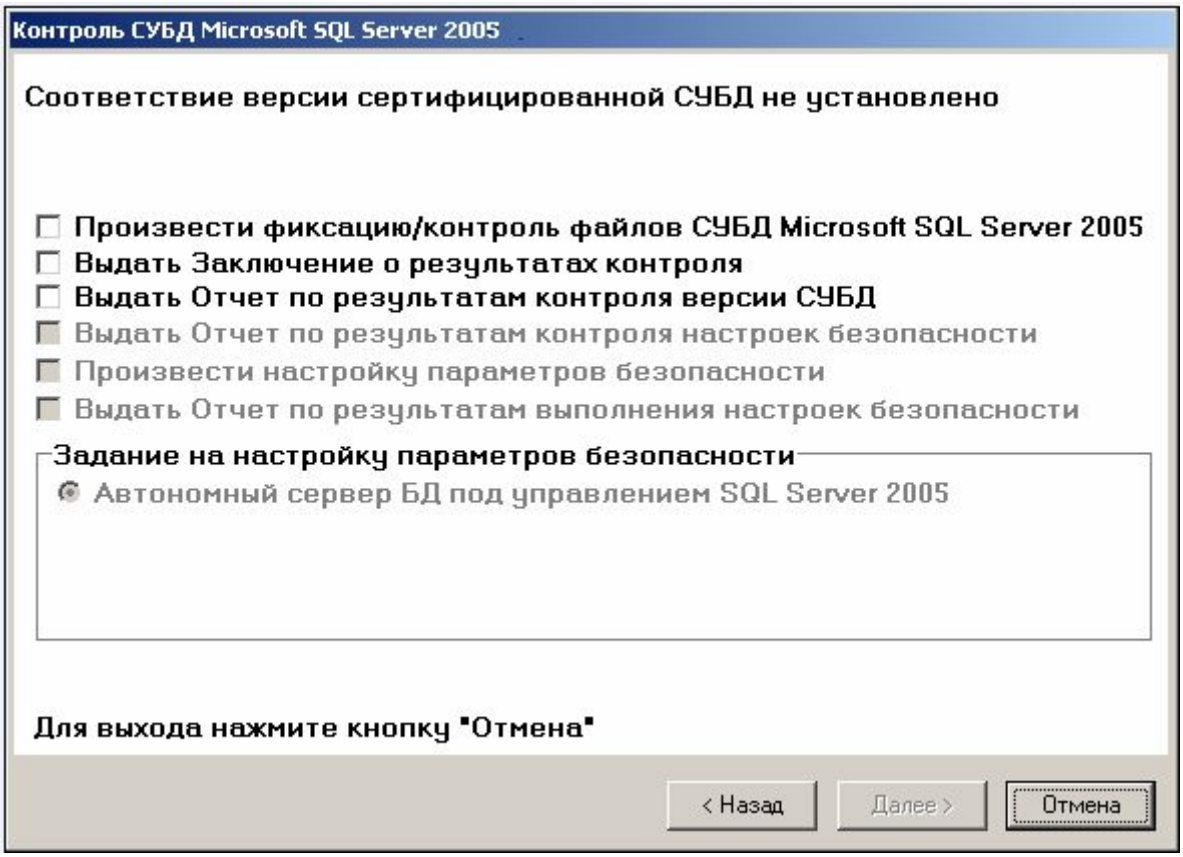

Рисунок 3.6 – Окно программы контроля в случае несоответствия версии СУБД Microsoft® SQL Server™ 2005

В случае, если соответствие версий и редакции установлено, инициируется процесс контроля соответствия файлов и текущих настроек безопасности экземпляра системы управления базами данных, установленного на компьютере, СУБД Microsoft® SQL Server™ 2005, прошедшей сертификационные испытания. Кроме того, на данном этапе инициируется проверка настроек безопасности операционной системы, требуемых для безопасного функционирования СУБД Microsoft® SQL Server™ 2005. После успешного завершения контроля соответствия файлов и настроек безопасности окно программы имеет вид, представленный на рисунке 3.7

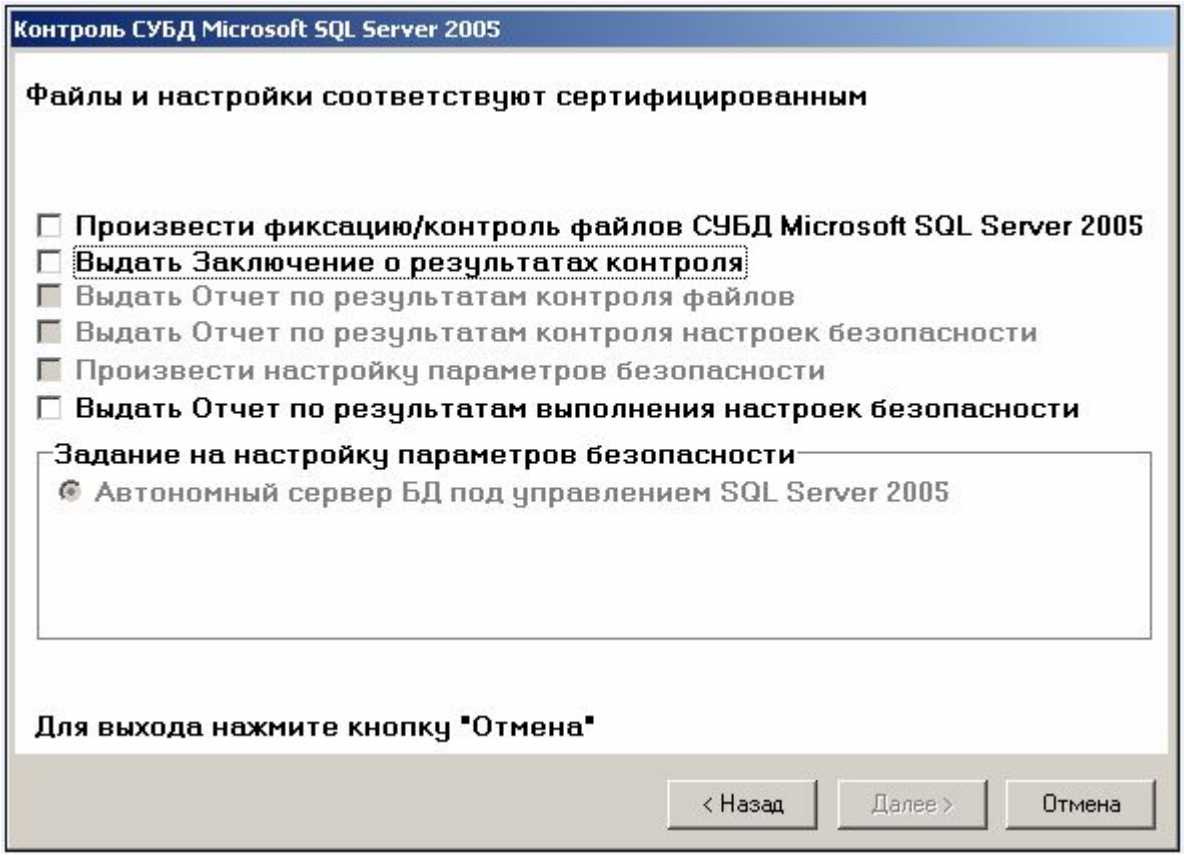

Рисунок 3.7 – Вид окна программы контроля сертифицированной версии СУБД Microsoft® SQL Server™ 2005 после успешного завершения контроля

При установлении соответствия файлов сертифицированной СУБД Microsoft® SQL Server™ 2005 и настроек безопасности операционной системы требуемым значениям, но несоответствии настроек СУБД Microsoft® SQL Server™ 2005 (например, уровня аудита) окно программы контроля будет иметь вид, представленный на рисунке 3.8.

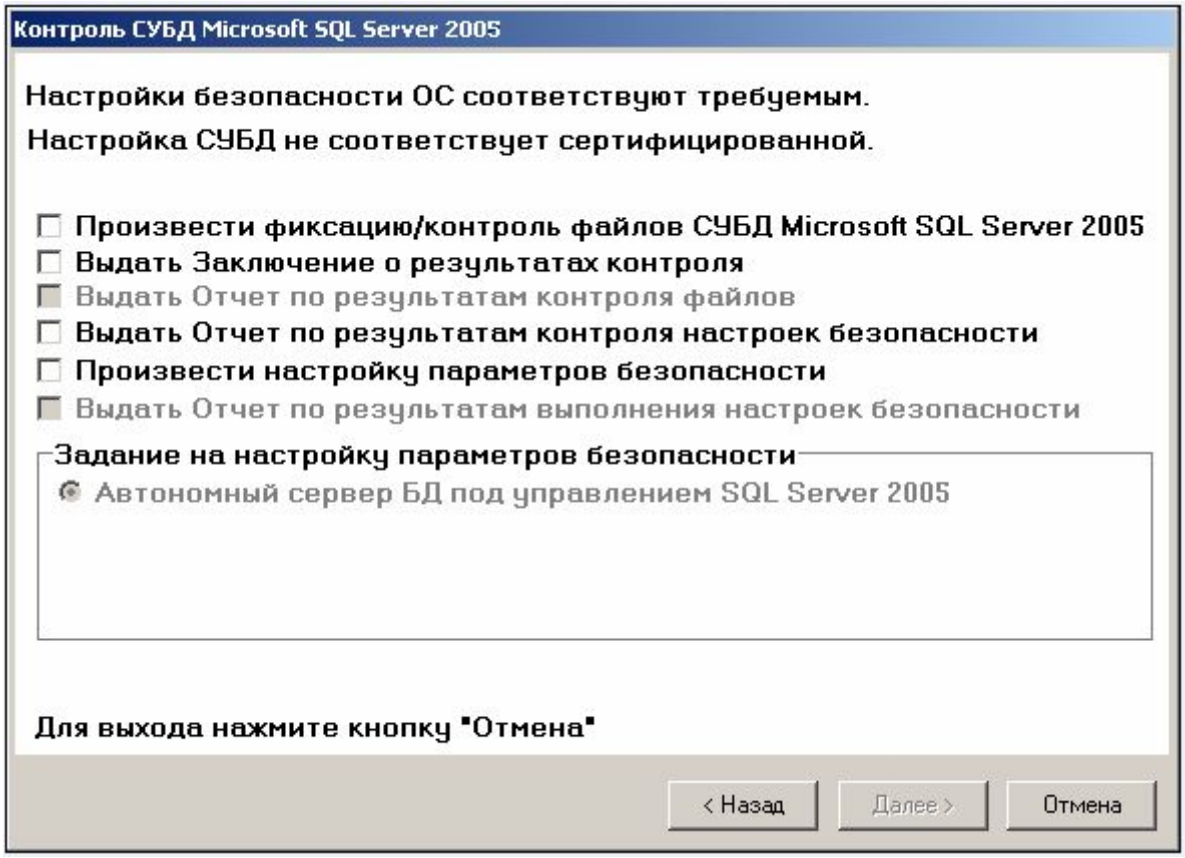

Рисунок 3.8 – Вид окна программы контроля сертифицированной версии СУБД Microsoft® SQL Server™ 2005 при несоответствии настроек безопасности

Для создания отчета по результатам контроля настроек безопасности операционной системы и СУБД Microsoft® SQL Server™ 2005 необходимо выбрать опцию «`Выдать Отчет по результатам контроля настроек безопасности`» и нажать кнопку «Далее». Анализ результатов контроля позволит выявить и в дальнейшем устранить существующие несоответствия между текущими и требуемыми настройками безопасности.

При необходимости произвести настройку параметров безопасности операционной системы, обязательных для обеспечения безопасного функционирования СУБД Microsoft® SQL Server™ 2005, следует выбрать опцию «`Произвести настройку параметров безопасности`». При этом выбор варианта функционирования СУБД Microsoft® SQL Server™ 2005 на автономном компьютере осуществляется автоматически. Порядок настройки параметров безопасности ОС, установленных на компьютерах, включенных в состав домена Active Directory, описан в разделе 2.3.

Для получения заключения о результатах контроля СУБД Microsoft® SQL Server™ 2005 необходимо выбрать опцию «`Выдать Заключение о результатах контроля`» и нажать кнопку «Далее».

Для проведения фиксации исходного состояния файлов системы управления базами данных необходимо выбрать опцию «Произвести фиксацию/контроль исходного состояния файлов СУБД Microsoft SQL Server 2005» и в появившемся диалоговом окне программы, представленном на рисунке 3.9, установить переключатель «Вид работы» в положение «Фиксация».

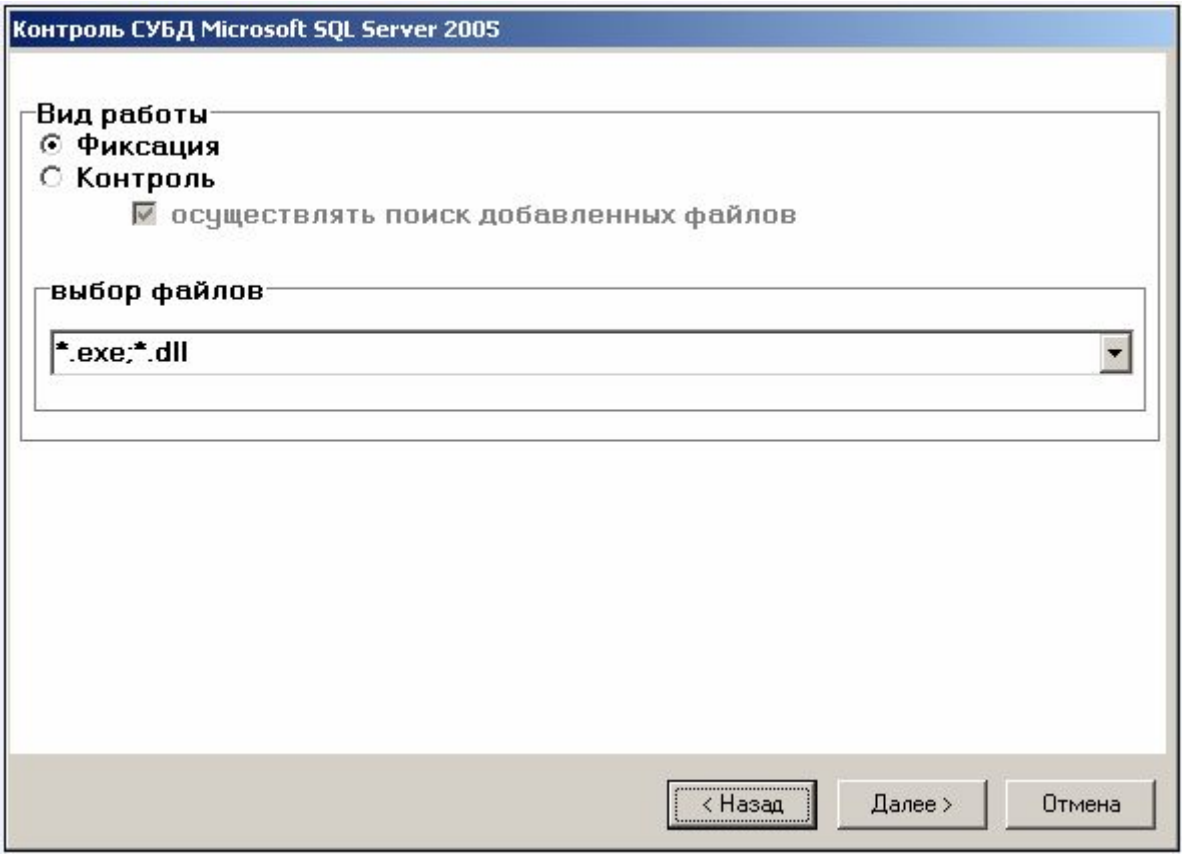

Рисунок 3.9 – Вид окна программы при проведении фиксации или контроля исходного состояния файлов СУБД Microsoft® SQL Server™ 2005

По умолчанию в поле «Выбор файлов» указана маска, предполагающая проведение фиксации всех программных файлов СУБД. При такой установке будет произведена фиксация всех файлов указанного экземпляра СУБД, находящихся в папке, что может занять длительное время. С целью уменьшения времени фиксации могут быть указаны другие маски, задаваемые вручную, или путем выбора из списка. Вызов списка осуществляется путем нажатия кнопки ▼, расположенной в правой части поля «Выбор файлов». После нажатия «Далее», окно программы приобретет вид, показанный на рисунке 3.10.

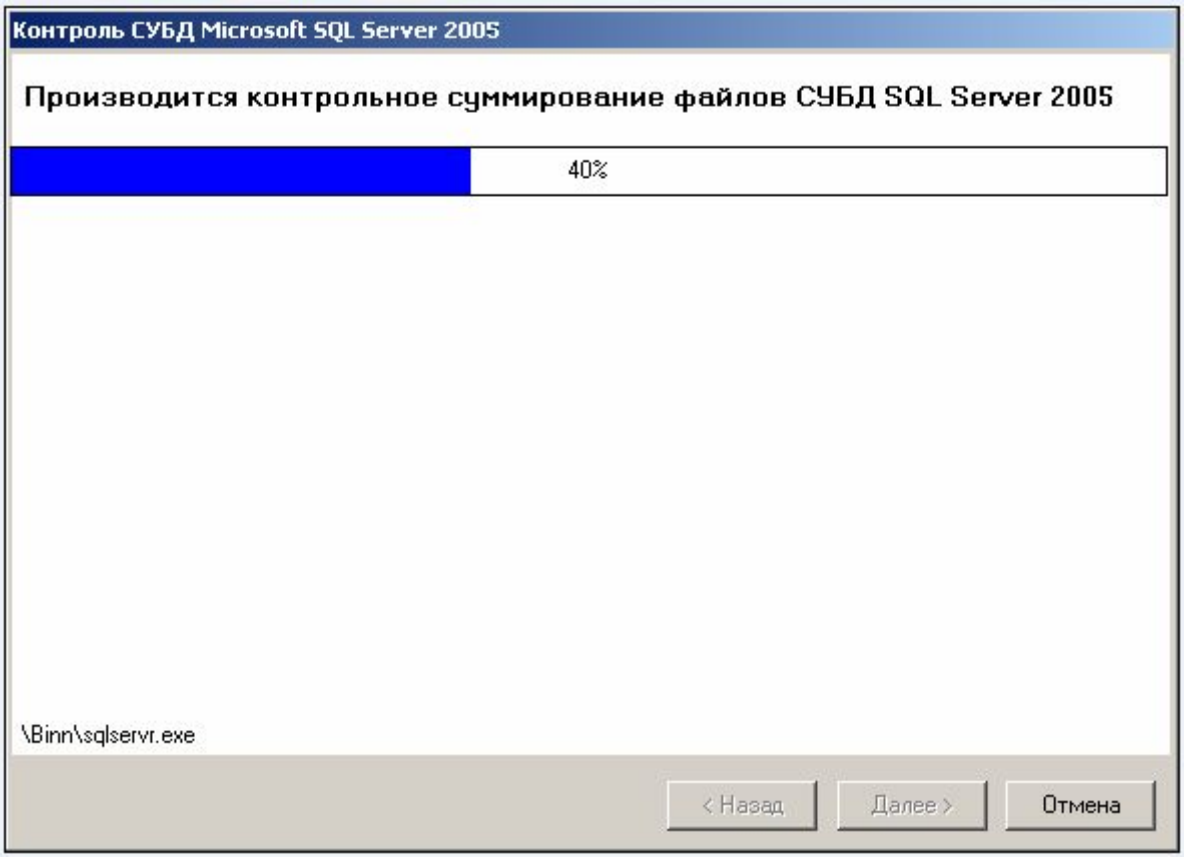

Рисунок 3.10 – Вид окна программы при проведении контрольного суммирования файлов СУБД Microsoft® SQL Server™ 2005

После завершения контрольного суммирования в появившемся диалоговом окне необходимо ввести имя файла, в который необходимо сохранить результаты фиксации исходного состояния файлов СУБД Microsoft® SQL Server™ 2005 для последующего контроля.

Для проведения контроля исходного состояния необходимо установить переключатель «Вид работы» в положение «Контроль». Для обнаружения в процессе контроля файлов, добавленных в папку, необходимо выбрать опцию «Осуществлять поиск добавленных файлов» и нажать кнопку «Далее». Поле «Выбор файлов» должно содержать такие маски, которые были заданы при проведении фиксации исходного состояния. После нажатия кнопки «Далее» в появившемся диалоговом окне необходимо выбрать имя файла, содержащего результаты фиксации исходного состояния, и нажать кнопку «Открыть». По завершении контроля окно программы будет иметь вид, представленный на рисунке 3.11.

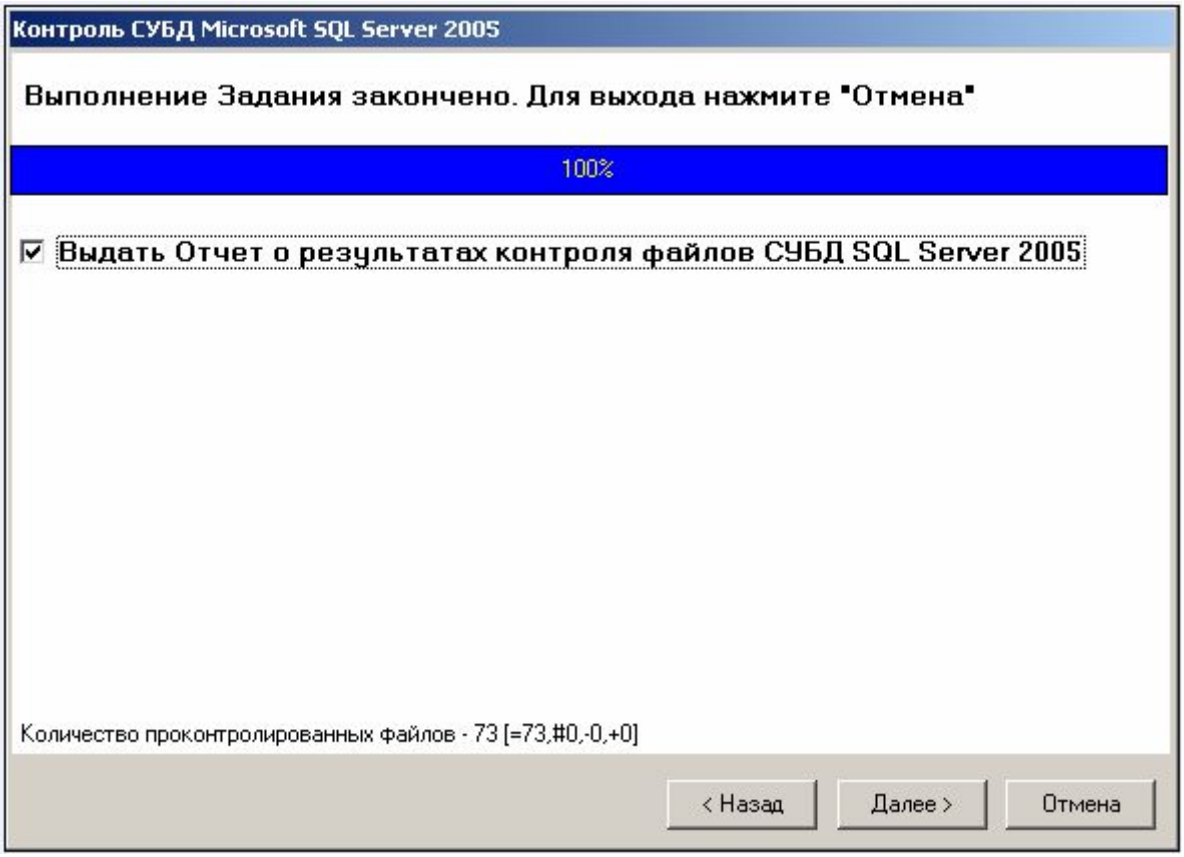

Рисунок 3.11 – Вид окна программы при проведении контроля исходного состояния файлов СУБД Microsoft® SQL Server™ 2005

В нижней части окна представлен обобщенный результат контроля – количество проконтролированных файлов. В скобках рядом указаны три или четыре цифры. Рядом со знаком «=» расположено число файлов, не изменившихся после выполнения фиксации. Рядом со знаком «#» - количество измененных файлов, рядом со знаком «-» - количество отсутствующих файлов, рядом со знаком «+» - число файлов, добавленных в папку с программными файлами контролируемого экземпляра СУБД (только при установленной опции «`Осуществлять поиск добавленных файлов`»).

Проведение контроля целостности рекомендуется осуществлять при появлении подозрений на вирусы, нарушении исправного функционирования СУБД Microsoft® SQL Server™ 2005, после установки программного обеспечения и т.п.

Приложение А

А.1 Групповая политика

Групповая политика представляет собой набор правил, определяющих параметры системы: безопасность, работу приложений и служб, установку программного обеспечения и т.д. Цель политик безопасности – определить процедуры выбора конфигурации и управления безопасностью в среде функционирования. Групповая политика помогает применить технические рекомендации в политике безопасности для всех компьютеров и серверов в доменах Active Directory.

Применение групповой политики осуществляется с целью контроля использования программ, сетевых ресурсов и операционной системы пользователями и компьютерами. Групповые политики позволяют легко и единообразно управлять настройками большого количества вариантов среды серверных компьютерных систем путем выборочного включения и выключения отдельных функций. В случае использования групповой политики для создания настроек безопасности, любые изменения, осуществляемые по отношению к какой-либо из политик, будут относиться ко всем серверам, клиентским компьютерам и пользователям, использующим эту политику.

Существует два типа групповых политик. Первый тип – это локальная групповая политика. Локальная групповая политика может быть только одна, и это единственная групповая политика, доступная на компьютерах, не являющихся членом домена. Она применяется также на всех компьютерах, которые входят в состав домена Active Directory, являясь его участниками.

Второй тип групповой политики – это групповая политика Active Directory. Интегрирование групповой политики со службой каталогов Active Directory позволяет обеспечить большую безопасность и гибкость управления пользователями и объектами сети, позволяя администраторам объединить их в логические группы, такие как организационные подразделения (Organizational Unit), а затем назначать группам единые параметры конфигурации, что обеспечит непротиворечивость их конфигураций. Использование групповой политики в сочетании со структурой организационных подразделений позволяет определять специфические настройки безопасности для тех или иных функций конкретного клиентского компьютера или сервера.

Объекты групповой политики, основанные на Active Directory, фактически состоят из двух разных объектов:

– контейнера групповой политики GPC (Group Policy Container), расположенного в каталоге Active Directory. Данный объект содержит список компонентов, используемый для определения того, параметры какой группы конфигурационных параметров (относящихся к пользователю или компьютеру) сконфигурированы в данном ОГП, информацию о версии групповой политики и информацию о состоянии, используемую для указания того, является ли ОГП действующим, или он заблокирован;
– шаблона групповой политики GPT (Group Policy Template). Данный объект содержит большинство фактических параметров настройки для групповой политики и расположен в папке совместно используемого ресурса `Sysvol` на каждом контроллере домена.

Шаблоны безопасности

Шаблон безопасности представляет собой текстовый файл, в котором определены параметры безопасности операционной системы. Каждый шаблон хранить в обычном текстовом файле с расширением `.inf`, что позволяет копировать, импортировать и экспортировать параметры безопасности.

Шаблоны безопасности могут импортироваться как в локальные объекты групповой политики, так и в объекты групповой политики, определяемые в Active Directory. В этом случае все компьютеры и учетные записи пользователей, на которые распространяется групповая политика, применяют конфигурацию безопасности, описанную с помощью данного шаблона. Импорт шаблонов безопасности упрощает администрирование, так как конфигурация безопасности автоматически настраивается сразу для нескольких объектов.

Для изменения шаблонов используется редактор (оснастка) шаблонов безопасности из состава оснасток консоли управления Microsoft Management Console или любой текстовый редактор (например, программа «Блокнот»). Шаблоны безопасности содержат все параметры безопасности, назначаемые объекту групповой политики, кроме относящихся к политикам открытых ключей и политике IPSec. Некоторые разделы шаблона могут содержать списки управления доступом Access Control List (ACL), которые определенны на языке Security Descriptor Definition Language (SDDL).

В таблице А.1.1 показано соответствие между разделами групповой политики и секциями файла шаблона безопасности.

Таблица А.1.1 – Формат шаблона безопасности

Раздел групповой политики	Раздел шаблона безопасности
Политика учетных записей (Account Policy)	[System Access]
Политика аудита (Audit Policy)	[System Log] [Security Log] [Application Log]
Назначенные права пользователя (User Rights Assignment)	[Privilege Rights]
Параметры безопасности (Security Options)	[Registry Values]
Журналы событий (Event Log)	[Event Audit]
Группы с ограниченным доступом (Restricted Groups)	[Group Membership]
Системные службы (System Services)	[Service General Setting]
Реестр (Registry)	[Registry Keys]
Файловая система (File System)	[File Security]

А.2 Параметры безопасности, определяемые для компьютеров с установленной СУБД Microsoft® SQL Server™ 2005

Параметры безопасности, представленные в данной главе, предназначены для приведения операционной системы семейства Microsoft® Windows Server™ 2003, под управлением которой функционирует СУБД Microsoft® SQL Server™ 2005, к необходимому для работы СУБД уровню защищенности и учитывают особенности конфигурации, в которой данная СУБД была сертифицирована. В данном разделе рассматриваются основные параметры безопасности, для настройки которых используется групповая политика. Применение рекомендованных параметров безопасности позволяет защитить обрабатываемую на серверах БД информацию.

Параметры локальной политики

Параметры локальной политики должны быть настроены централизованно для всего множества серверов БД, функционирующих в заданной конфигурации безопасности. Для этого используется объекты групповой политики, базирующиеся на основе службы каталогов Active Directory. К параметрам локальной политики относят политику аудита, назначение прав пользователям и параметры безопасности.

Параметры назначения прав пользователей

Задачи, которые пользователь имеет право выполнять в домене или в системе, установленной на компьютере, называются правами пользователя. Существует два типа прав: права, связанные с входом в систему, и привилегии. Права, связанные с входом в систему, определяют, кто и каким образом имеет право входить в систему на конкретном компьютере. Привилегии определяют возможные действия, которые разрешены пользователю в системе. Причем привилегии могут переопределять разрешения доступа, установленные для отдельных контролируемых объектов.

В операционной системе семейства Microsoft® Windows Server™ 2003 назначение прав учетной записи, используемой для запуска служб SQL Server и SQL Server Agent (см. таблицу А.2.1), следует осуществлять с использованием групповой политики в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\Конфигурация Windows\Параметры безопасности \Локальные политики\Назначение прав пользователей`.

Таблица А.2.1 – Параметры назначения прав пользователей

№ п/п	Название параметра	Значение параметра безопасности
1.	Работа в режиме операционной системы[1]	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent
2.	Обход перекрестной проверки	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent
3.	Настройка квот памяти для процесса	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent
4.	Отклонить локальный вход	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent
5.	Закрепление страниц в памяти	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent
6.	Вход в качестве службы	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent

[1] Данный параметр (также как и все остальные, описанные в таблице) не включен в файл шаблона безопасности, поскольку учетная запись, для которой осуществляется назначение прав пользователей, имеет уникальный для каждого домена Active Directory идентификатор безопасности SID (Security Identifier). Таким образом, при настройке групповой политики назначение прав пользователей для данной учетной записи должно быть выполнено администратором безопасности самостоятельно.

№ п/п	Название параметра	Значение параметра безопасности
7.	Замена маркера уровня процесса	Учетная запись, используемая для запуска служб SQL Server и SQL Server Agent

Право «Работа в режиме операционной системы» разрешает процессу проходить проверку подлинности как обычному пользователю, выступая в последствии от его имени, и таким образом получать доступ к тем же ресурсам, что и любой пользователь. Эта привилегия требуется только для служб проверки подлинности низкого уровня.

Право «Обход перекрестной проверки» определяет, какие пользователи могут проходить по дереву каталога, независимо от того, имеются ли у них разрешения на доступ к этому каталогу. Данная привилегия не позволяет пользователю выводить список содержимого каталога, а только перемещаться по его структуре.

Параметр «Настройка квот памяти для процесса» определяет, какие учетные записи служб могут использовать процесс, обладающий разрешением «Запись свойства» для доступа к другому процессу, с целью увеличить назначенную последнему квоту ресурсов процессора. Данная привилегия используется системой управления базами данных в части задания и управления квотами вычислительных ресурсов.

Право «Отклонить локальный вход в систему» определяет перечень пользователей, которым запрещено осуществлять интерактивный вход в систему. Указанное право назначается учетной записи, используемой для запуска служб SQL Server и SQL Server Agent, с целью исключить возможность интерактивной регистрации с ее помощью нарушителя в случае компрометации данной учетной записи.

Параметр «Закрепление страниц в памяти» определяет, какие учетные записи могут использовать процесс для хранения данных в физической памяти, избегая подкачки страниц в виртуальную память на диск. Учетные записи, обладающие данным правом, могут определять размер оперативной памяти, который система должна выделить для указного множества процессов.

Наличие права «Вход в качестве службы» определяет, какие учетные записи служб могут зарегистрировать процесс в качестве службы. Данное право необходимо для корректного функционирования служб системы управления базами данных.

Учетная запись службы, обладающая правом «Замена маркера уровня процесса», может инициировать процесса замены стандартного маркера доступа, ассоциированного с запущенным дочерним процессом (подпроцессом). Данное право может

быть использовано с целью изменения маркера доступа подпроцесса, что приведет к изменению контекста безопасности и повышению его привилегий. Данное право необходимо для корректного функционирования служб системы управления базами данных.

Группы с ограниченным доступом

Параметр «Группы с ограниченным доступом» позволяет регулировать принадлежность групп безопасности в операционной системе Microsoft® Windows Server™ 2003 Enterprise Edition. При вводе ограничений доступа для групп безопасности следует исходить из существующих потребностей. В данном руководстве к группам с ограниченным доступом следует относить группы безопасности, обладающие административными полномочиями в системе, а также группы безопасности, членами которых должны являться только учетные записи, используемые для запуска служб SQL Server и SQL Server Agent. Администратору необходимо тщательно контролировать состав административных групп безопасности с целью исключения возможности включения (умышленного или непреднамеренного) в их состав учетной записи, используемой для запуска служб SQL Server и SQL Server Agent, и тем самым предоставления ее административных полномочий.

Членство в группах с ограниченным доступом следует настраивать с использованием редактора групповой политики в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Группы с ограниченным доступом`.

Администраторы могут задавать группы с ограниченным доступом через объекты групповой политики, добавляя нужную группу прямо в раздел «Группы с ограниченным доступом» пространства имен объектов групповой политики. Когда группа определена в качестве группы с ограниченным доступом, для нее можно назначать членов, а также задавать другие группы, куда она сама входит в качестве члена. Если для группы не определено ни одного члена, доступ в нее будет полностью ограничен.

Рекомендуется также вводить ограничения для всех встроенных групп, которые не планируется использовать в организации.

Параметры безопасности

Данные параметры позволяют включать и отключать параметры безопасности операционной системы семейства Microsoft® Windows Server™ 2003 и по существу позволяют пользователям изменять параметры системного реестра, влияющие на безопасность, без непосредственного редактирования самого реестра. Они позволяют

определить дополнительные характеристики, определяющие поведение системы, и в основном требуются только при повышении уровня ее защищенности, необходимого для безопасного функционирования СУБД Microsoft® SQL Server™ 2005.

С помощью редактора объектов групповой политики необходимо настроить параметры безопасности операционной системы семейства Microsoft® Windows Server™ 2003, представленные в таблице А.2.2. Параметры безопасности следует настраивать с использованием редактора групповой политики в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\Конфигурация Windows \Параметры безопасности\Локальные политики\Параметры безопасности.`

Таблица А.2.2 – Параметры, используемые для обеспечения безопасности компьютеров под управлением операционной системы семейства Microsoft® Windows Server™ 2003

№ п/п	Название параметра	«High Security»
1.	Учетные записи: состояние учетной записи «Гость»	Отключен
2.	Учетные записи: переименование учетной записи администратора	<*Новое_имя_учетной_записи*>
3.	Учетные записи: переименование учетной записи гостя	<*Новое_имя_учетной_записи*>
4.	Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями	Включен
5.	Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями	Включен
6.	Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям	Отключен
7.	Сетевой доступ: разрешать анонимный доступ к именованным каналам	Нет значений

Параметр безопасности «Учетные записи: состояние учетной записи «Гость» определяет, включена или выключена учетная запись пользователя «Гость». Данная учетная запись позволяет пользователям осуществлять доступ к компьютеру из сети без прохождения процедур идентификации и аутентификации, т.е. в качестве анонимных пользователей. Исходя из этого, учетная запись пользователя «Гость» должна быть отключена.

Параметр безопасности «Учетные записи: переименование учетной записи администратора» определяет необходимость переименования учетной записи «Администратор». Однако, одного только переименования учетной записи без изменения стандартного описания «Встроенная учетная запись для администрирования компьютера или домена» недостаточно, чтобы дезориентировать нарушителя. Поэтому помимо переименования самой учетной записи, должно быть изменено ее описание. Кроме того, важно помнить, что разрешение анонимным пользователям перечислять учетные записи практически сводит на нет преимущества в безопасности, полученные при переименовании учетной записи администратора. Исходя из этого, данный параметр безопасности должен быть использован для переименования встроенной учетной записи «Администратор» с целью исключения ассоциации с ее реальным назначением и уровнем доступа.

Параметр безопасности «Учетные записи: переименование учетной записи гостя» определяет необходимость переименования учетной записи «Гость», чтобы исключить ассоциации с ее реальным назначением и уровнем доступа.

Параметр безопасности «Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями» определяет, какие дополнительные разрешения будут предоставлены пользователям при анонимных подключениях к компьютеру, и позволяет проконтролировать, смогут ли анонимные пользователи запрашивать перечень учетных записей в базе данных диспетчера учетных записей безопасности SAM (Security Account Manager). В случае активации данного параметра пользователи с анонимным подключением не смогут перечислять имена учетных записей домена на компьютерах. Этот параметр вводит дополнительные ограничения на анонимные подключения. Поэтому для данного параметра должно быть установлено значение «Включен». Указанное значение позволит заменить в маркере доступа, создаваемом для анонимных подключений, идентификатор безопасности группы «Все» на идентификатор группы «Прошедшие проверку».

Параметр безопасности «Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями» позволяет

проконтролировать, смогут ли анонимные пользователи осуществлять перечисление учетных записей SAM и совместно используемых ресурсов. В случае активации данного параметра анонимные пользователи не смогут перечислить имена доменных учетных записей и имена совместно используемых сетевых ресурсов на компьютерах. Поэтому для данного параметра должно быть установлено значение «Включен».

Параметр безопасности «Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям» определяет, какие дополнительные разрешения предоставляются при анонимном подключении к компьютеру. Операционная система семейства Microsoft® Windows Server™ 2003 предоставляет анонимным пользователям возможность выполнять ряд операций (например, производить перечисление имен учетных записей домена и сетевых ресурсов). Это удобно в случае, если администратору требуется предоставить доступ пользователям в доверенном домене, в котором не поддерживается двусторонние доверительные отношения. По умолчанию из маркера доступа, создаваемого для анонимных подключений, система удаляет идентификатор безопасности группы «Все». Поэтому разрешения, предоставленные данной группе безопасности, не применяются к анонимным пользователям. Если данный параметр установлен, анонимный пользователь получит доступ только к тем ресурсам, для которых ему явным образом предоставлено разрешение. Поскольку при включении данной политики анонимные пользователи смогут получить перечень имен учетных записей пользователей и сетевых ресурсов, и в дальнейшем использовать полученную информацию для организации атак различных типов, то использование данного параметра должно быть запрещено.

Параметр безопасности «Сетевой доступ: разрешать анонимный доступ к именованным каналам» определяет, каким сеансам связи (именованным каналам) будут назначаться атрибуты и разрешения, допускающие анонимный доступ пользователей. В рассматриваемой конфигурации безопасности данному параметру не должно быть присвоено никаких значений. Добавление каких-либо именованных каналов связано с потенциальной угрозой их доступности любому сетевому пользователю, что в свою очередь может привести к компрометации или утрате информации.

Системные службы

При установке операционной системы семейства Microsoft® Windows Server™ 2003 создаются и настраиваются стандартные системные службы, которые начинают функционировать при запуске системы. Однако при функционировании СУБД Microsoft® SQL Server™ 2005 в том или ином окружении для нормальной работы ряд служб не

требуется. Поскольку любая служба или приложение является потенциальным объектом атаки, то следует отключить (или удалить) ненужные для работы СУБД Microsoft® SQL Server™ 2005 службы или исполняемые файлы.

Параметры системных служб операционной системы семейства Microsoft® Windows Server™ 2003 следует настраивать с использованием редактора групповой политики в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Системные службы`.

Рекомендуемые параметры настройки системных служб операционной системы семейства Microsoft® Windows Server™ 2003 представлены в таблице А.2.3.

Таблица А.2.3 – Параметры настройки системных служб

№ п/п	Системная служба	Короткое имя службы	Тип запуска службы
1.	Оповещатель	Alerter	Запрещен
2.	Сервер папки обмена	ClipSrv	Запрещен
3.	DHCP-клиент	DHCP	Запрещен
4.	Распределенная файловая система DFS	DFS	Запрещен
5.	Служба факсов	Fax	Запрещен
6.	Брандмауэр Интернета (ICF) /Общий доступ к Интернету (ICS)	SharedAccess	Запрещен
7.	Службы IPSec	PolicyAgent	Запрещен
8.	Служба учета лицензий	LicenseService	Запрещен
9.	Служба администрирования диспетчера логических дисков	Dmadmin	Запрещен
10.	Служба сообщений	Messenger	Запрещен
11.	NetMeeting Remote Desktop Sharing	mnmsrvc	Запрещен
12.	Служба сетевого DDE	NetDDE	Запрещен
13.	Диспетчер сетевого DDE	NetDDEdsdm	Запрещен
14.	Диспетчер очереди печати	Spooler	Запрещен

№ п/п	Системная служба	Короткое имя службы	Тип запуска службы
15.	Диспетчер автоматических подключений удаленного доступа	RasAuto	Запрещен
16.	Диспетчер подключений удаленного доступа	RasMan	Запрещен
17.	Удаленный реестр	RemoteRegistry	Запрещен
18.	Съемные ЗУ	NtmsSvc	Вручную
19.	Смарт-карта	SCardSvr	Запрещен
20.	Планировщик заданий	Schedule	Запрещен
21.	Телефония	TapiSrv	Запрещен
22.	Служба Telnet	TlntSvr	Запрещен

Служба «Оповещатель» посылает выбранным пользователям и компьютерам административные оповещения. Отключение этой службы приводит к прекращению получения административных оповещений программами, в которых они используются. С целью обеспечения более высокого уровня безопасности для службы «Оповещатель» должен быть установлен режим запуска «Запрещен», который препятствует запуску данной службы и соответственно передаче данных по сети.

Служба «Сервер папки обмена» позволяет создавать и совместно использовать «страницы» данных в папке обмена, которые можно просматривать с удаленных компьютеров. Эта служба зависит от службы сетевого DDE (NetDDE) в процессе создания общих файловых ресурсов, к которым могут подключаться другие компьютеры. Чтобы обеспечить более высокий уровень безопасности, режим запуска для данной службы должен соответствовать значению «Запрещен».

Служба «DHCP-клиент» управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен. Данная служба обеспечивает автоматическое получение клиентом IP-адреса и всех сетевых настроек компьютера независимо от того, к какой вычислительной сети осуществлено подключение. В случае если данная служба остановлена, конфигурирование сетевых настроек должно осуществляться администратором вручную. Поскольку обычно для серверов БД под управлением СУБД Microsoft® SQL Server™ 2005

используются статически выделяемые IP-адреса, службу «DHCP-клиент» рекомендуется отключить.

Служба «Распределенная файловая система DFS» объединяет разрозненные общие файловые ресурсы в единое логическое пространство имен и управляет данными логическими томами. Поскольку в функционировании службы «Распределенная файловая система DFS» на серверах БД нет необходимости, она должна быть запрещена.

«Служба факсов» совместимая с Telephony API (TAPI), обеспечивает для компьютеров возможность работы с факсами. Служба факсов позволяет пользователям отправлять и получать факсимильные сообщения из своих настольных приложений с помощью локального или общего сетевого устройства факсимильной связи. В рассматриваемой конфигурации с целью обеспечения требуемого уровня безопасности данная служба должна быть запрещена.

Служба «Брандмауэр Интернета (ICF)/Общий доступ к Интернету (ICS)» обеспечивает поддержку служб трансляции адресов, адресации и разрешения имен, а также служб предотвращения вторжения для компьютеров вычислительной сети. В рассматриваемой конфигурации безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

«Службы IPSec» обеспечивают безопасность сетевых подключений между сервером и клиентом в сетях TCP/IP, а также управляют политикой IP-безопасности, запускают процесс согласования ключей ISAKMP/Oakley (IKE) и согласуют настройки политики IPSec. По причине отсутствия необходимости использования указанных возможностей служба IPSec на серверах БД должна быть запрещена.

«Служба учета лицензий» обеспечивает лицензирование клиентского доступа для компонентов операционной системы (IIS-сервер, службу терминалов), а также для продуктов, не входящих в состав операционной системы (Microsoft Exchange Server). В рассматриваемой конфигурации безопасности службу учета лицензий рекомендуется запретить.

«Служба администрирования диспетчера логических дисков» выполняет настройку жестких дисков и томов. Данная служба необходима только во время процессов настройки и конфигурации жестких дисков и дисковых томов. Таким образом, на серверах БД под управлением СУБД Microsoft® SQL Server™ 2005 запуск службы администрирования диспетчера логических дисков должен быть запрещен.

«Служба сообщений» осуществляет передачу и отправку сообщений службы «Оповещатель» между клиентскими и серверными компьютерами. Эта служба не имеет

отношения к программе Windows Messenger и не является обязательной для компьютеров под управлением операционной системы семейства Microsoft® Windows Server™ 2003. По этим причинам службу сообщений необходимо отключить.

Служба «NetMeeting Remote Desktop Sharing» разрешает авторизованным пользователям с помощью программы Microsoft NetMeeting® получать удаленный доступ к компьютеру через корпоративную интрасеть. Чтобы запретить удаленный доступ пользователей к компьютерам, эту службу необходимо отключить.

«Служба сетевого DDE» обеспечивает сетевой транспорт и безопасность динамического обмена данными (DDE) для программ, выполняющихся на одном или на разных компьютерах. Служба сетевого DDE, а также другие подобные автоматические сетевые службы могут использоваться нарушителями в своих целях. Поэтому с целью обеспечения требуемого уровня безопасности данная служба должна быть запрещена.

Служба «Диспетчер сетевого DDE» управляет сетевыми общими ресурсами динамического обмена данными DDE. Эта служба используется только службой сетевого DDE для управления общими каналами связи DDE. Диспетчер сетевого DDE, а также другие подобные автоматические сетевые службы могут служить объектами атак. Поэтому с целью обеспечения требуемого уровня безопасности запуск данной службы должен быть запрещен.

Служба «Диспетчер очереди печати» управляет всеми локальными и сетевыми очередями печати, а также контролирует все задания печати. Диспетчер печати является ключевым компонентом системы печати в Windows. Он управляет очередями печати в системе, а также взаимодействует с драйверами принтеров и компонентами ввода-вывода, например USB-портами и протоколами семейства TCP/IP. Поскольку серверам БД не свойственна роль сервера печати, поэтому данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Диспетчер автоматических подключений удаленного доступа» обеспечивает обнаружение неудачных попыток подключения к удаленной сети или удаленному компьютеру, а также предоставляет альтернативные методы подключения. Данная служба предлагает создать подключение к удаленной сети в случае неуспешной попытки обращения программы к удаленному DNS- или NetBIOS-имени или адресу. Данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Диспетчер подключений удаленного доступа» управляет подключениями удаленного доступа и подключениями виртуальных частных сетей к Интернету или другим вычислительным сетям. Данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Удаленный реестр» позволяет удаленным пользователям изменять параметры реестра на локальном компьютере при условии, что они имеют для этого необходимые права. В основном эта служба используется удаленными администраторами и счетчиками производительности. Отключение службы удаленного реестра ограничивает возможность изменения реестра только локальными пользователями, работающими на этом компьютере. При отключении данной службы администратор вынужден будет вручную управлять получением обновлений на каждом компьютере или обеспечить пользователям возможность самостоятельной установки обновлений. Исходя из этого, запуск службы «Удаленный реестр» на компьютерах в рассматриваемой конфигурации безопасности должен быть запрещен.

Служба «Съемные ЗУ» обеспечивает управление и систематизацию съемных носителей, управление автоматическими съемными носителями, а также поддерживает каталог идентификационной информации о каждом съемном устройстве, используемом на целевом компьютере. Поскольку на серверах БД может осуществляться создание и хранение резервных копий на съемных носителях, то, следовательно, существует необходимость использования возможностей, обеспечиваемых данной службой. Поэтому для нее рекомендуется установить режим запуска «Вручную».

Служба «Смарт-карты» управляет доступом к устройствам чтения смарт-карт. Если эта служба остановлена, этот компьютер не сможет считывать смарт-карты. Если эта служба отключена, любые службы, которые явно зависят от нее, не могут быть запущены. Поскольку для серверов БД под управлением СУБД Microsoft® SQL Server™ 2005 Standard Edition, аутентификация пользователей с использованием смарт-карт не осуществляется, указанную службу рекомендуется отключить.

Служба «Планировщик заданий» позволяет настраивать расписание автоматического выполнения задач на заданном компьютере. В тоже время его использование должно быть ограничено в средах с повышенными требованиями к безопасности, что позволит предотвратить неправильное использование системных ресурсов или запуск злонамеренного кода. По этой причине данную службу рекомендуется отключить.

Служба «Телефония» обеспечивает поддержку интерфейса Telephony API (TAPI) для программ, управляющих телефонным оборудованием и голосовой связью через протокол IP на целевом компьютере, а также через сеть - на серверах, где запущена соответствующая служба. Поскольку для серверов БД под управлением СУБД Microsoft® SQL Server™ 2005 эти возможности не требуются, указанную службу рекомендуется отключить.

Служба «Telnet» предоставляет клиентам Telnet сеансы терминала ASCII. Эта служба предусматривает поддержку проверки подлинности и поддержку следующих типов терминалов: ANSI, VT-100, VT-52 и VTNT. Для большинства серверов БД эти возможности не требуются, поэтому во всех рассматриваемых конфигурациях безопасности служба «Telnet» должна быть отключена.