СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

«Dallas Lock 8.0»

Инструкция по использованию MS SQL-сервера для СБ

RU.48957919.501410-02 И3

Листов 31

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

АИБ	администратор информационной безопасности
СУБД	система управления базами данных
БД	база данных
MS	Microsoft
ОС	операционная система
СБ	сервер безопасности
ОА	оболочка администратор
СЗИ НСД	средство защиты информации от несанкционированного доступа

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Общие сведения и назначения

Наличие системы управления базами данных позволит:

- сохранять данные аудита Сервера безопасности, Windows клиентов и Linux клиентов во внешней базе данных (по запросу АИБ, по расписанию, с периодом);
- выполнять необходимую выборку данных в соответствии с имеющимся функционалом фильтрации записей.

1.2 Системные требования

Системные требования представлены на таблице 1.

Таблица 1 – Системные требования

Версия MS SQL Server	Требования к системе
Microsoft SQL Server 2008 Express, Microsoft SQL Server 2008 Express with Advanced Services, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2	**Поддерживаемая операционная система:** Windows Server 2003 SP 2; Windows Server 2003 R2 SP2; Windows Server 2008; Windows Server 2008 SP2; Windows Server 2008 R2; Windows Server 2012; Windows 8; Windows 7; Windows Vista; Windows Vista Service Pack 1; Windows XP Service Pack 2; Windows XP Service Pack 3. **Требования к аппаратному обеспечению:** **1) Оперативная память:** • экспресс-выпуски: 512 МБ и выше; • все другие выпуски: 1 ГБ и выше. **2) Быстродействие процессора:** • процессор x86 с тактовой частотой 1,0 ГГц и выше; • процессор x64 с тактовой частотой 1,4 ГГц и выше; **3) Объем жесткого диска:** • 2,2 ГБ свободного места на диске.
Microsoft SQL Server Express 2012, Microsoft SQL Server 2012	**Поддерживаемая операционная система:** Windows 7; Windows 8; Windows 8.1; Windows Server 2008 R2; Windows Server 2008 Service Pack 2; Windows Server 2012; Windows Server 2012 R2; Windows Vista Service Pack 2. **Требования к аппаратному обеспечению:** **1) Оперативная память:**

	• экспресс-выпуски: 512 МБ и выше; • все другие выпуски: 1 ГБ и выше. **2) Быстродействие процессора:** • процессор x86 с тактовой частотой 1,0 ГГц и выше; • процессор x64 с тактовой частотой 1,4 ГГц и выше; **3) Объем жесткого диска:** • 2,2 ГБ свободного места на диске.
Microsoft SQL Server 2014, Microsoft SQL Server Express 2014	**Поддерживаемая операционная система:** Windows 7; Windows 7 Service Pack 1; Windows 8; Windows 8.1; Windows 10; Windows Server 2008 R2; Windows Server 2008 R2 SP1; Windows Server 2012; Windows Server 2012 R2. **Требования к аппаратному обеспечению:** **1) Оперативная память:** • экспресс-выпуски: 512 МБ и выше; • все другие выпуски: 1 ГБ и выше. **2) Быстродействие процессора:** • процессор x86 с тактовой частотой 1,0 ГГц и выше; • процессор x64 с тактовой частотой 1,4 ГГц и выше; **3) Объем жесткого диска:** • 4,2 ГБ свободного места на диске.

2 УСТАНОВКА СУБД

Сервер безопасности и MS SQL Server могут быть установлены на разных компьютерах (рекомендуется) или на одном компьютере.

Перед установкой сервера MS SQL должна быть выполнена установка компонента .NET Framework соответствующей версии и языкового пакета для этого компонента.

Общий порядок действий для установки сервера MS SQL с использованием указанных средств:

1. Включить в ОС компонент .NET Framework 3.5.
2. Установить .NET Framework 4.0.
3. Установить сервер MS SQL.

В данном руководстве рассмотрен пример установки и настройки Microsoft SQL Server 2008 Express with Advanced Services в ОС Windows Server 2008.

2.1 Установка MS SQL Server 2008 Express with Advanced Services

1. Запустить программу-установщик с правами администратора.
2. В разделе «Планирование» нажать пункт «Средство проверки конфигурации» (Рис. 1).

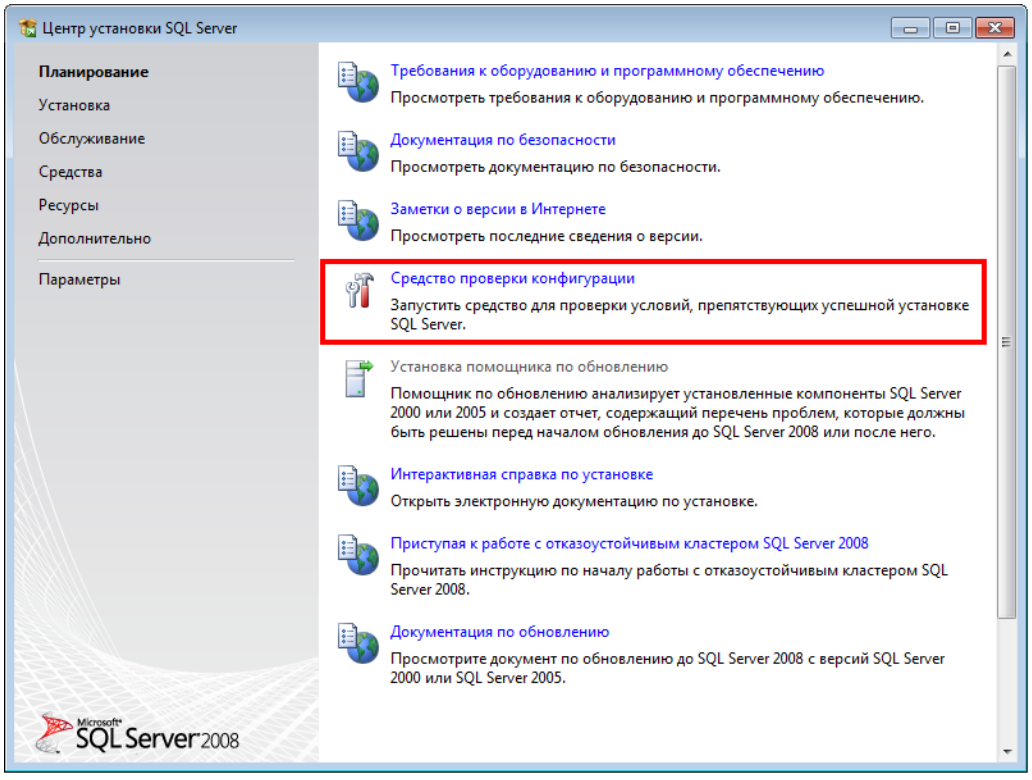

Рис. 1 – Раздел «Планирование»

3. Нажать кнопку «Показать подробности» и убедиться, что все проверки успешно пройдены. Если были обнаружены какие-либо проблемы, то необходимо их устранить и повторить процедуру проверки, нажав кнопку «Включить заново».

Затем закрыть данное окно кнопкой «ОК» (Рис. 2).

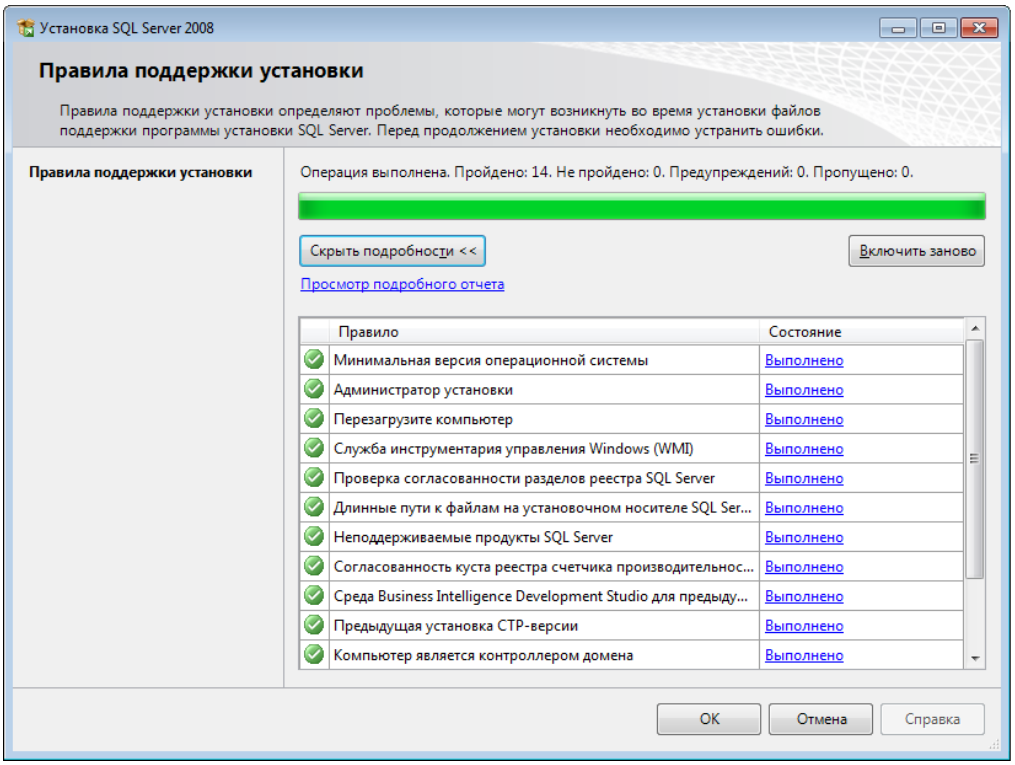

Рис. 2 – Проверка правил поддержки установки

4. Открыть раздел «Установка» и нажать на пункт «Новая установка изолированного SQL Server или добавление компонентов к существующему экземпляру» (Рис. 3).

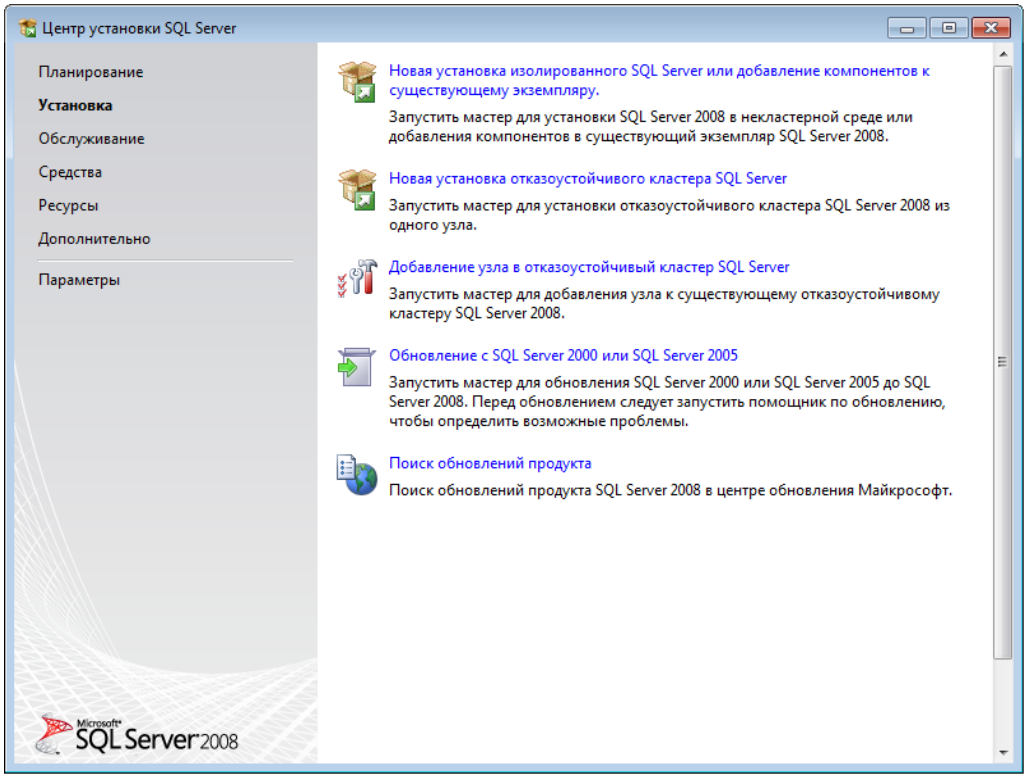

Рис. 3 – Раздел «Установка»

5. Нажать кнопку «Показать подробности» и убедиться, что все проверки успешно

пройдены. Если будут обнаружены какие-то проблемы, то необходимо их устранить и запустить повторную проверку кнопкой «Включить заново». После нажать кнопку «Далее» (Рис. 4).

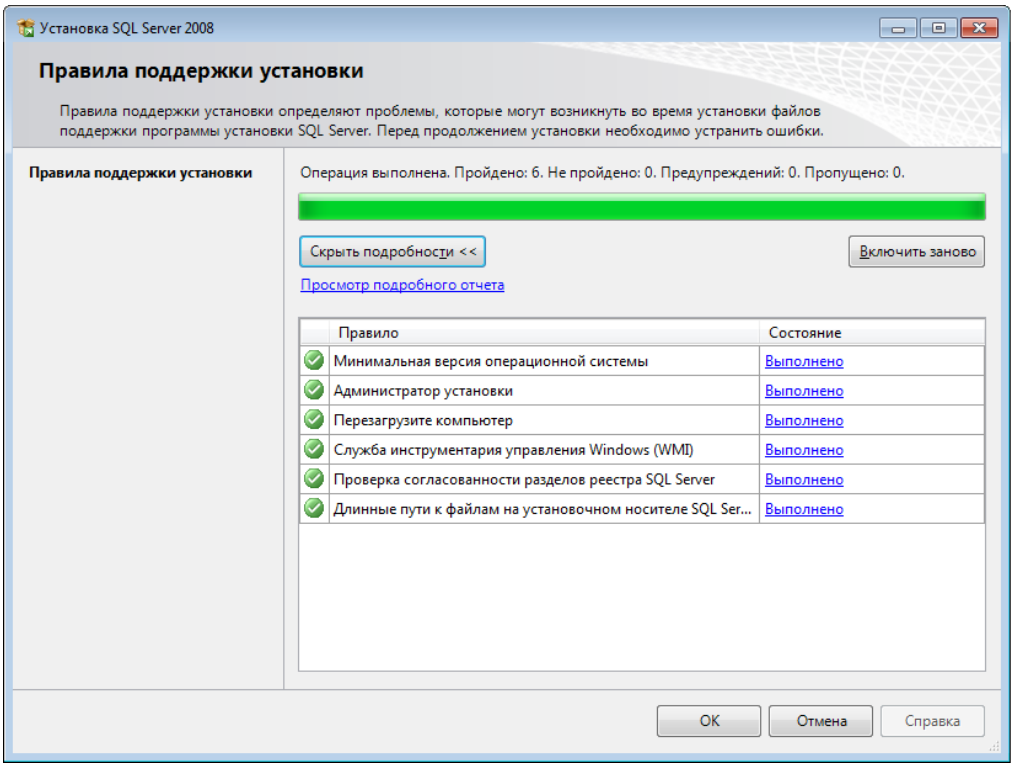

Рис. 4 – Проверка правил поддержки установки

6. Ввести ключ продукта (для Express версии не требуется) и нажать кнопку «Далее» (Рис. 5).

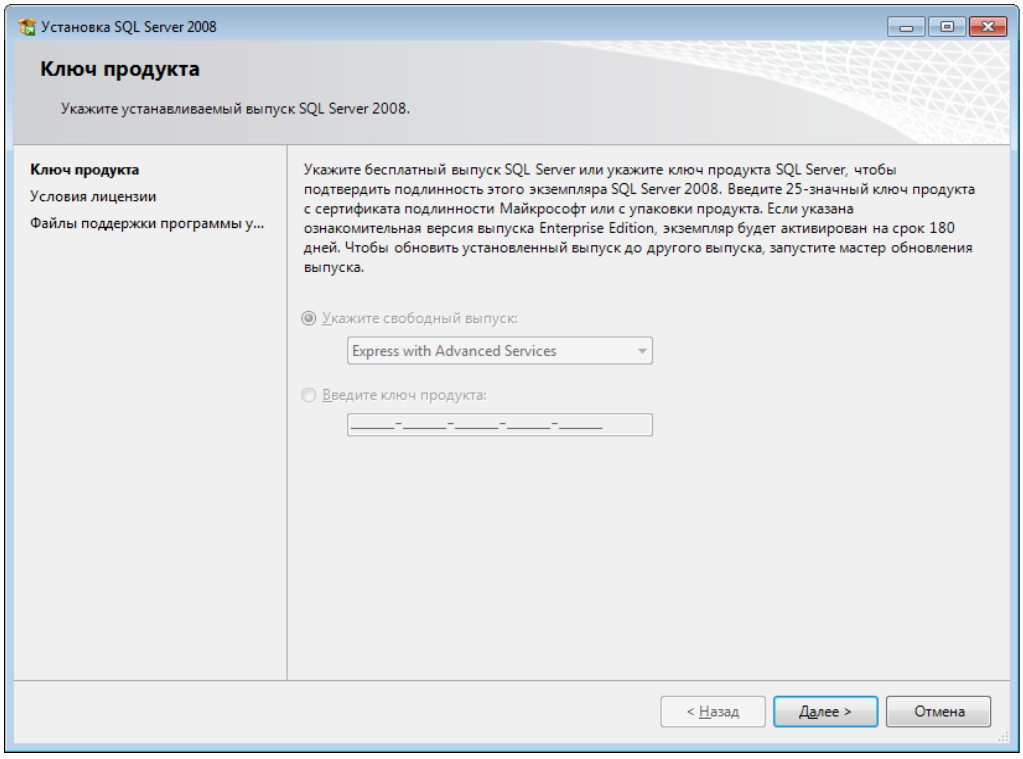

Рис. 5 – Ввод ключа продукта

7. Прочитать лицензию, установить флаг «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее» (Рис. 6).

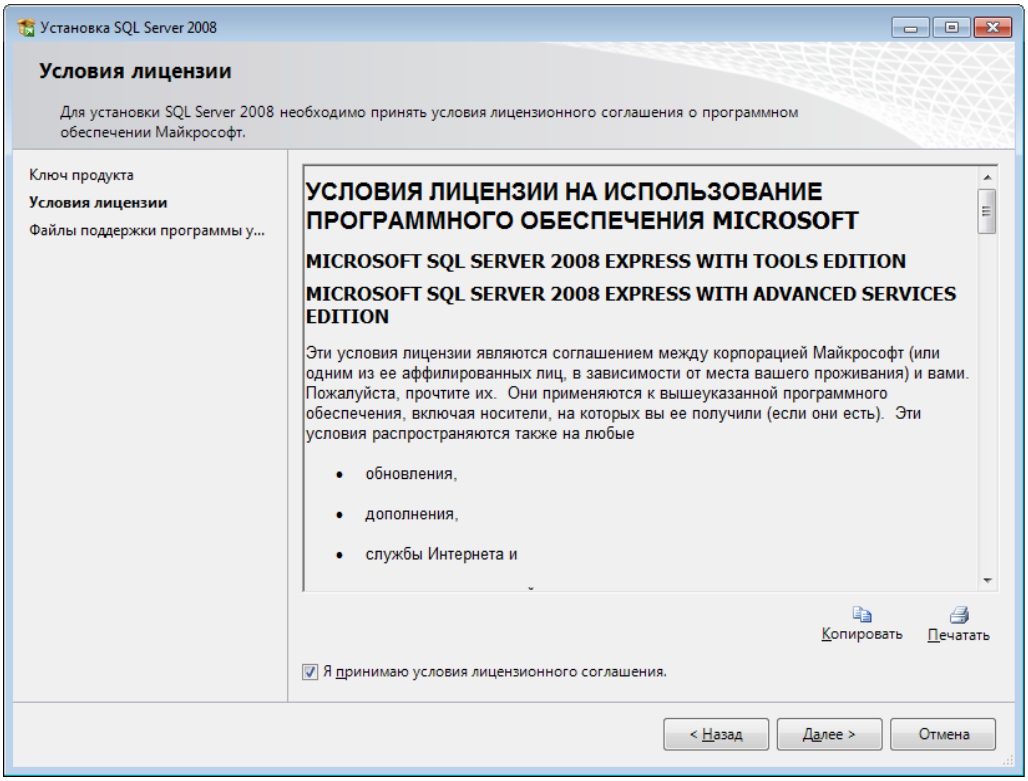

Рис. 6 – Условия лицензии

8. Нажать кнопку «Установить» (Рис. 7).

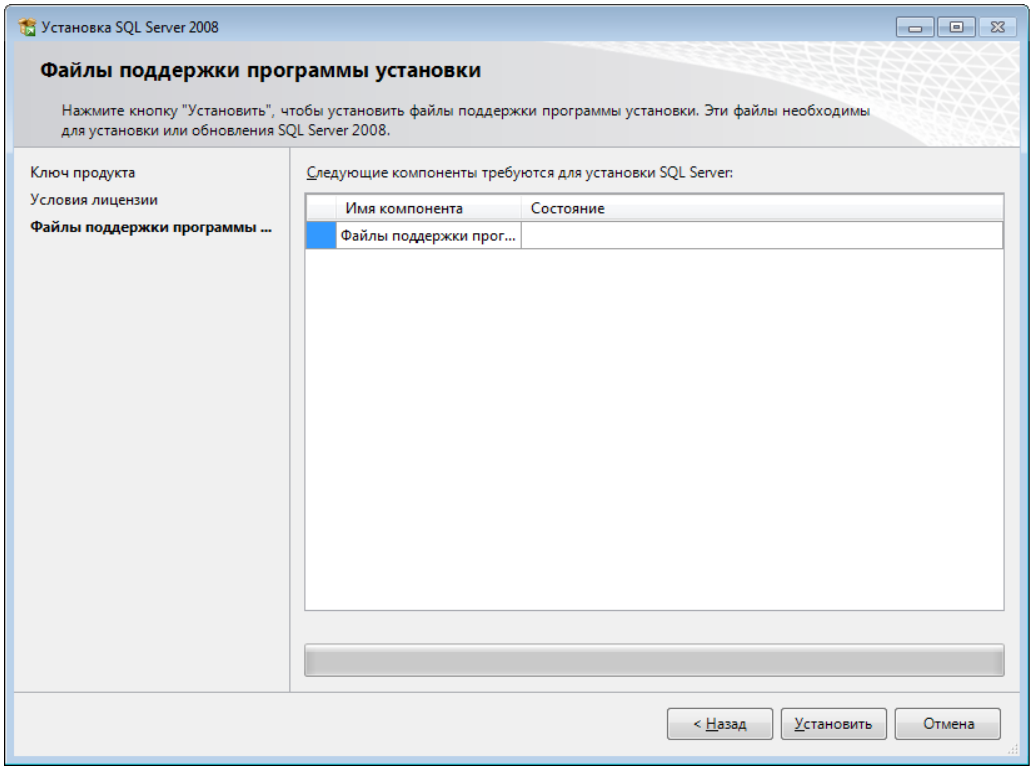

Рис. 7 – Файлы поддержки программы установки

9. Нажать кнопку «Показать подробности» и убедиться, что все проверки успешно

пройдены. Если были обнаружены какие-либо проблемы, то необходимо их устранить и повторить процедуру проверки, нажав кнопку «Включить заново». После нажать кнопку «Далее» (Рис. 8).

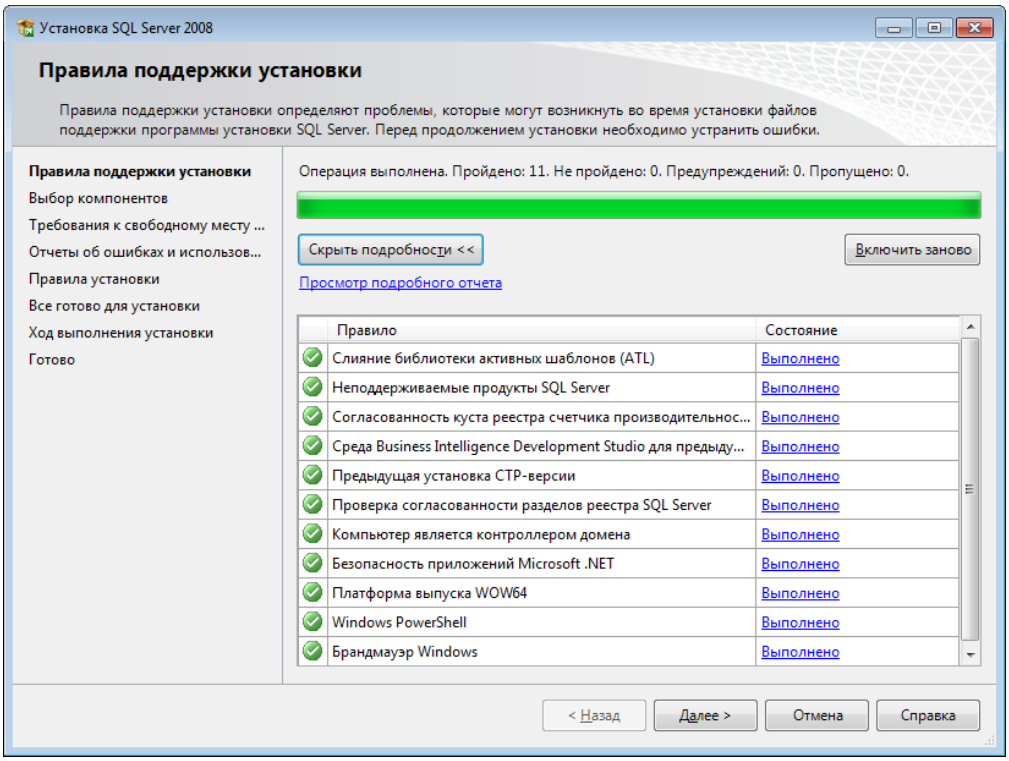

Рис. 8 – Проверка правил поддержки установки

10. Выбрать компоненты для установки, как показано на рисунке, и нажать кнопку «Далее» (Рис. 9).

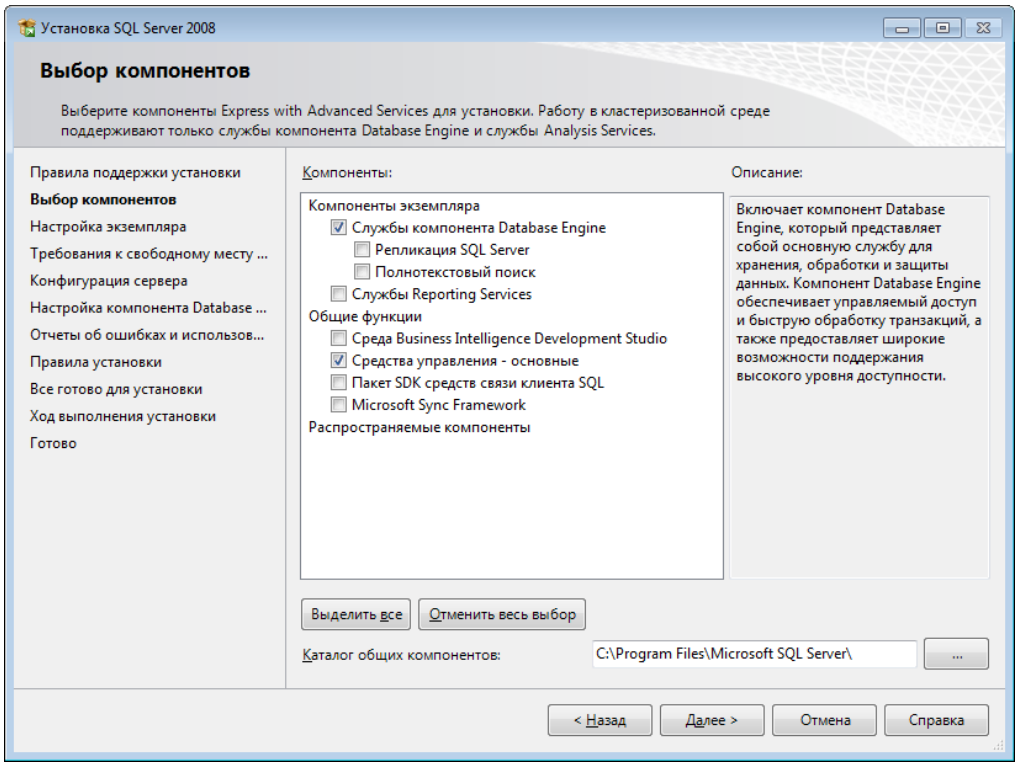

Рис. 9 – Выбор компонентов

11. Выбрать значение «Экземпляр по умолчанию» и нажать далее (Рис. 10).

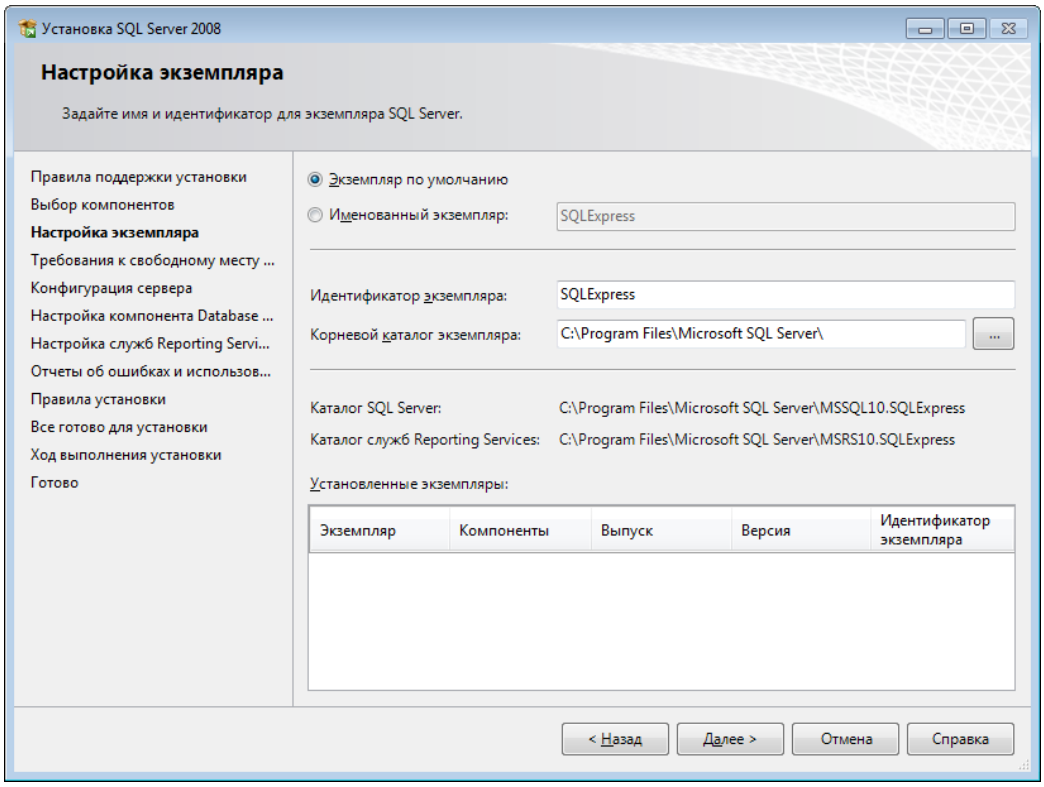

Рис. 10 – Настройка экземпляра

12. Нажать кнопку «Далее» (Рис. 11).

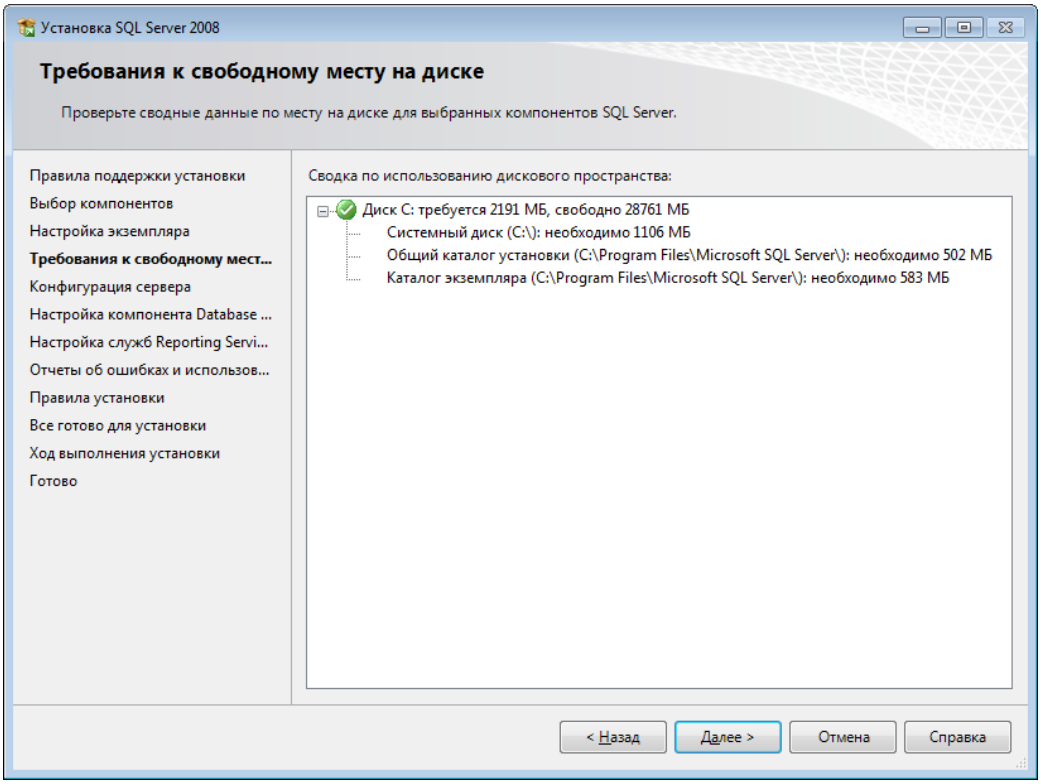

Рис. 11 – Требования к свободному месту на диске

13. Настроить службы, как показано на рисунке и перейти на вкладку «Параметры сортировки» (Рис. 12).

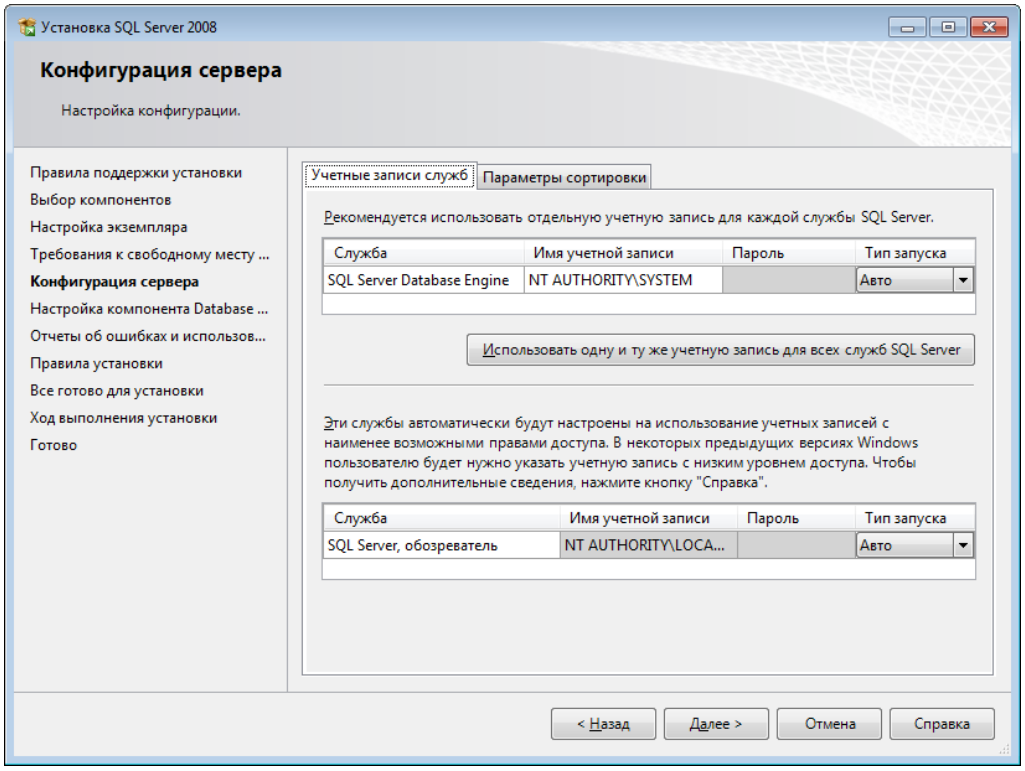

Рис. 12 – Учетные записи служб

14. Настроить параметры, как показано на рисунке и нажать кнопку «Далее» (Рис. 13).

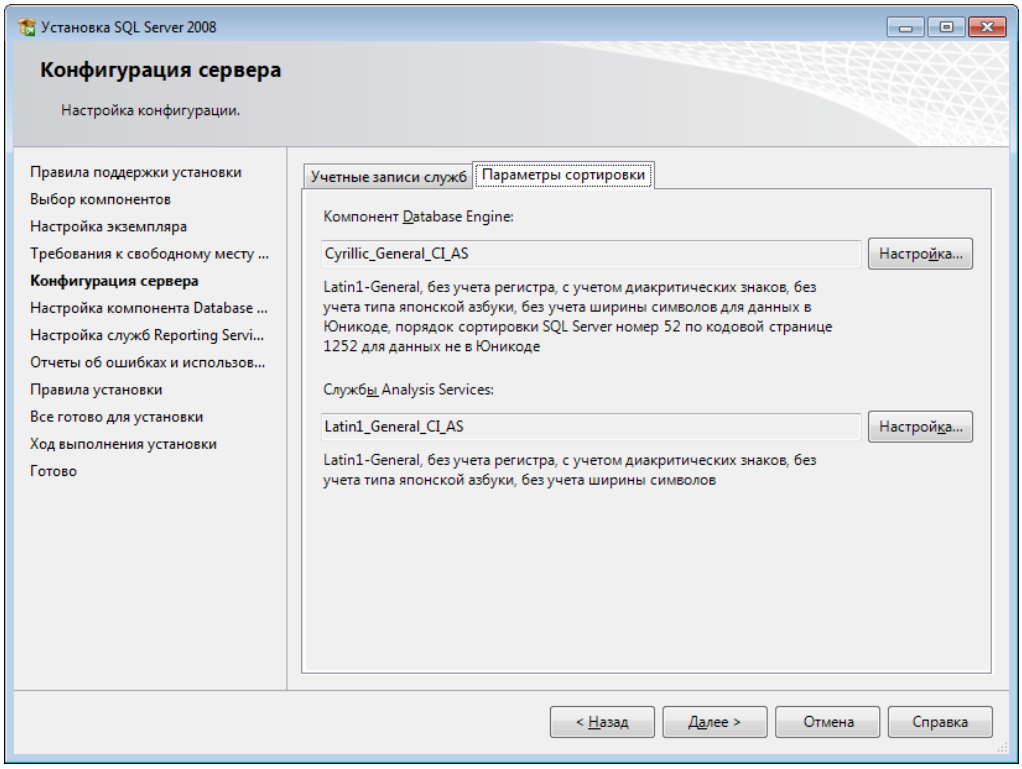

Рис. 13 – Параметры сортировки

Чтобы изменить параметр, необходимо нажать на кнопку «Настройка» и установить значения, как показано на рисунке (Рис. 14).

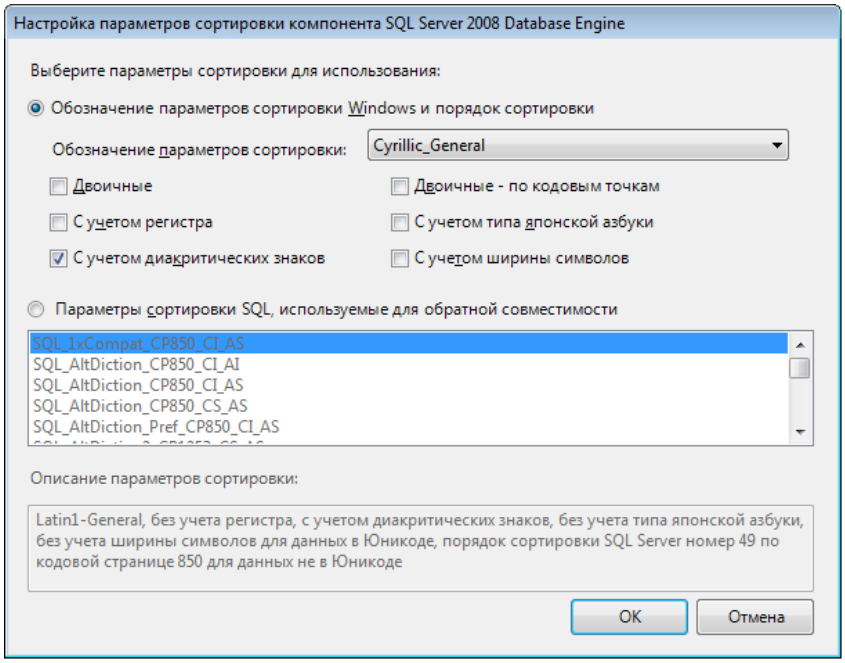

Рис. 14 – Настройка параметров сортировки компонента

15. Выбрать значение «Смешанный режим» и задать пароль для встроенной учетной записи администратора «sa». Данная учетная запись обладает максимальными правами доступа на SQL-сервере.

    Также можно указать учетные записи пользователей или группы пользователей, которые будут обладать максимальными правами доступа на SQL-сервере. Далее необходимо перейти на закладку «Каталоги данных» (Рис. 15).

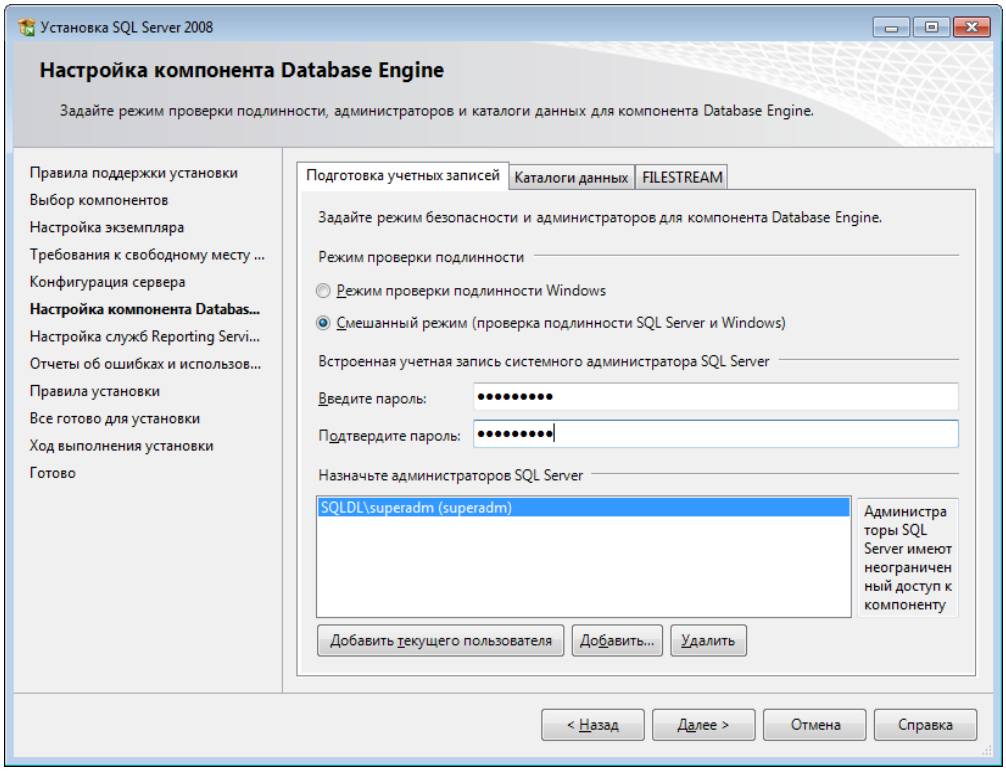

Рис. 15 – Подготовка учетных записей

16. В поле «Корневой каталог данных» возможно ввести путь к папке, где будут размещаться файлы БД (рекомендуется использовать отдельный от ОС физический диск), и нажать кнопку «Далее» (Рис. 16).

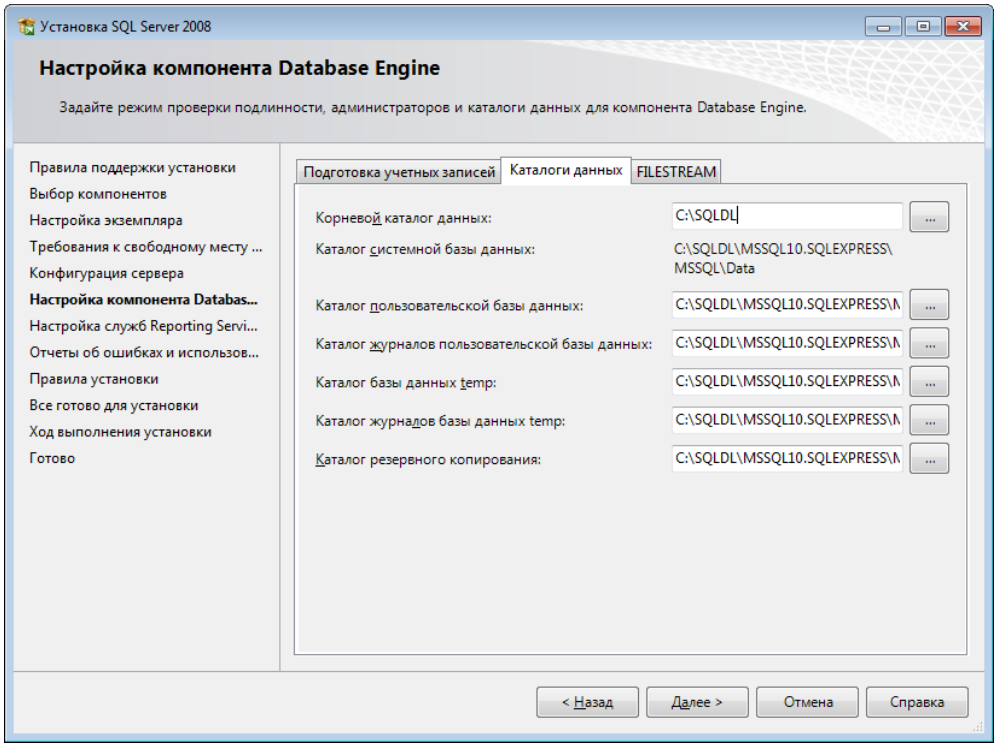

Рис. 16 – Выбор корневого каталога данных

17. Выбрать значение «Установить конфигурацию по умолчанию для работы в собственном режиме» и нажать далее (Рис. 17).

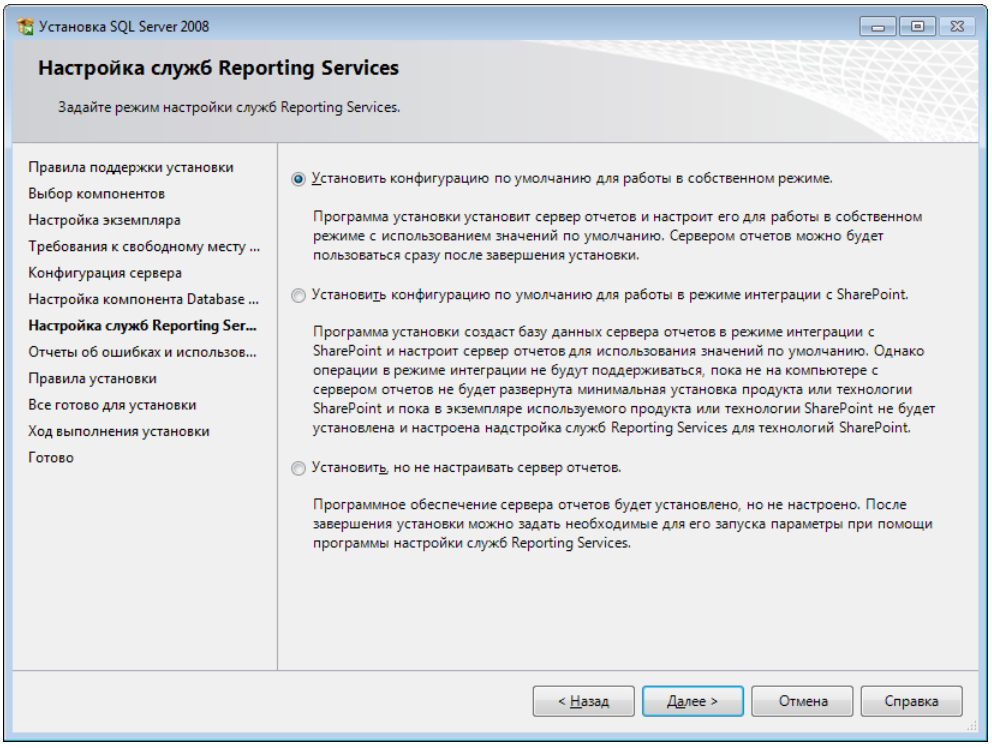

Рис. 17 – Настройка служб Reporting Services

18. Снять флаги с двух параметров при необходимости, и нажать кнопку «Далее» (Рис. 18).

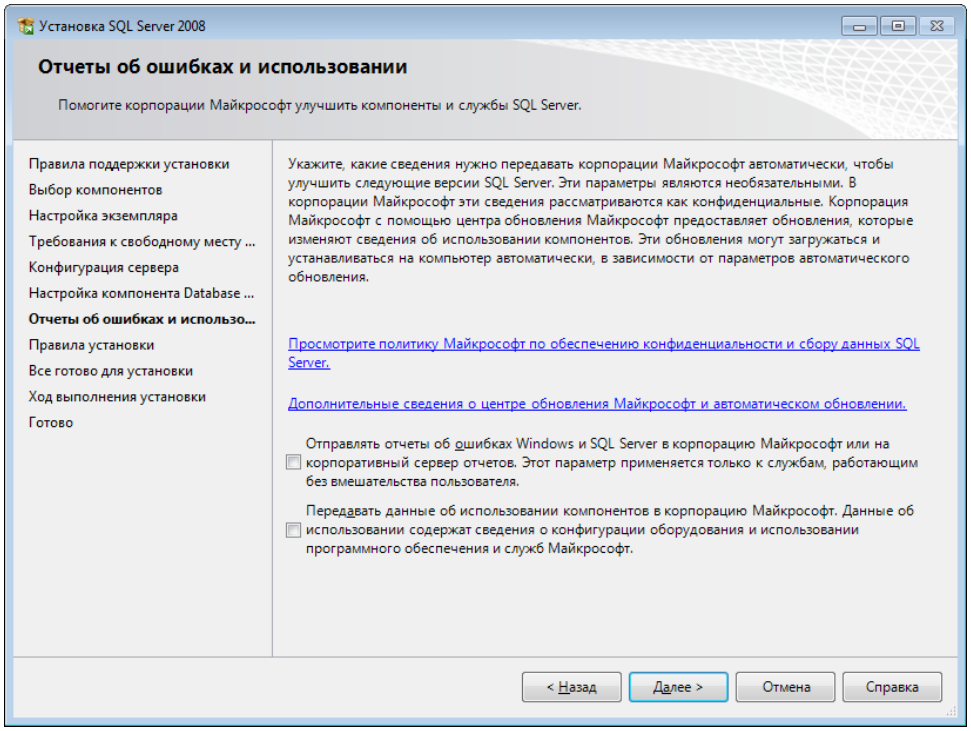

Рис. 18 – Отчеты об ошибках и использовании

19. Нажать кнопку «Показать подробности» и убедиться, что все проверки успешно пройдены. Если были обнаружены какие-либо проблемы, то необходимо их устранить и повторить процедуру проверки, нажав кнопку «Включить заново». После нажать кнопку «Далее» (Рис. 19).

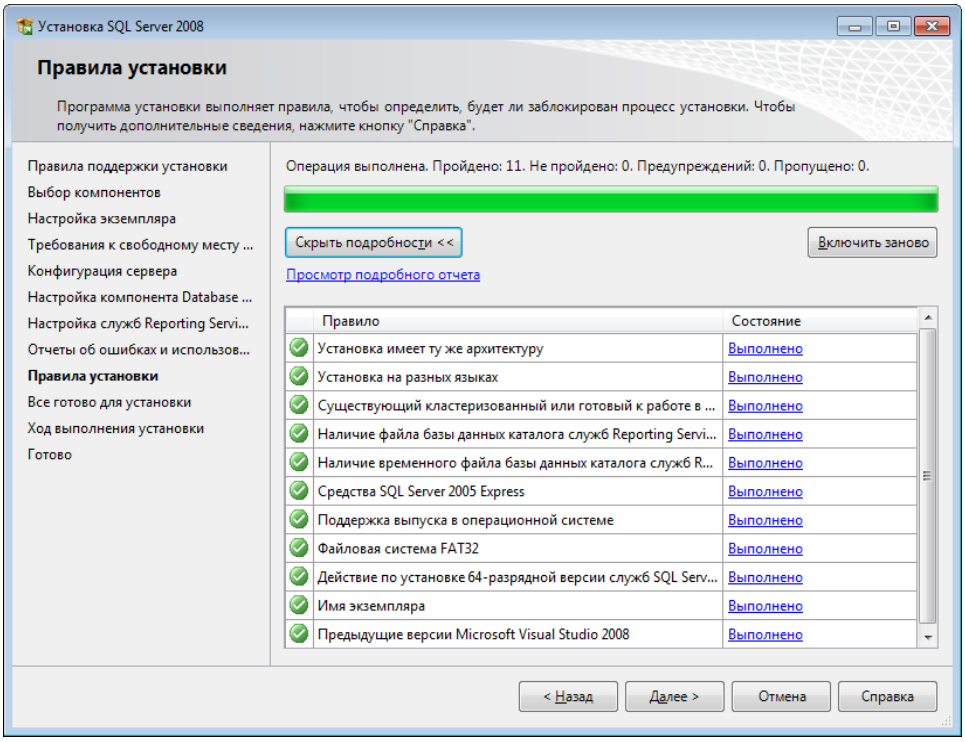

Рис. 19 – Проверка правил установки

20. Нажать кнопку «Установить» (Рис. 20).

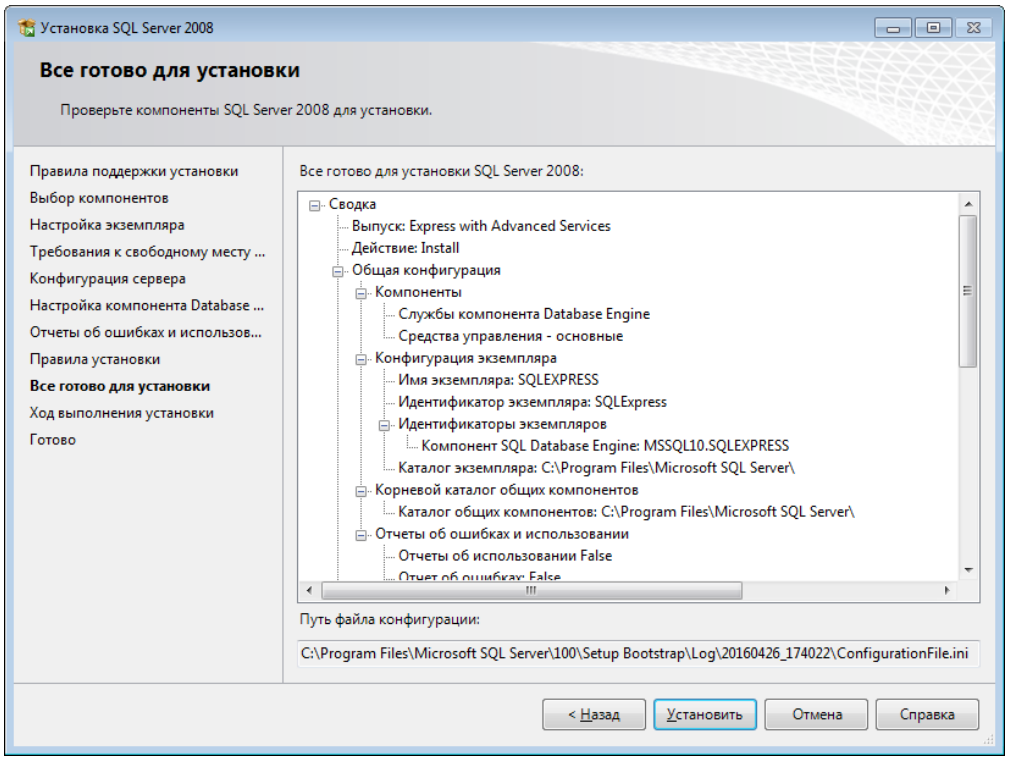

Рис. 20 – Сводка компонентов SQL Server 2008

21. После завершения установки нажать кнопку «Далее» (Рис. 21).

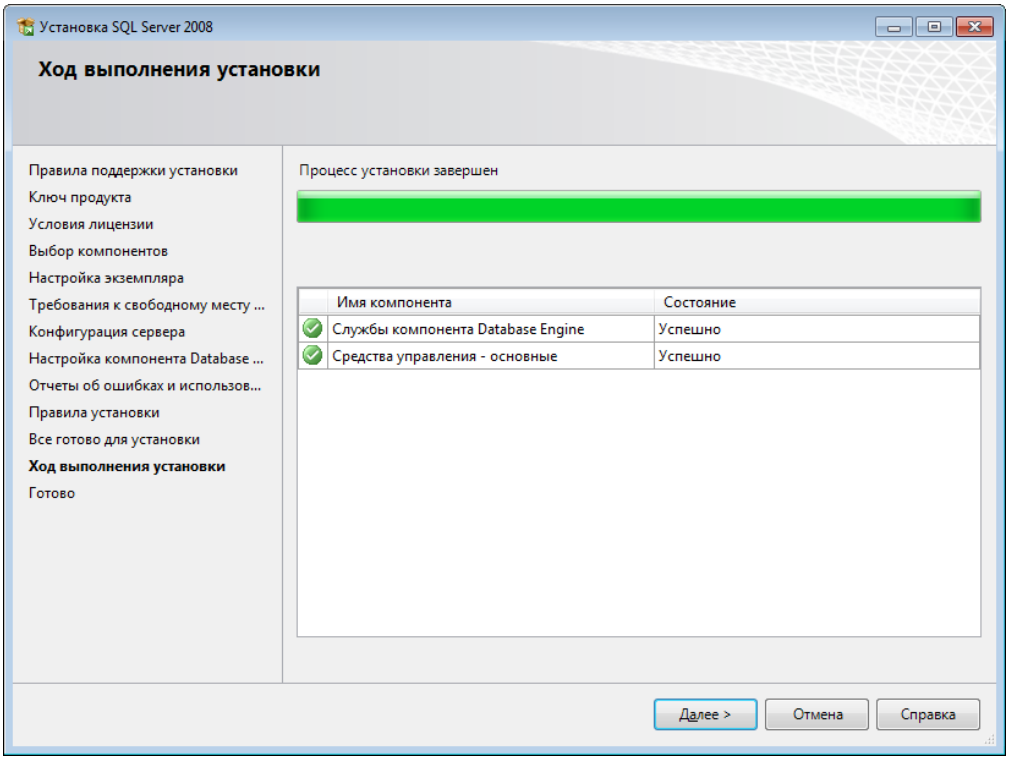

Рис. 21 – Ход выполнения установки

22. Нажать кнопку «Закрыть» (Рис. 22).

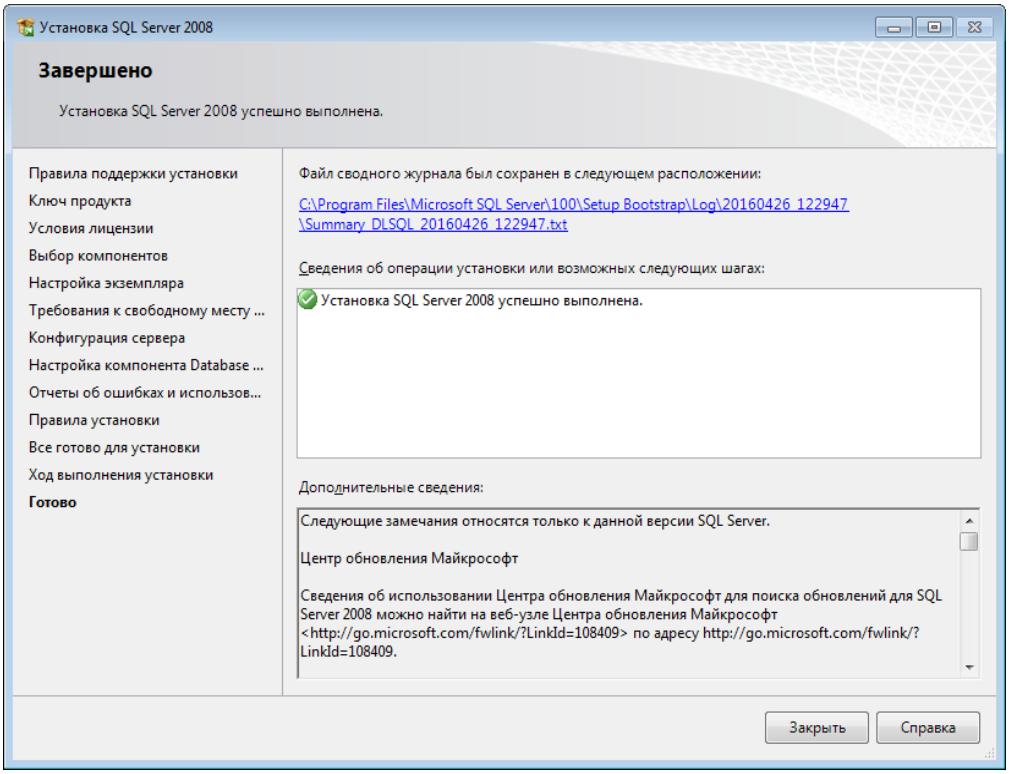

Рис. 22 – Завершение установки

23. Запустить утилиту «Диспетчер конфигурации SQL Server» открыв «Пуск → Все программы → Microsoft SQL Server 2008 → Средства настройки → Диспетчер конфигурации SQL Server». В разделе «Сетевая конфигурация SQL Server → Протоколы для <Имя_экземляра_БД>», нажать правой кнопкой по параметру «TCP/IP» и контекстном меню выбрать пункт «Свойства» (Рис. 23).

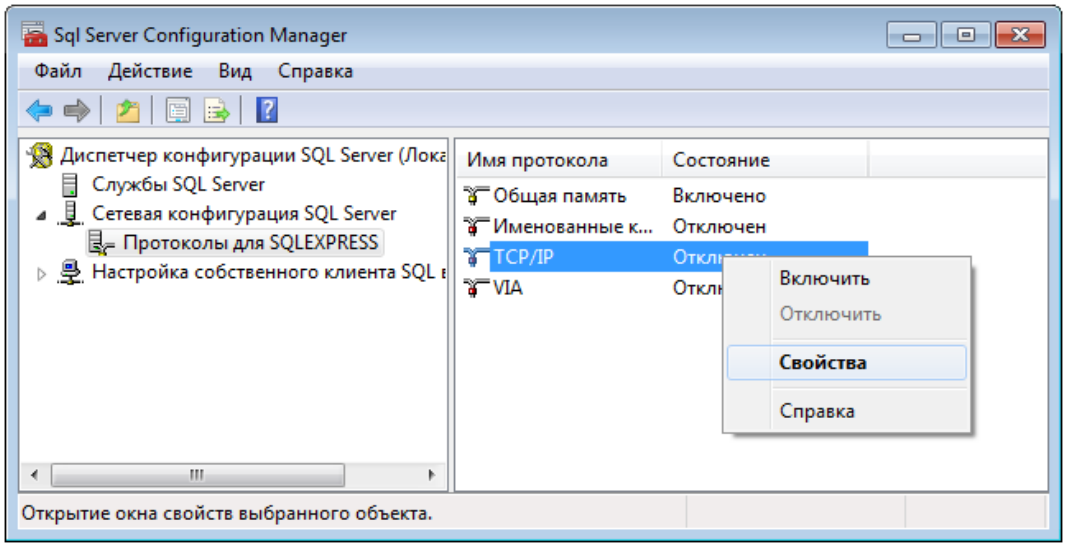

Рис. 23 – Вызов свойств параметра TCP/IP

24. Во вкладке «Протокол» установить значение «Да» для параметра «Включено». На вкладке «IP-адреса» в разделе «IPAII» для параметров «TCP-порт» и «Динамические TCP-порты», необходимо указать порт «1433» и пустое значение соответственно

(Рис. 24).

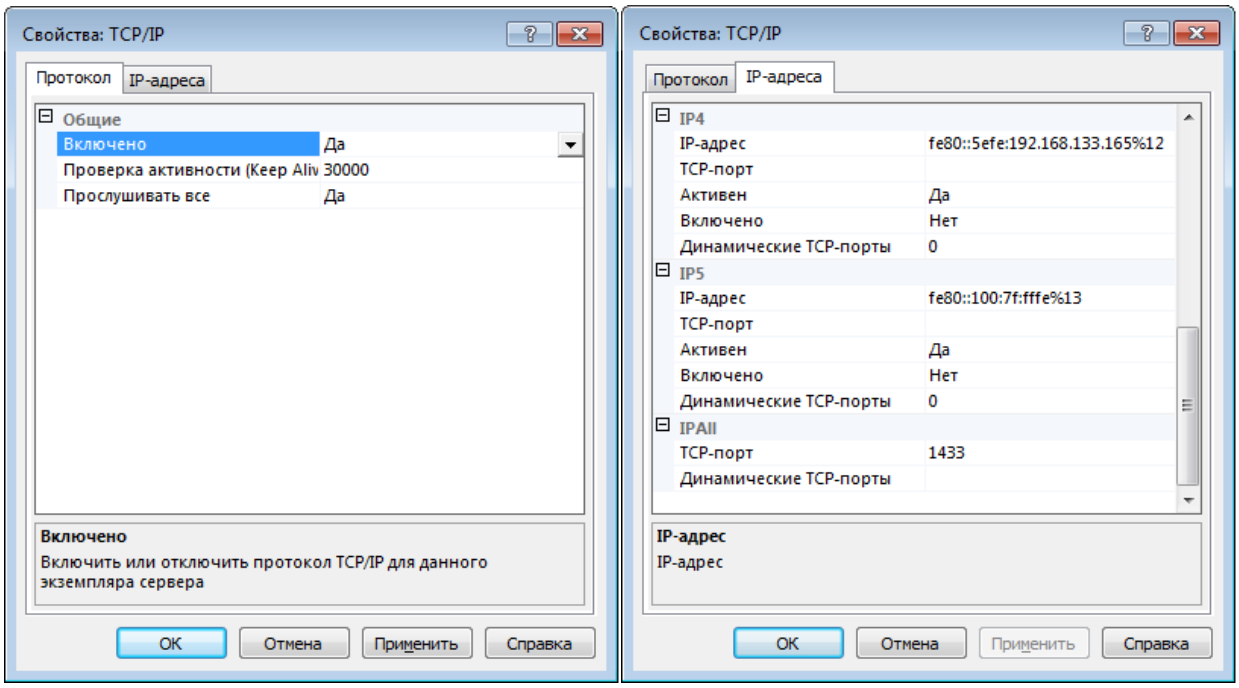

Рис. 24 – Настройка свойств параметра TCP/IP

25. В разделе «Службы SQL Server» нажать правой кнопкой мыши по службе «SQL Server <Имя_экземпляра_БД>» и в контекстном меню выбрать пункт «Перезапустить» (Рис. 25).

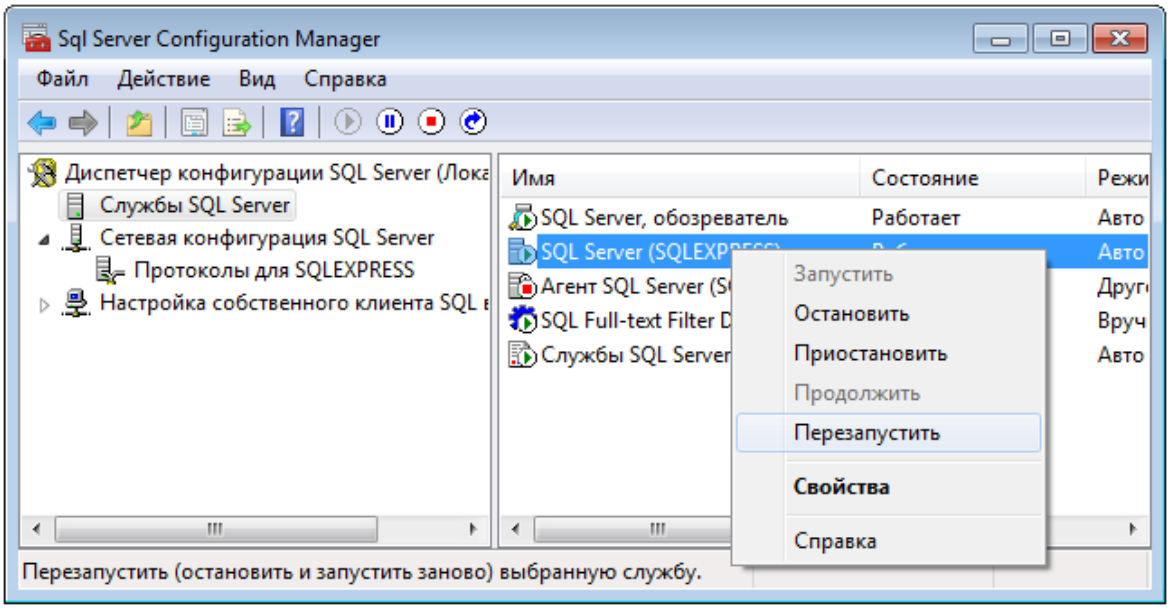

Рис. 25 – Перезапуск службы SQL Server

3 ПОДКЛЮЧЕНИЕ БД К СБ

Администратору ИБ предоставляется возможность использовать встроенную систему хранения данных СЗИ НСД Dallas Lock 8.0 или СУБД MS SQL Server.

Для корректного взаимодействие сервера безопасности и СУБД MS SQL необходимо выполнение следующих условий на компьютере сервера MS SQL:

1. Если сервер MS SQL установлен на удаленном компьютере – требуется включить службу «Обозреватель SQL Server». Это возможность сделать, как при установке СУБД, так и после (Рис. 26, Рис. 27).

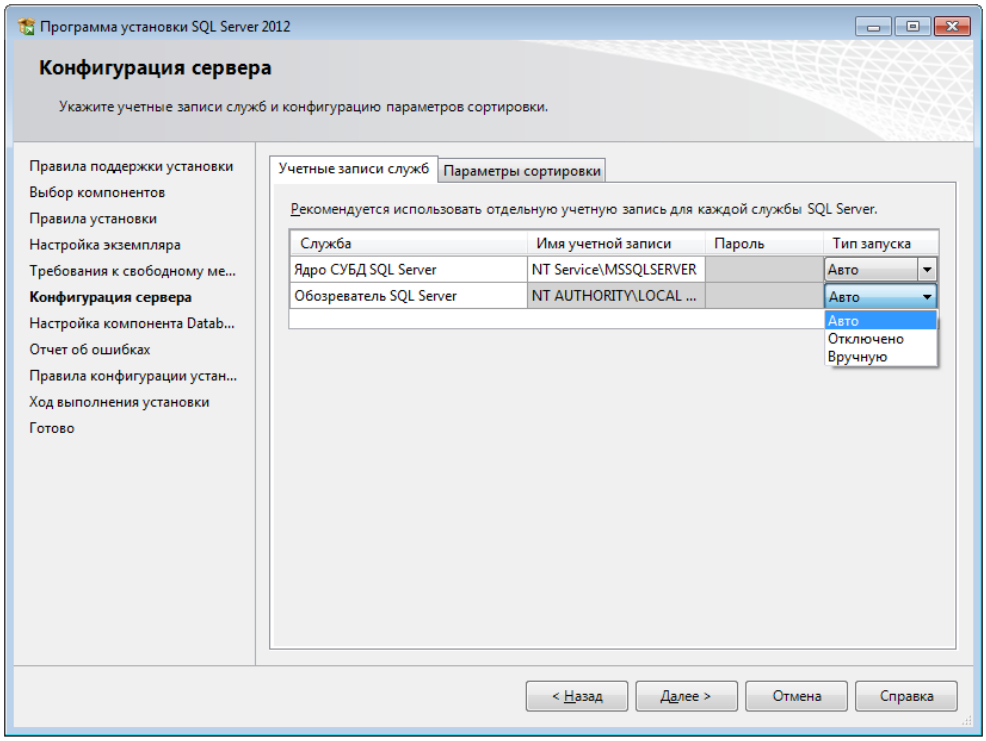

Рис. 26 – Включение обозревателя SQL Server в процессе установки MS SQL

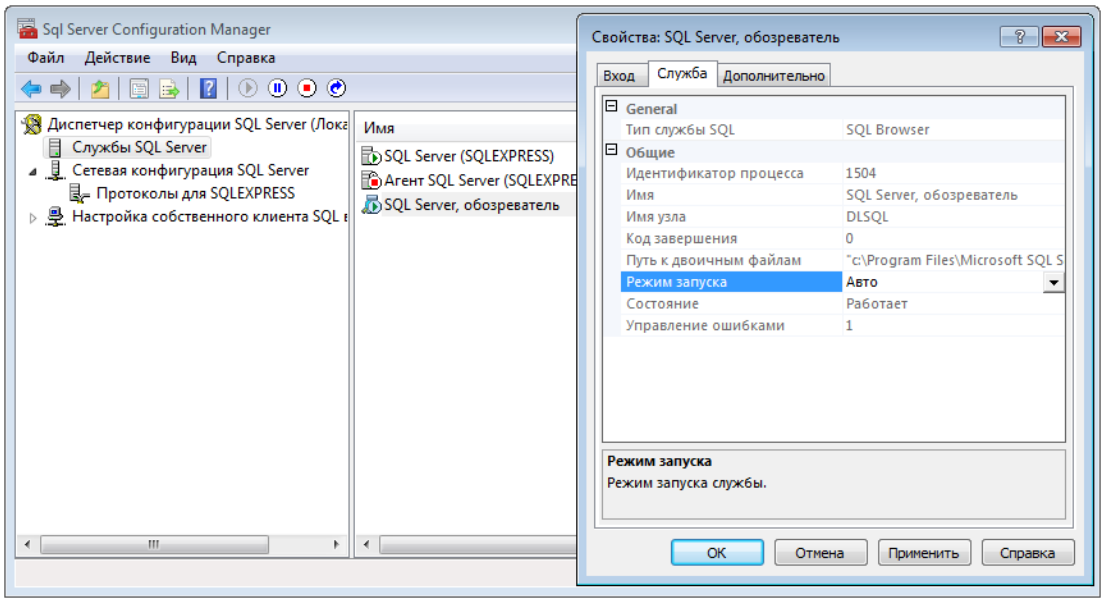

Рис. 27 – Включение обозревателя в диспетчере конфигурации SQL Server

2. Включена поддержка сортировки кириллицы для экземпляра базы данных – для этого при установке экземпляра необходимо в параметрах сортировки для компонента Database Engine указать значение «Cyrillic_General_CI_AS» (Рис. 28).

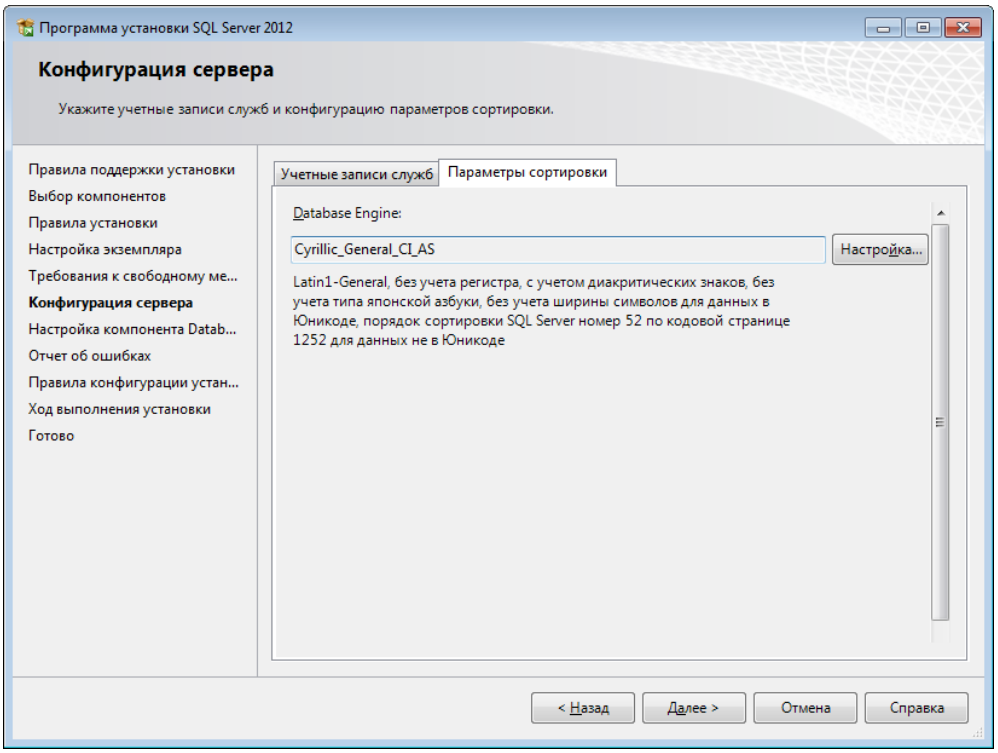

Рис. 28 – Параметры сортировки

3. Включен режим проверки подлинности SQL Server и Windows – для этого на сервере MS SQL необходимо включить «Смешанный режим» (Рис. 29).

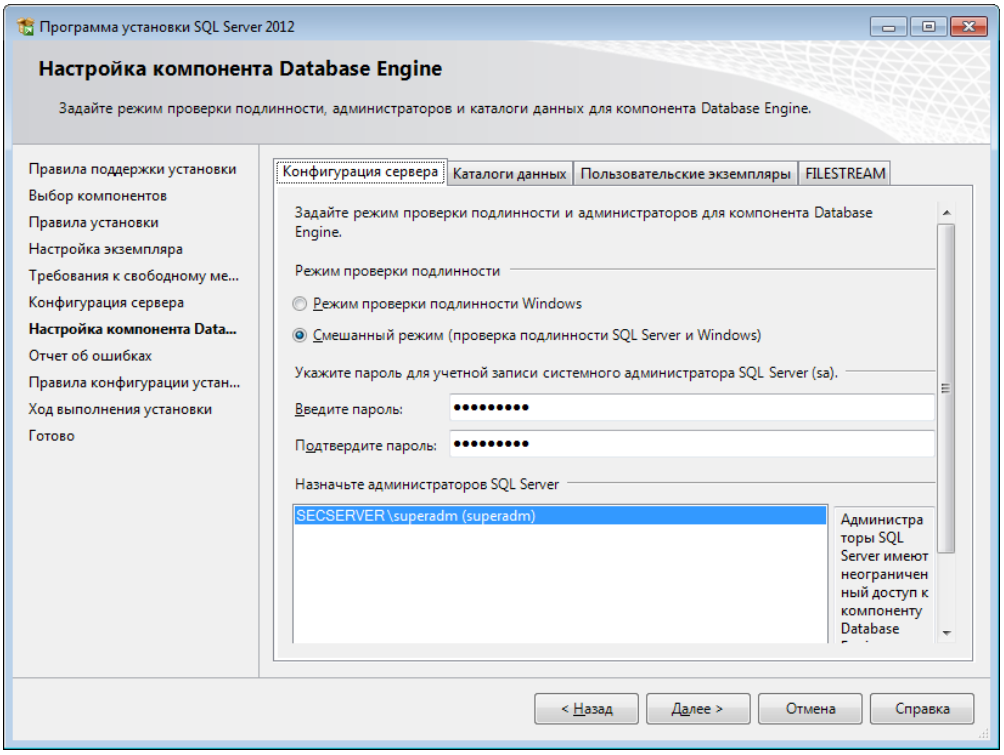

Рис. 29 – Режим проверки подлинности

4. Включен протокол TCP/IP для необходимого экземпляра сервера. Протокол по умолчанию отключен при использовании SQL Server Express. Для включения протокола необходимо запустить «Диспетчер конфигурации SQL Server» и перейти к разделу "Сетевая конфигурация SQL Server → Протоколы для <имя_ экземпляра_ БД>". Далее нужно открыть свойства параметра "TCP/IP" и во вкладке "Протокол" указать значение "Да" для параметра "Включено" (Рис. 30).

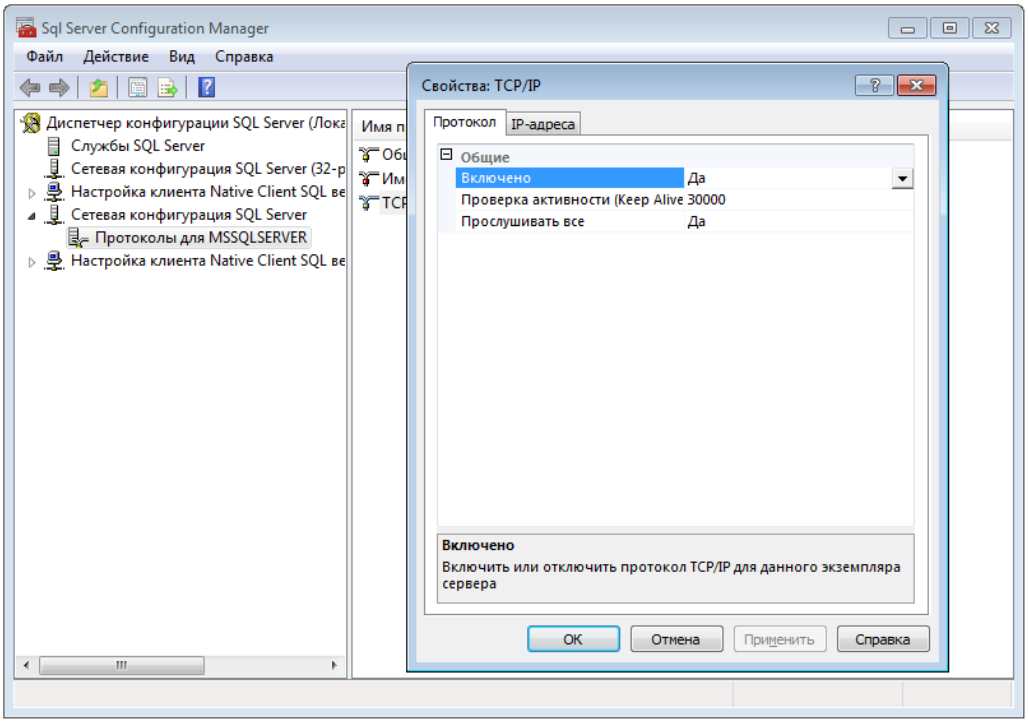

Рис. 30 – Включение протокола TCP/IP

5. Если сервер MS SQL установлен на отдельном компьютере – в брандмауэре необходимо разрешить входящие соединения по протоколу TCP/IP на порт 1433, а также по протоколу UDP на порт 1434. Для этого требуется в стандартном «Брандмауэре Windows» (Панель управления → Брандмауэр Windows), перейти в раздел «Правила для входящих подключений» и на панели «Действия» нажать кнопку «Создать правило…» (Рис. 31).

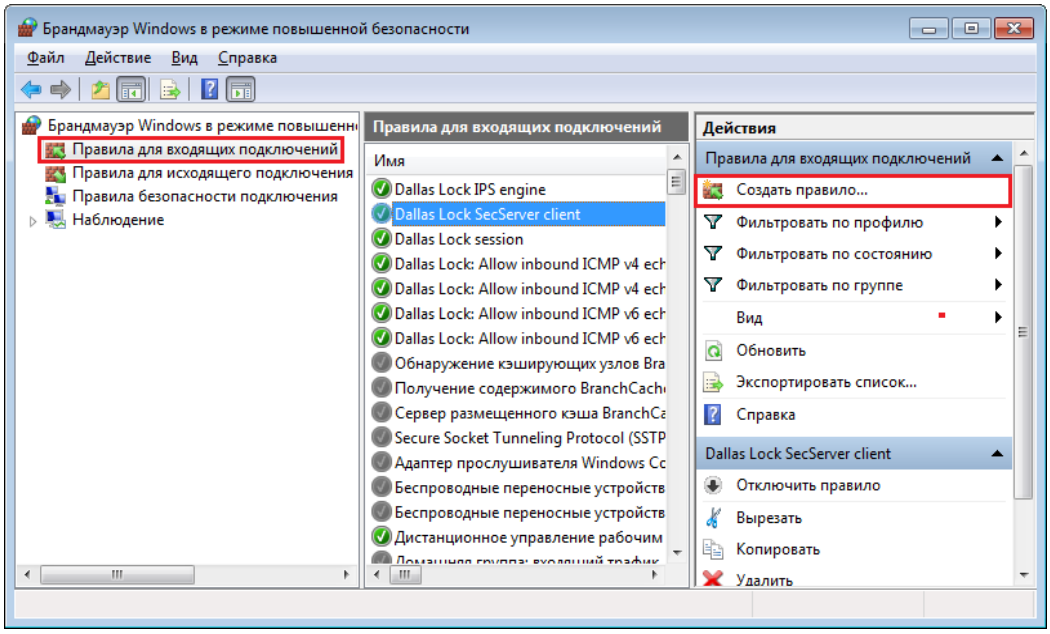

Рис. 31 – Создание правила для входящего соединения

Далее необходимо, выбрать тип правила «Для порта» и нажать далее. После чего выбрать параметр «Протокол TCP» и указать в поле «Определенные локальные порты» 1433 порт (Рис. 32). В следующем окне выбрать параметр «Разрешить подключение». Создание правила для «Протокола UDP» аналогично.

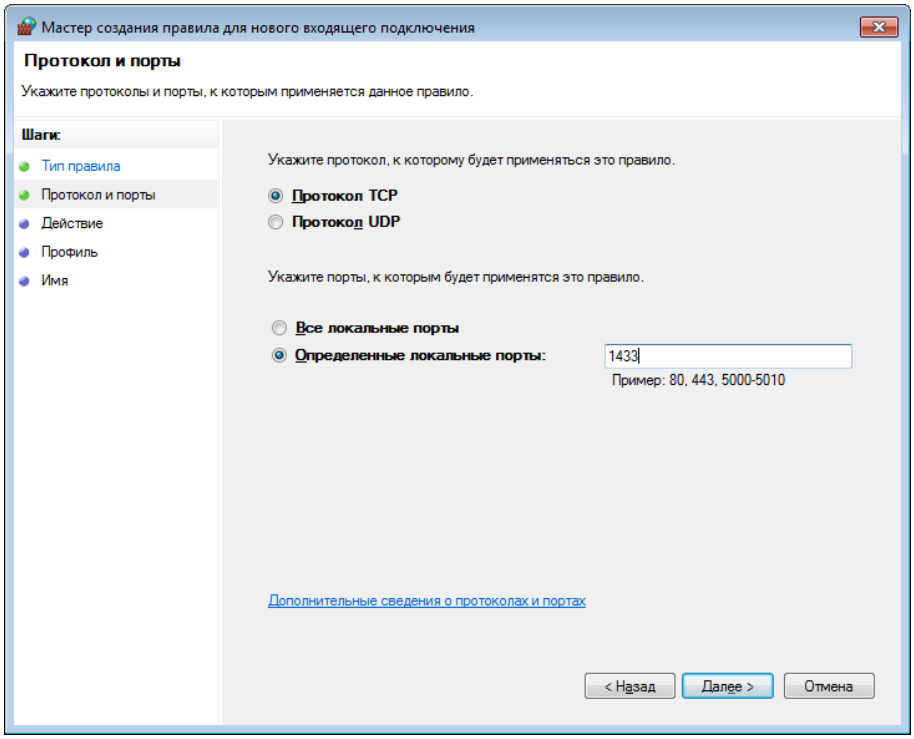

Рис. 32 – Создание правила для входящего соединения по протоколу TCP

6. На СБ в оболочке администратора СЗИ НСД Dallas Lock 8.0, активировано 2 сессии-исключения «Для работы MsSQL» (Рис. 33).

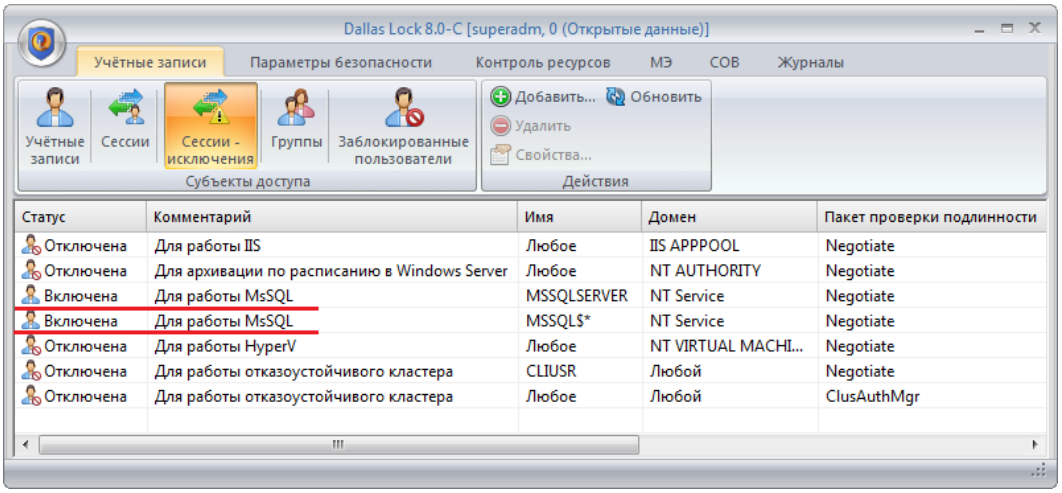

Рис. 33 – Сессии-исключения

3.1 Подключение БД в процессе установки СБ

В процессе установки СБ, возможно подключить существующую БД, либо создать новую. Для этого необходимо в окне «Параметры хранения журналов» поставить флаг у параметра «Использовать базу данных MS SQL Server» и заполнить требуемые поля.

3.1.1 Подключение к существующей БД

Для подключения к существующей базе данных необходимо указать (Рис. 34):

1. Имя ПК, на котором установлена БД (поле «Сервер базы данных»).
2. Порт подключения.
3. Имя базы данных.
4. Логин и пароль пользователя базы данных.

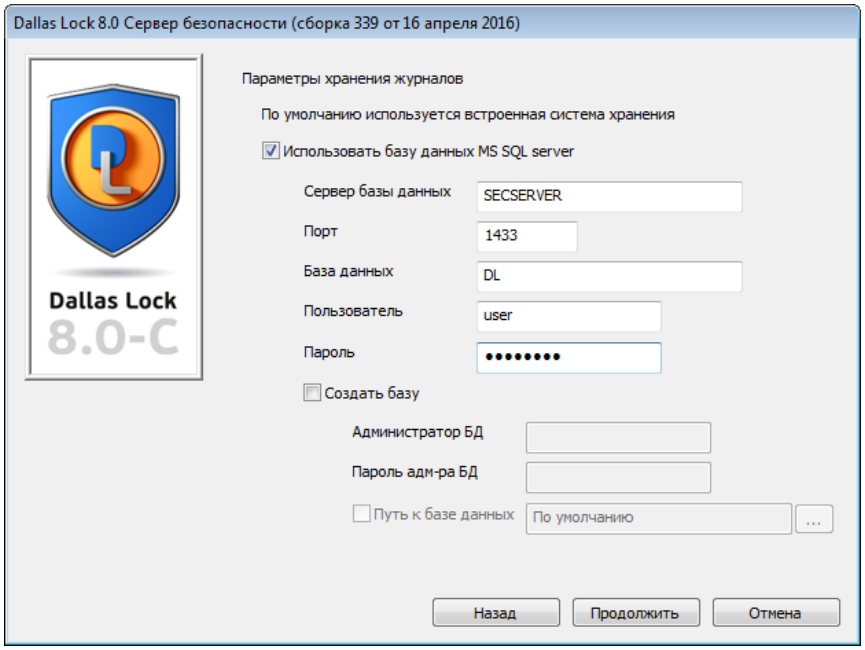

Рис. 34 – Подключение к существующей БД в процессе установки СБ

3.1.2 Создание новой БД и пользователя

Для создания новой БД и пользователя необходимо:

1. Поставить флаг у параметра «Создать базу».
2. Указать логин и пароль администратора БД, от имени которого будет осуществляться создание БД.
3. Задать имя нового пользователя, его пароль и название создаваемой БД, в полях «Пользователь», «Пароль» и «База данных» соответственно (Рис. 35).

   При необходимости указывается путь к базе данных.

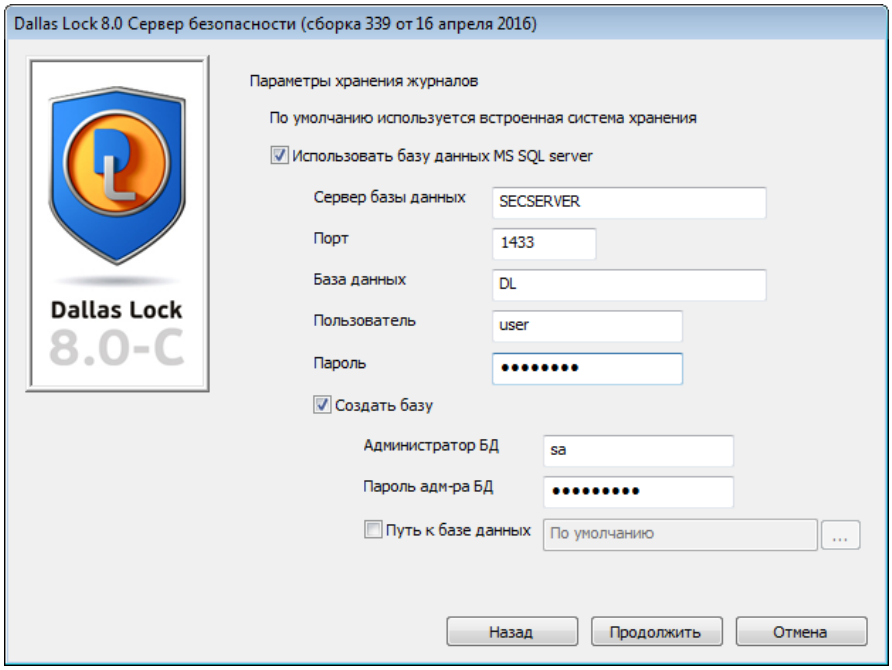

Рис. 35 – Создание новой БД и пользователя

В случае ввода неверных данных, появится окно с описанием ошибки (Рис. 36).

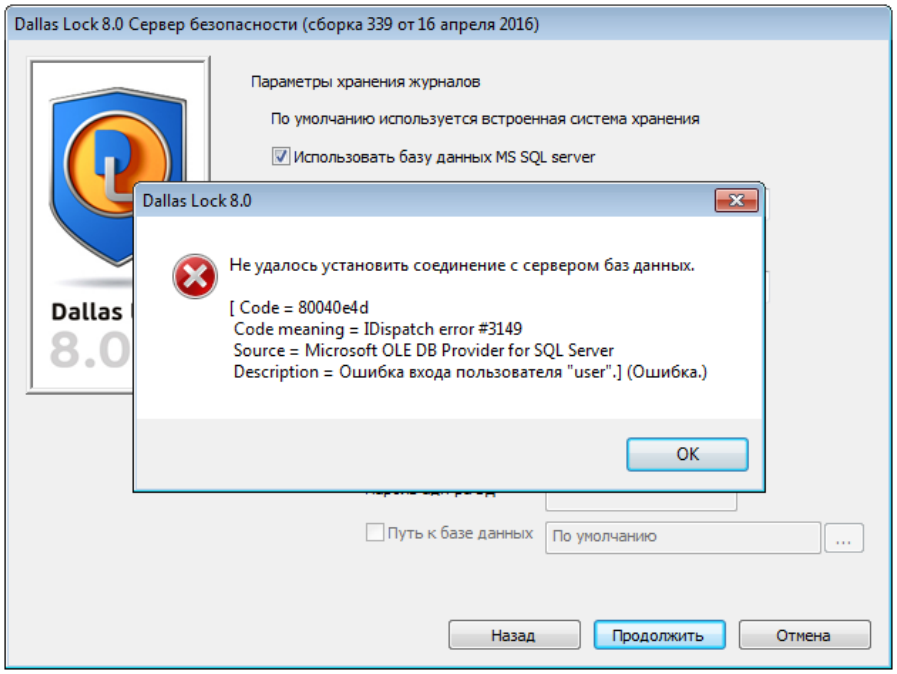

Рис. 36 – Ошибка при вводе неверных данных

При выполнении операции, откроется следующее окно установки СБ (Рис. 37).

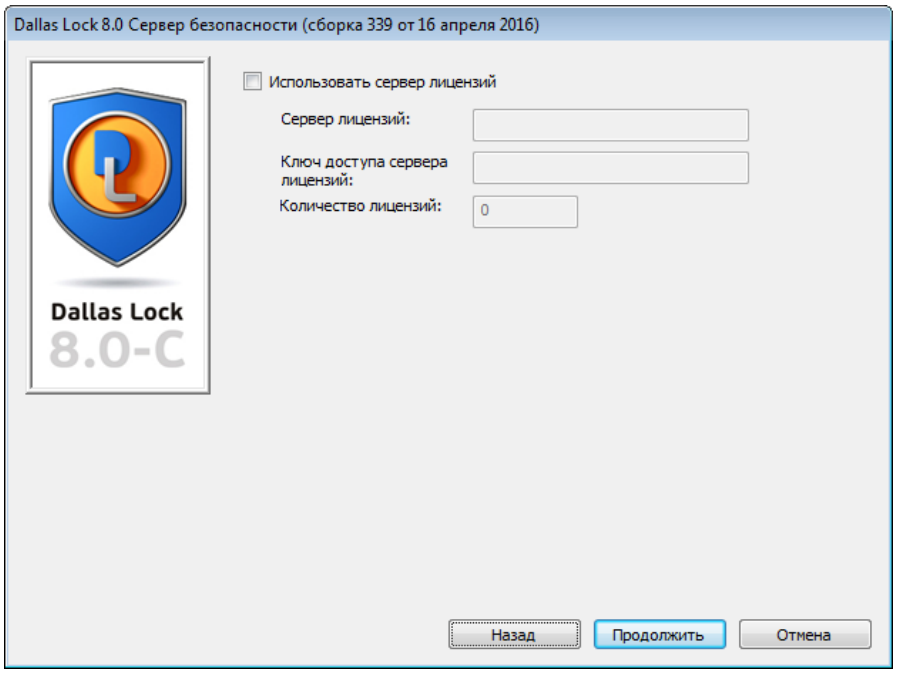

Рис. 37 – Окно установки СБ

3.2 Подключение БД с Консоли сервера безопасности

Для подключения БД с помощью Консоли сервера безопасности необходимо:

1. В основном меню КСБ, выбрав пункт «Основное», нажать кнопку «Параметры хранения журналов» (Рис. 38).

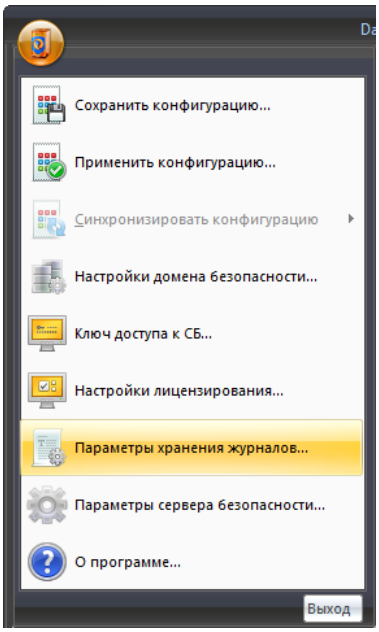

Рис. 38 – Консоль сервера безопасности

2. Далее откроется окно «Параметры хранения журналов». Для сохранения журналов в БД, необходимо поставить флаг у параметра «Использовать базу данных MS SQL Server» и заполнить параметры подключения к БД (Рис. 39).

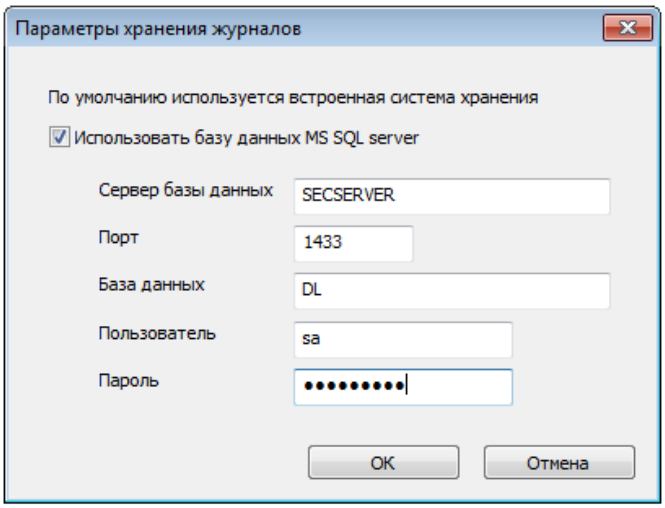

Рис. 39 – Параметры хранения журналов

Для сохранения журналов в файлы, требуется снять флаг с параметра «Использовать базу данных MS SQL Server».

4 ЭКСПЛУАТАЦИЯ

При использовании внешней БД для СБ возможно задать предельный размер БД в Мб. Для этого необходимо:

1. Запустить Microsoft SQL Server Management Studio и авторизоваться под администратором БД.
2. В обозревателе объектов развернуть узел «Базы данных», щелкнуть правой кнопкой мыши на БД, которой необходимо задать предельный размер, и выбрать пункт «Свойства» (Рис. 40).

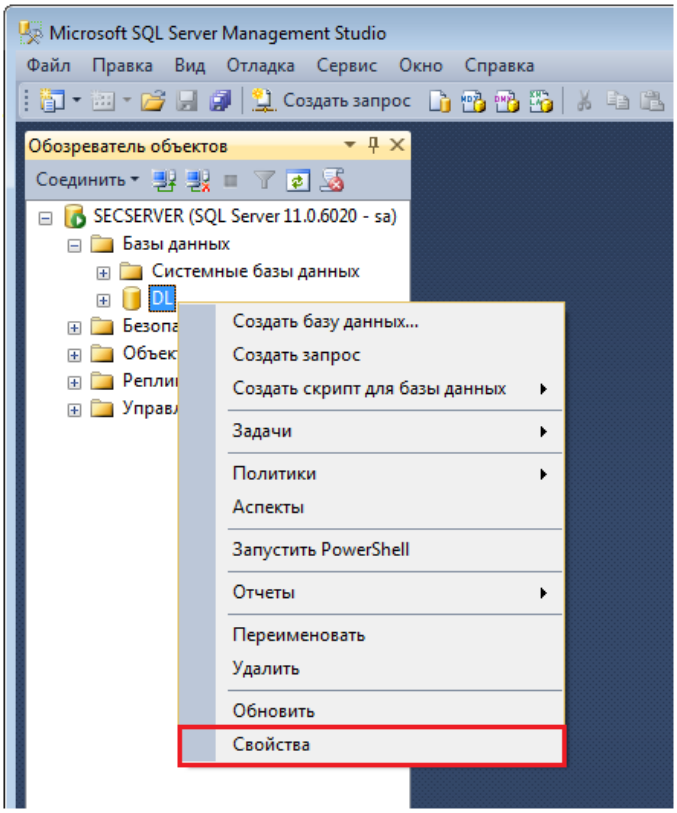

Рис. 40 – Обозреватель объектов

3. В окне «Свойства базы данных – <имя_БД>» перейти на страницу «Файлы» и в столбце «Автоувеличение/максимальный размер» нажать на кнопку с тремя точками файла БД «имя_базы_данных» (Рис. 41).

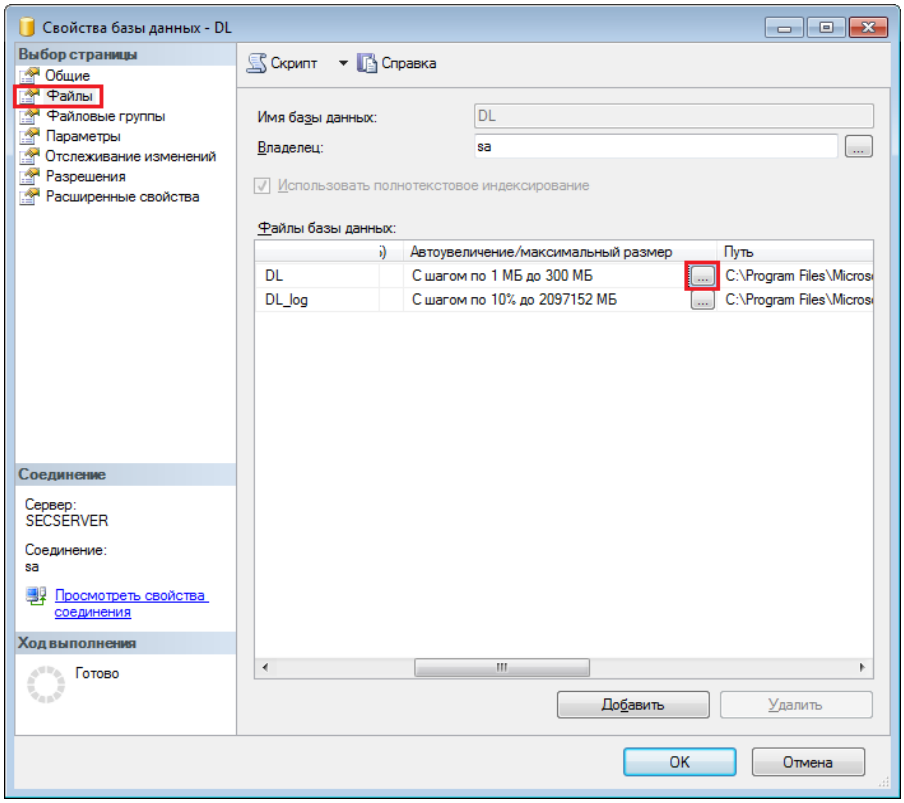

Рис. 41 – Свойства базы данных

4. Откроется окно, в котором возможно задать предельный размер БД (Рис. 42).

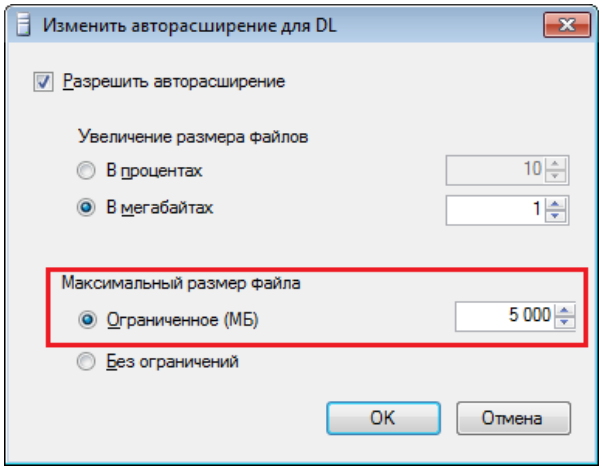

Рис. 42 – Изменение предельного размера БД

В случае заполнении БД на 80% и более выводится предупреждение при подключении Консоли сервера безопасности (Рис. 43).

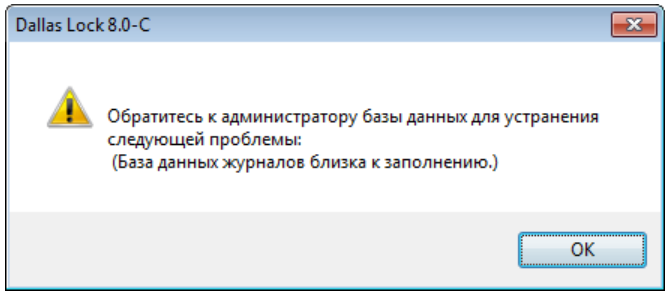

Рис. 43 – База данных журналов близка к заполнению

События, связанные с БД, фиксируются в «Журнал СБ». Для более детального просмотра события, необходимо щелкнуть по нему два раза левой кнопкой мыши (Рис. 44).

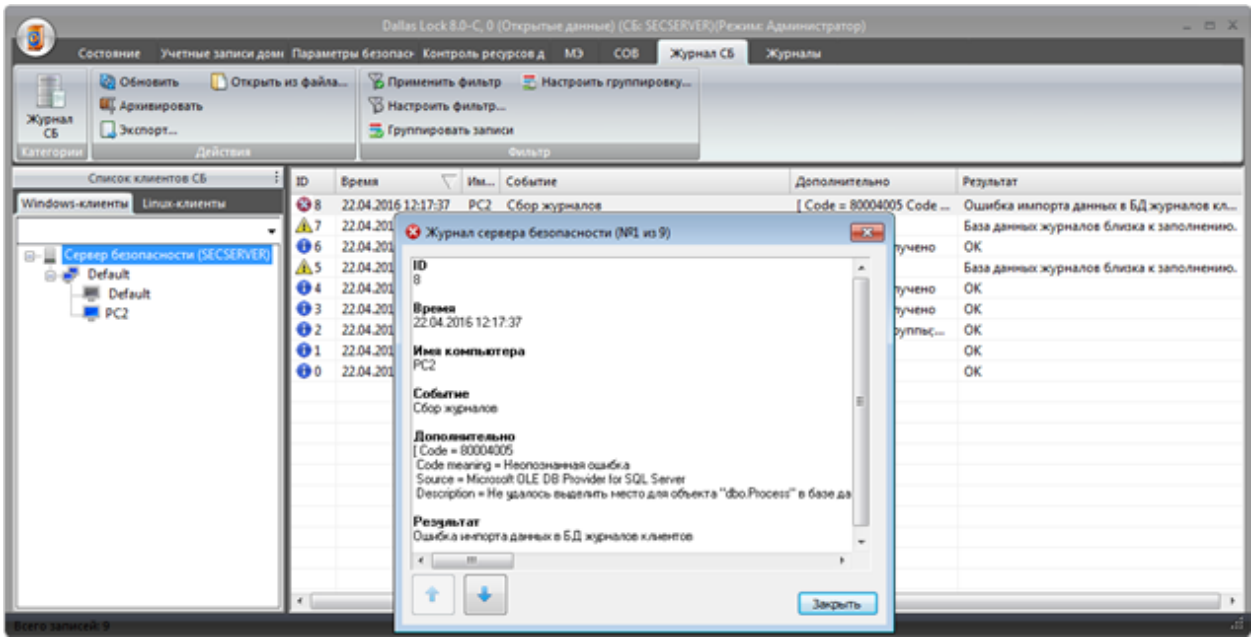

Рис. 44 – Ошибка импорта данных в БД

Во внешней БД сохраняются данные журналов клиентов, с установленной СЗИ НСД Dallas Lock 8.0 и СЗИ НСД Dallas Lock Linux, а также журнала СБ.

Для того, чтобы собрать журналы со всех Windows или Linux клиентов, необходимо открыть соответствующее дерево объектов, выбрать СБ в дереве объектов, перейти на вкладку «Состояние» → «Основное» и нажать на кнопку «Собрать журналы» (Рис. 45).

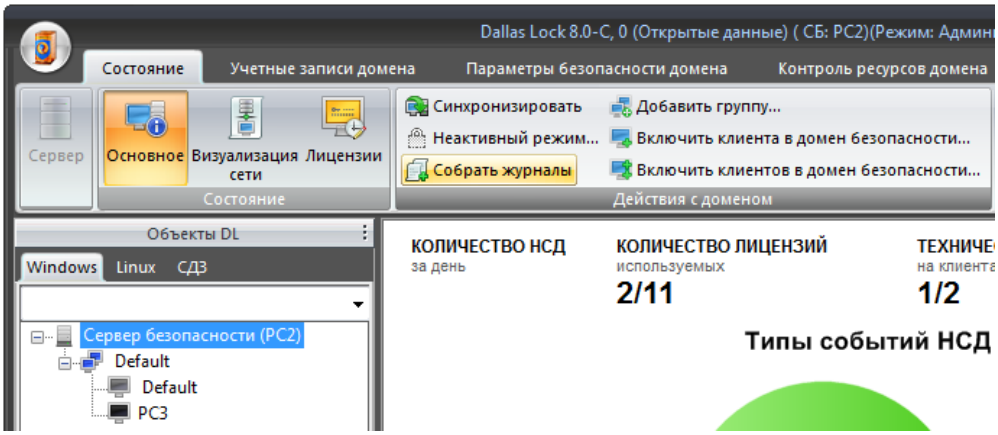

Рис. 45 – Собрать все журналы всех Windows клиентов

Также возможно собрать журнал у определенного Windows или Linux клиента, для этого необходимо открыть соответствующее дерево объектов, выбрать нужного клиента в дереве объектов и перейти на вкладку «Журналы». Далее на панели «Действия с журналами» нажать на кнопку «Собрать журналы» (Рис. 46).

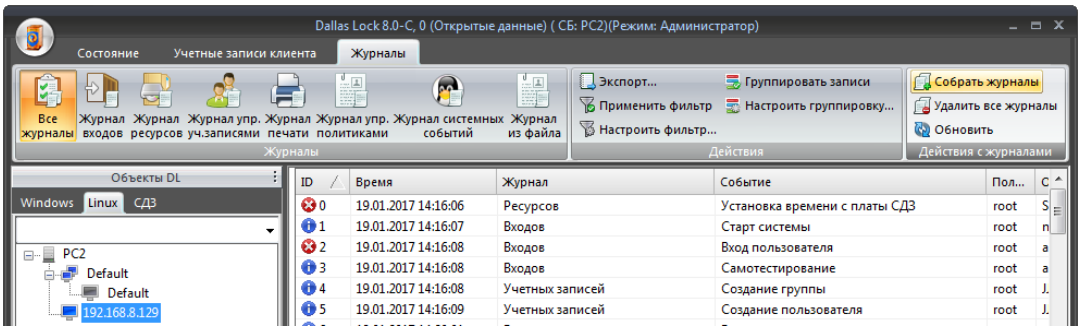

Рис. 46 – Собрать журналы клиента Linux

В случае возникновении сбоя при сохранении данных аудита, собранные файлы журналов хранятся на СБ до тех пор, пока не будут загружены в БД. Зачистка файла журнала на клиенте выполняется только при успешной передаче файла СБ.

Для просмотра собранных журналов со всех Windows или Linux клиентов, необходимо открыть соответствующее дерево объектов, выбрать СБ в дереве объектов, перейти на вкладку «Журналы» (Рис. 47). Формирование этих журналов и записей в них происходит на момент команды сбора от администратора, по настроенному расписанию, а также при периодическом сборе журналов в параметрах данного СБ.

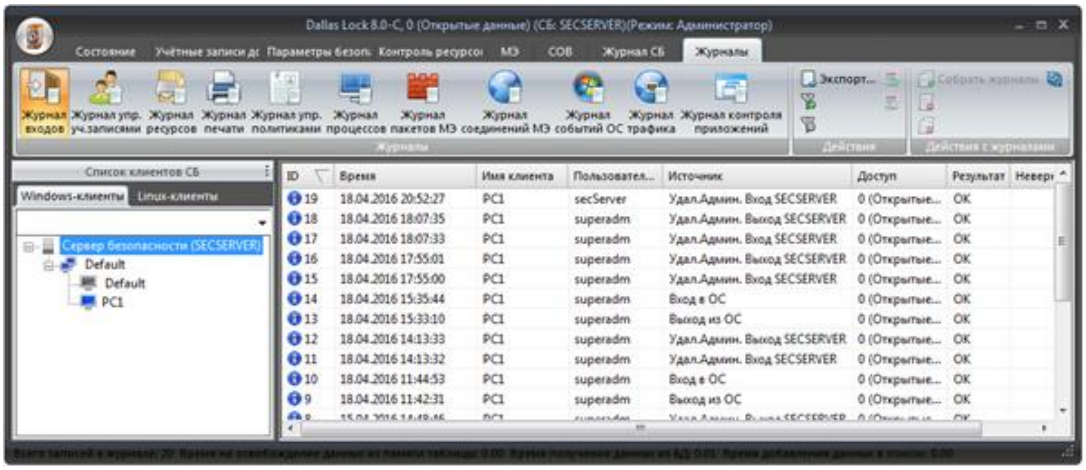

Рис. 47 – Журналы всех Windows клиентов

Взаимодействие с журналами подробно описано в разделе 6.3, документа «Руководство по эксплуатации» RU.48957919.501410-02 92.

При необходимости администратор может подгрузить нужный экземпляр БД или подключиться к уже существующей, при условии, что нет противоречия между форматами таблиц, определенных в СЗИ НСД Dallas Lock и выгружаемых ею, и форматами таблиц существующей БД.

При использовании внешней БД реплицирование выполняется только для параметров безопасности СБ и настроек подключения к БД. Дублирование журналов происходит на уровне репликации самой базы данных и настраивается администратором ИБ за рамками функционала СЗИ.