УТВЕРЖДЕНО
ПФНА.501410.001 ИЗ-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

Dallas Lock

(версия 3.50)

Инструкция по использованию SQL-сервера для Сервера управления доступом

ПФНА.501410.001 ИЗ

Листов 30

Аннотация

Настоящая инструкция распространяются на изделие «Система защиты информации в виртуальных инфраструктурах Dallas Lock».

Данная инструкция освещает вопросы по установке, подключению и эксплуатации системы управления базами данных MS SQL Server совместно с Сервером управления доступом системы защиты информации в виртуальных инфраструктурах Dallas Lock и предназначена для системных администраторов или других сотрудников организации, осуществляющих установку СЗИ ВИ и поддерживающих ее в рабочем состоянии.

Инструкция подразумевает наличие у пользователя навыков работы в операционной системе Windows.

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Общее описание и назначение

Наличие системы управления базами данных позволит:

- сохранять данные аудита Сервера управления доступом (далее — Сервера УД), 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**	**Поддерживаемые операционные системы:** 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**	**Поддерживаемые операционные системы:** 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**	**Поддерживаемые операционные системы:** 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. Для установки Microsoft SQL Server 2008 Express with Advanced Services в ОС Windows Server 2008 необходимо запустить программу-установщик с правами администратора.
2. В разделе «Планирование» нажать пункт «Средство проверки конфигурации» (рис. 1).

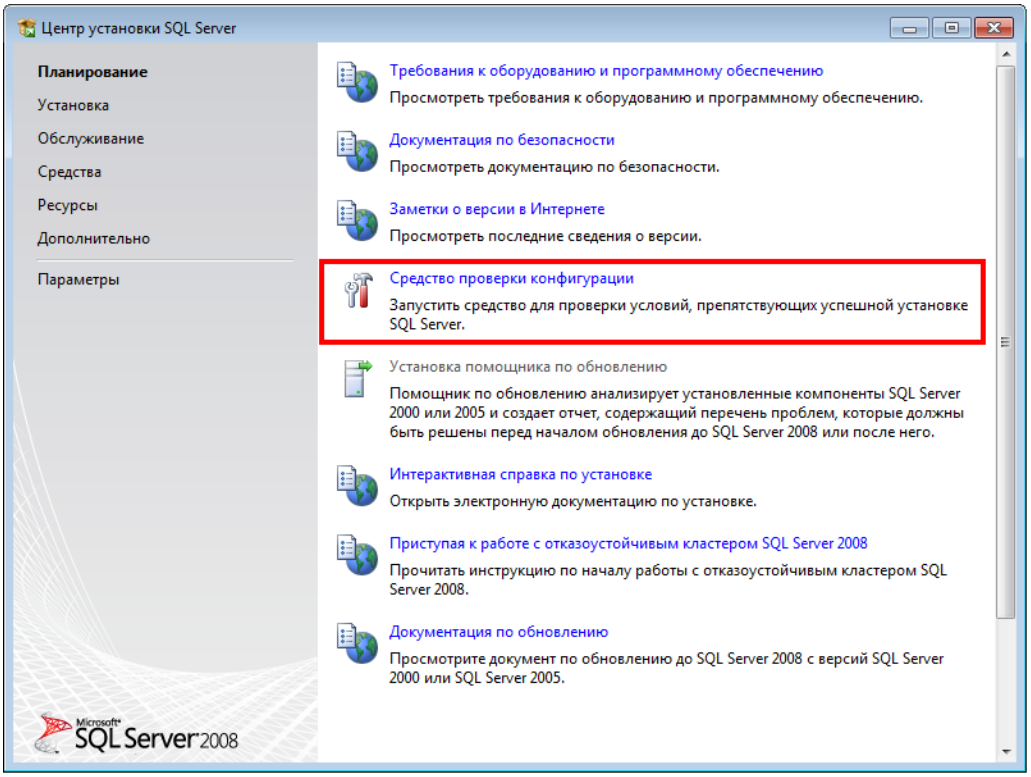

Рис. 1. Раздел «Планирование»

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» (рис. 2).

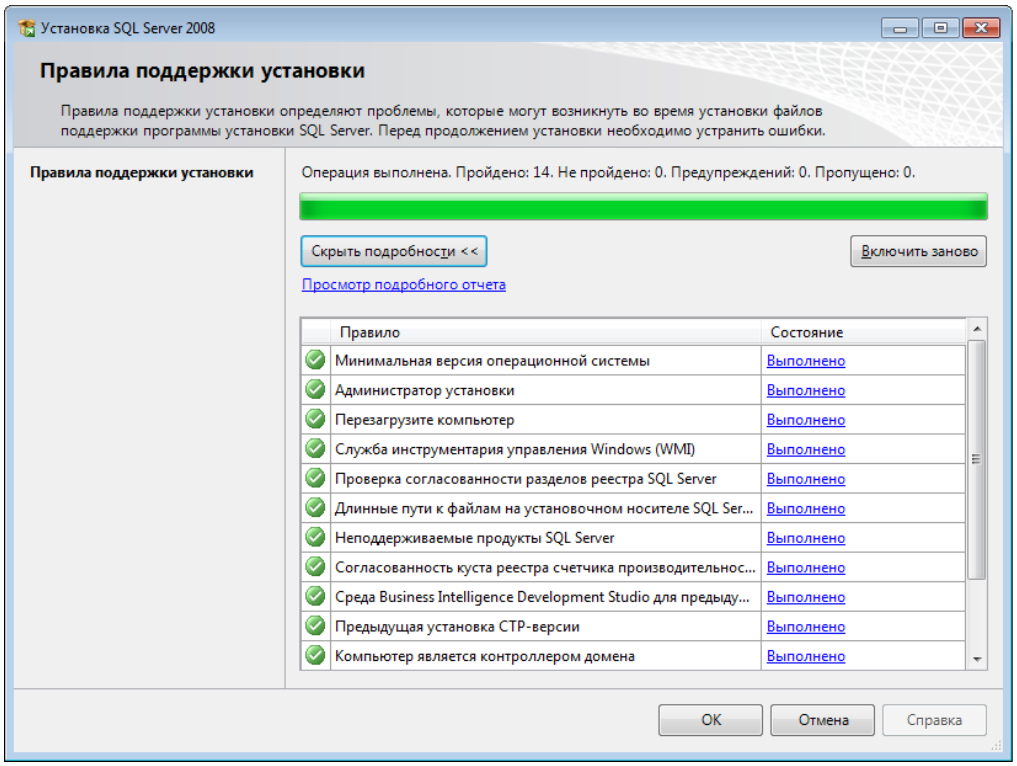

Рис. 2. Проверка правил поддержки установки

4. Для продолжения установки нажать кнопку «ОК» (рис. 2).
5. Открыть раздел «Установка» и нажать на пункт «Новая установка изолированного SQL Server или добавление компонентов к существующему экземпляру» (рис. 3).

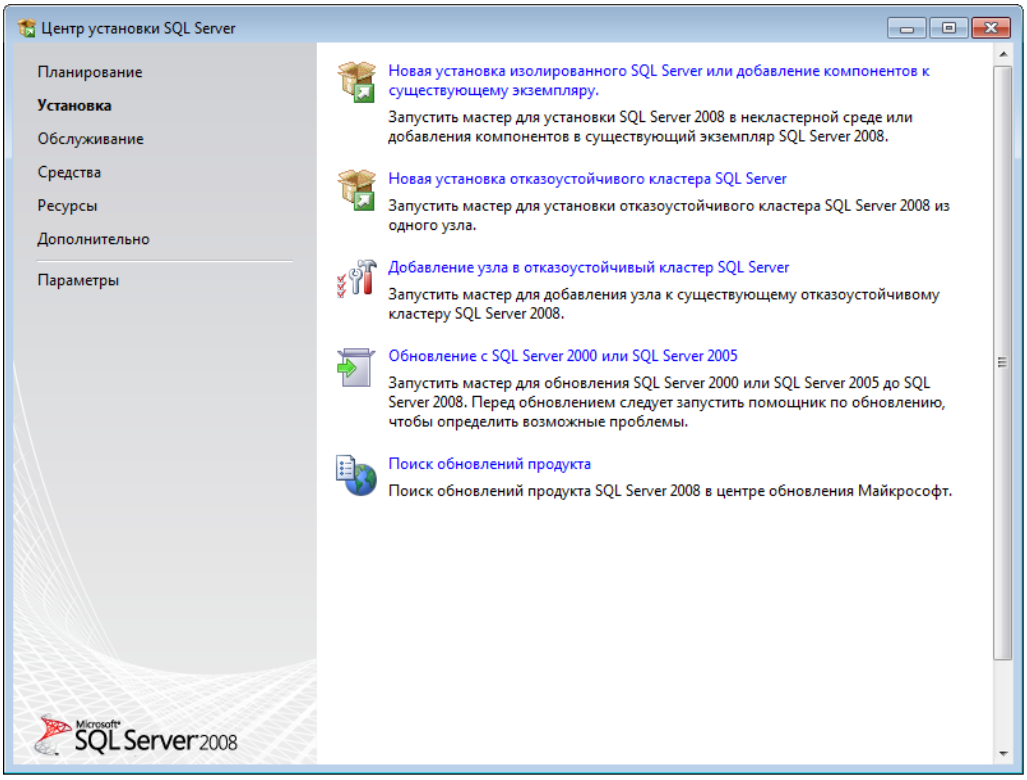

Рис. 3. Раздел «Установка»

6. 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» (рис. 4).

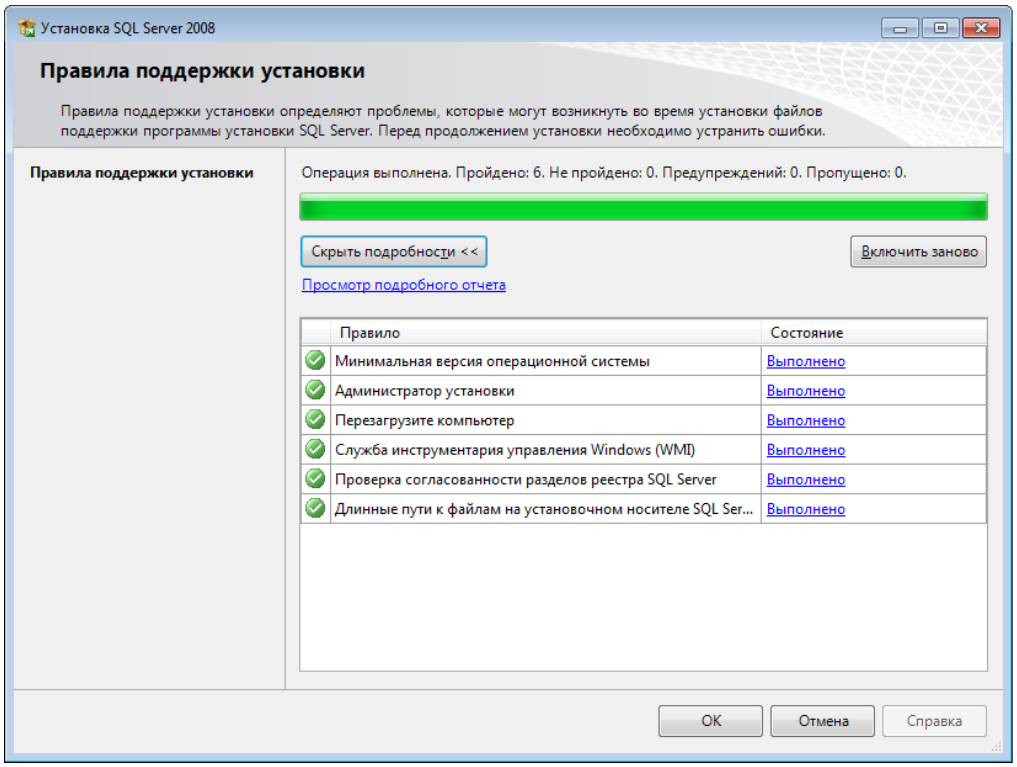

Рис. 4. Проверка правил поддержки установки

7. Для продолжения установки нажать кнопку «ОК».
8. Ввести ключ продукта (для Express версии не требуется) и нажать кнопку «Далее» (рис. 5).

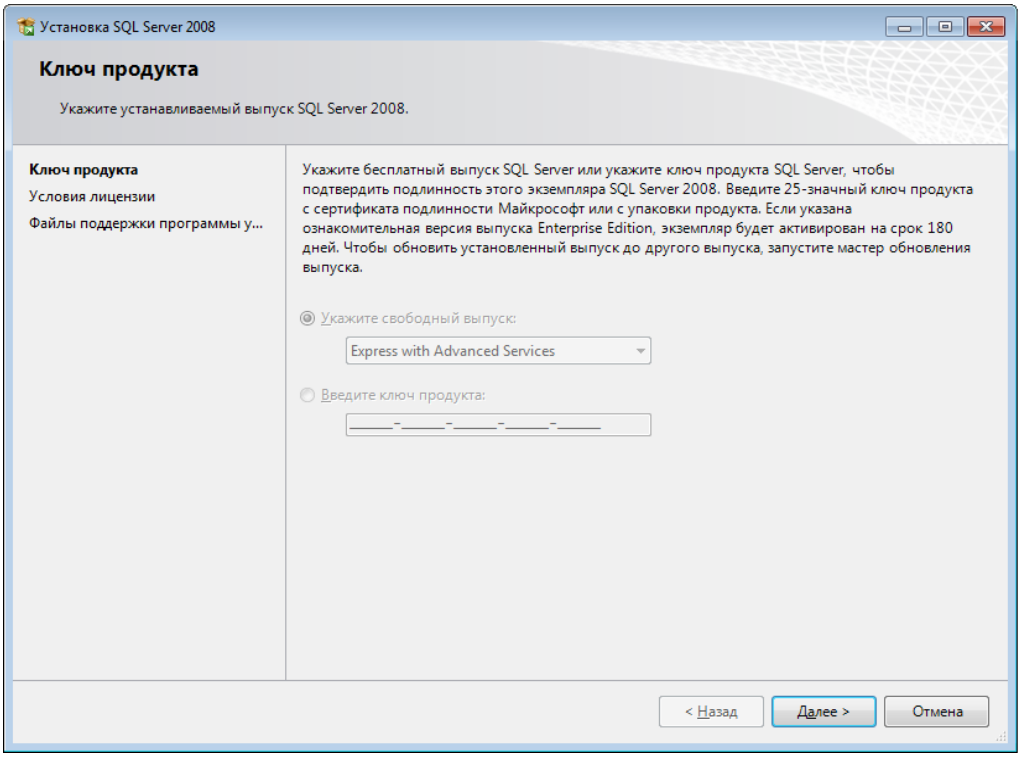

Рис. 5. Выбор устанавливаемого выпуска SQL-сервера

9. Ознакомиться с лицензией, установить флаг «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее» (рис. 6).

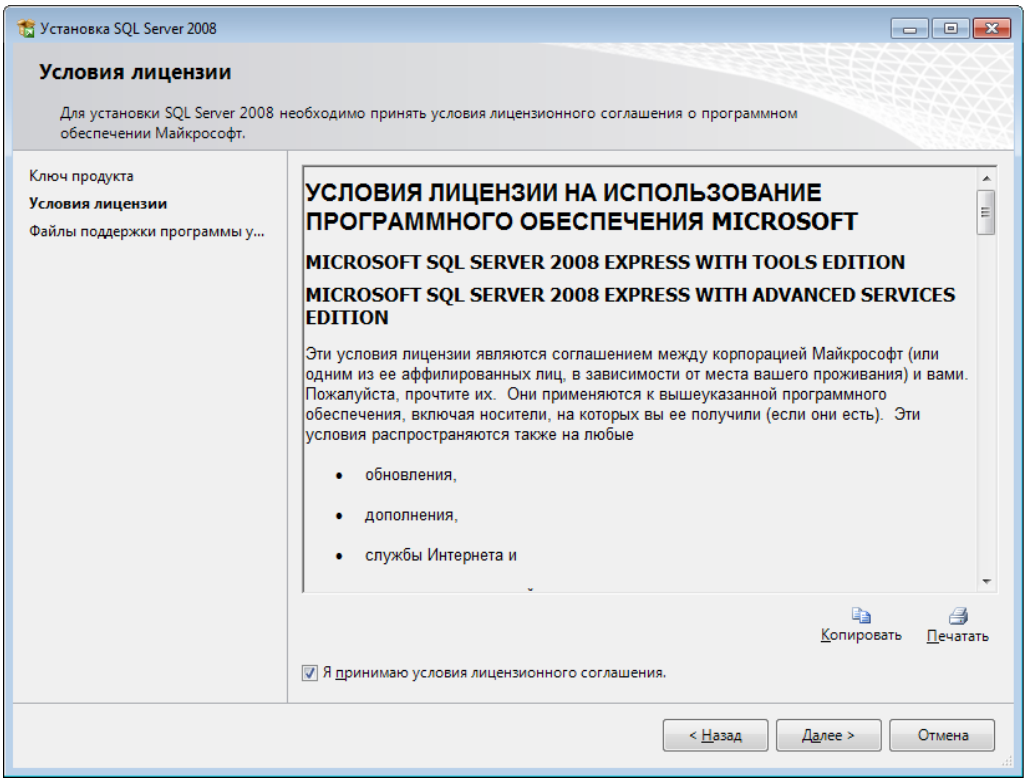

Рис. 6. Условия лицензии

10. Нажать кнопку «Установить» (рис. 7).

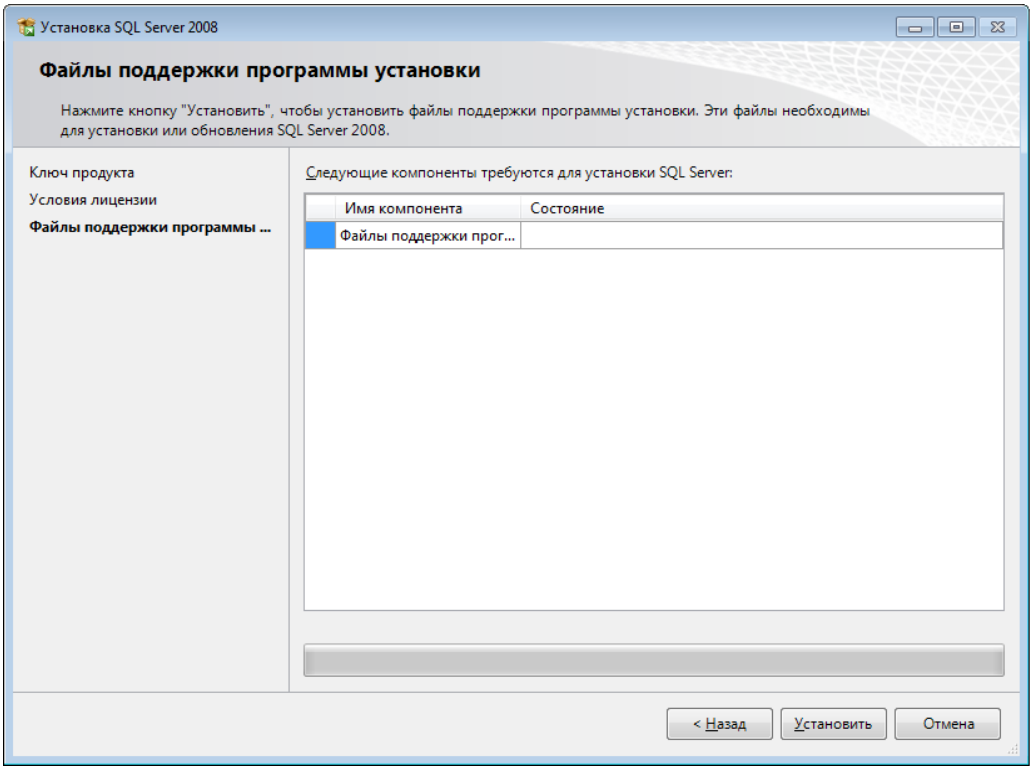

Рис. 7. Файлы поддержки программы установки

11. 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» (рис. 8).

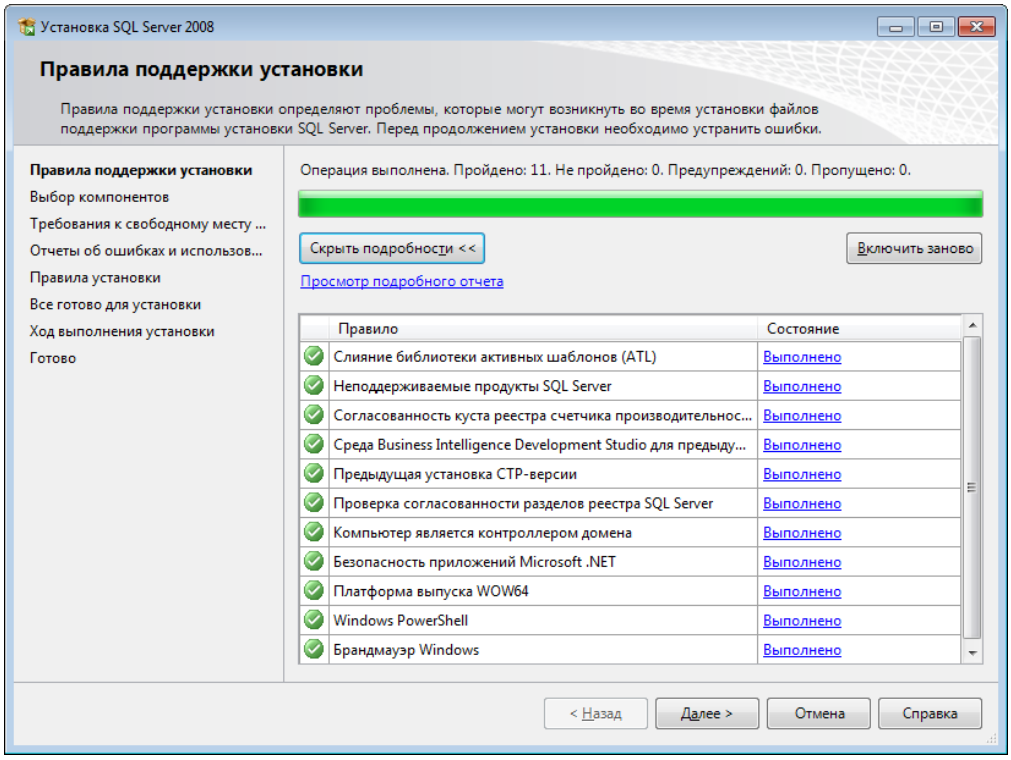

Рис. 8. Проверка правил поддержки установки

12. Для продолжения установки нажать кнопку «Далее».

13. Выбрать компоненты для установки «Службы компонента Database Engine» и «Средства управления — основные» (рис. 9), и нажать кнопку «Далее».

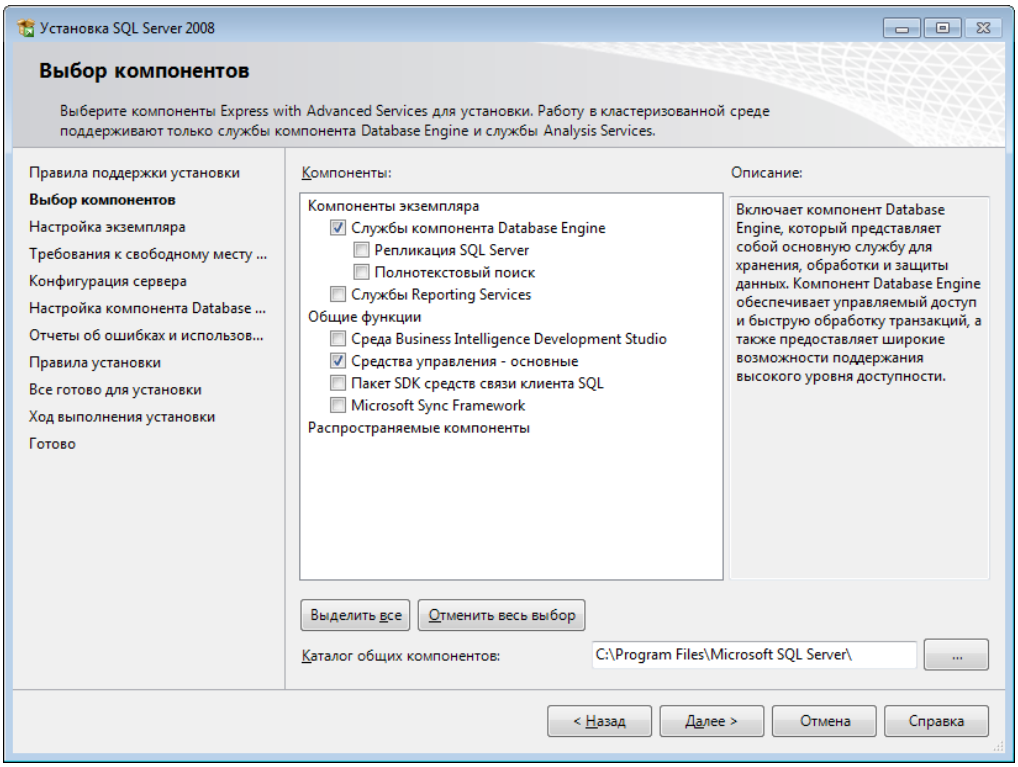

Рис. 9. Выбор компонентов

14. Выбрать значение «Экземпляр по умолчанию» и нажать кнопку «Далее» (рис. 10).

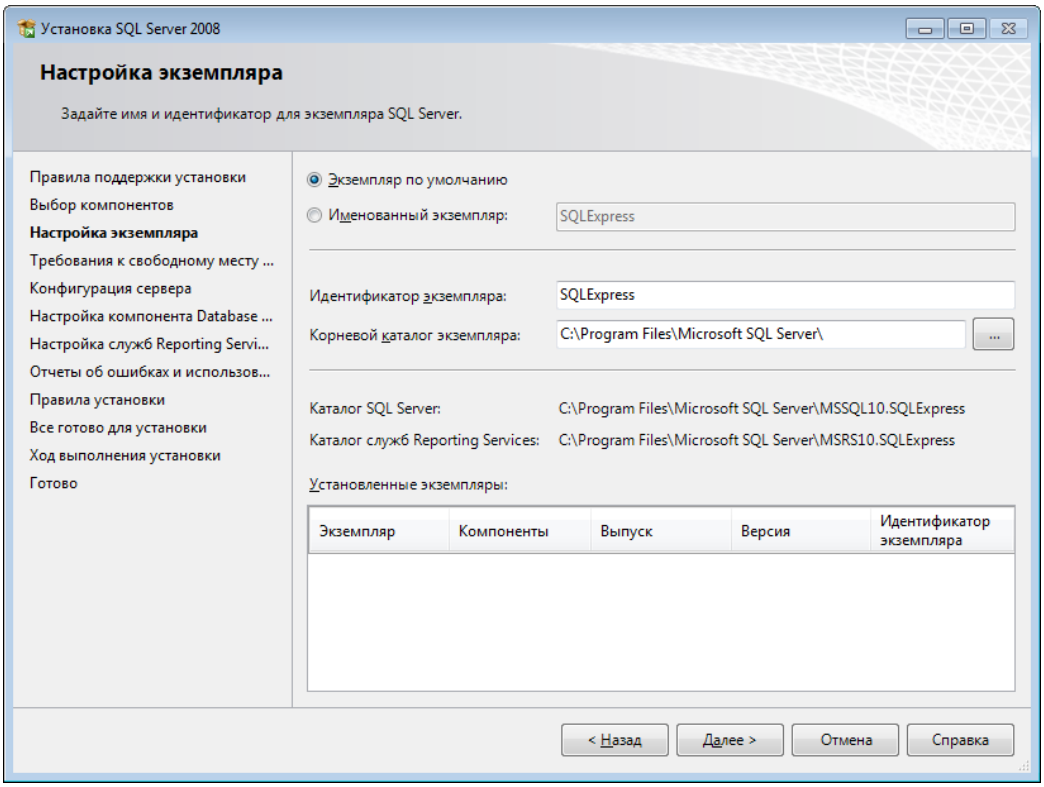

Рис. 10. Настройка экземпляра

15. Убедиться, что доступно необходимое дисковое пространство и нажать кнопку «Далее» (рис. 11).

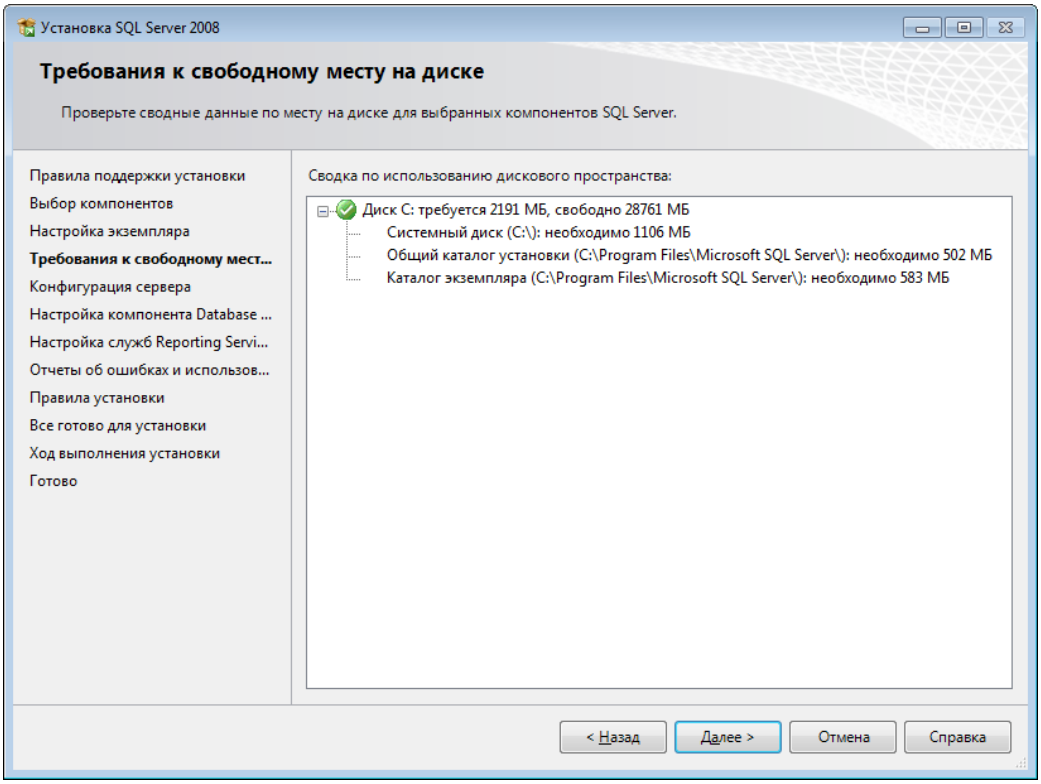

Рис. 11. Требования к свободному месту на диске

16. Настроить службы. Для службы «SQL Server Database Engine» указать имя учетной записи «NT AUTHORITY\SYSTEM» и тип запуска «Авто». Для службы «SQL Server, обозреватель» указать имя учетной записи «NT AUTHORITY\LOCAL SERVICE» и тип запуска «Авто» (рис. 12).

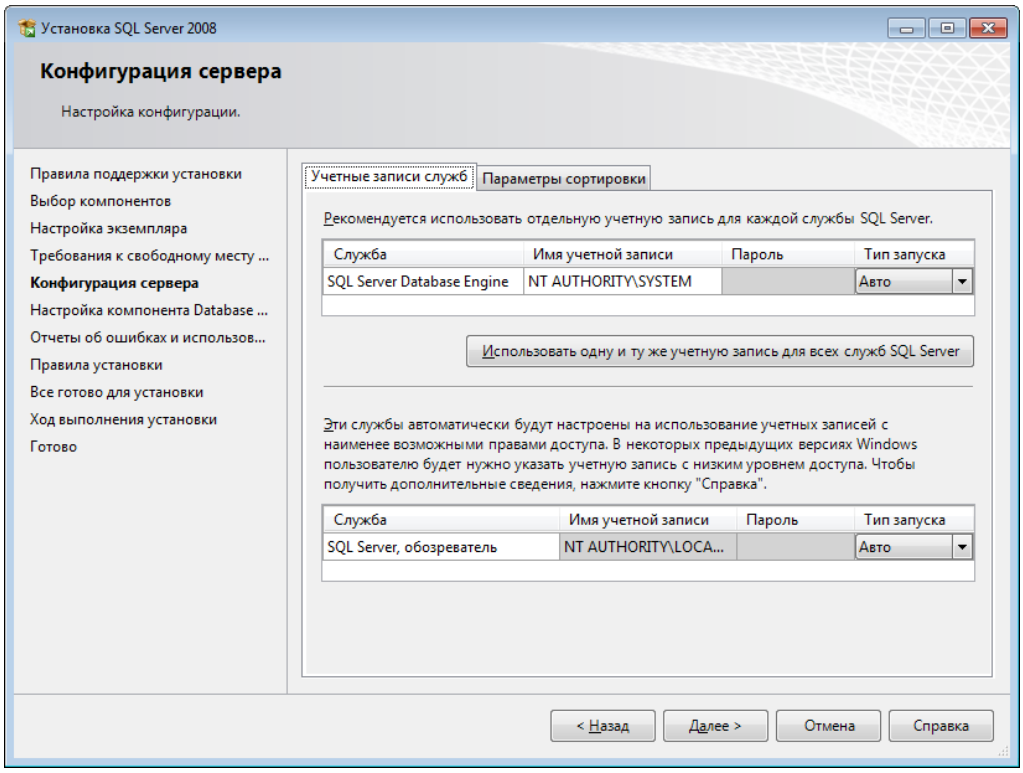

Рис. 12. Учетные записи служб

17. Настроить параметры сортировки. Для компонента Database Engine параметр должен иметь значение «Cyrillic_General_CI_AS». Для службы Analysis Services должен иметь значение «Latin1_General_CI_AS». Нажать кнопку «Далее» (рис. 13).

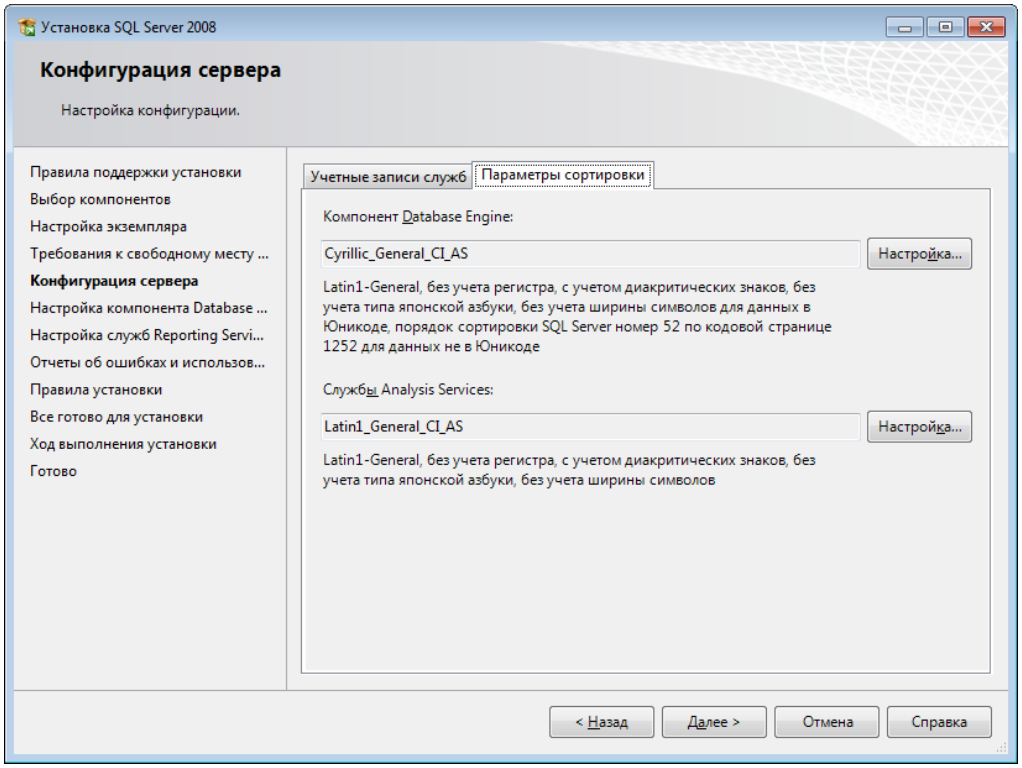

Рис. 13. Параметры сортировки

18. Чтобы изменить параметр, необходимо нажать кнопку «Настройка» рядом с параметром и установить значения, как показано на рисунке (рис. 14).

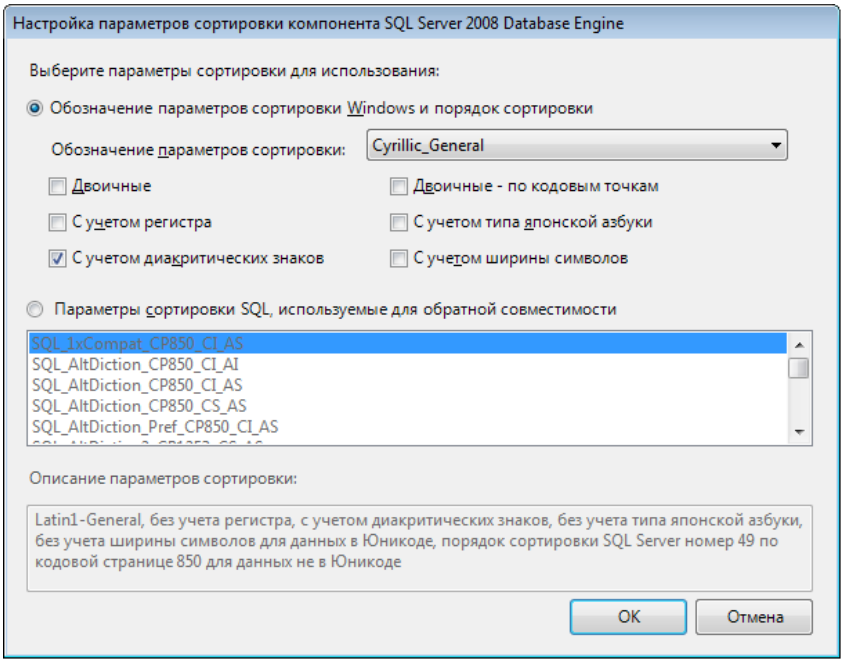

Рис. 14. Настройка параметров сортировки компонента

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

Примечание. По умолчанию на SQL Server действует механизм политики паролей Windows, поэтому указанный пароль должен отвечать требованиям безопасности, именно:

- длина пароля составляет не менее 8 символов;
- пароль содержит символы, соответствующие трем из следующих категорий:

1. прописные латинские буквы (A-Z);
2. строчные латинские буквы (a-z);
3. цифры (0-9);
4. спецсимволы (например: «!», «#», «%»).

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

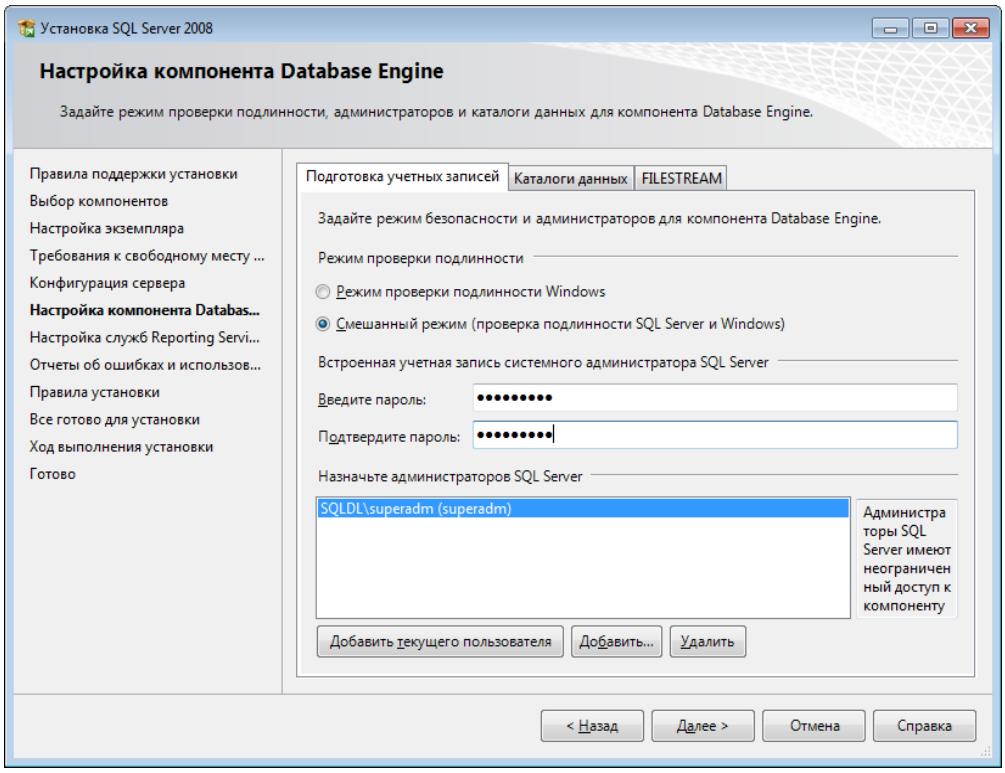

Рис. 15. Подготовка учетных записей

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

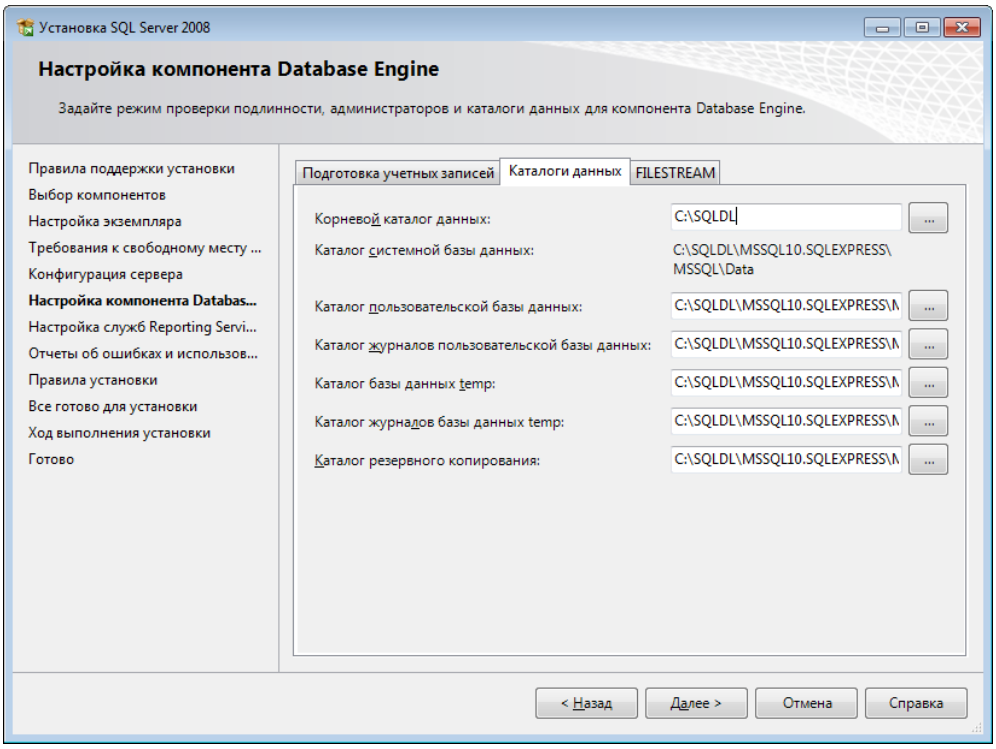

Рис. 16. Выбор корневого каталога данных

22. Для продолжения установки нажать кнопку «Далее».

23. Выбрать значение «Установить конфигурацию по умолчанию для работы в собственном режиме» и нажать кнопку «Далее» (рис. 17).

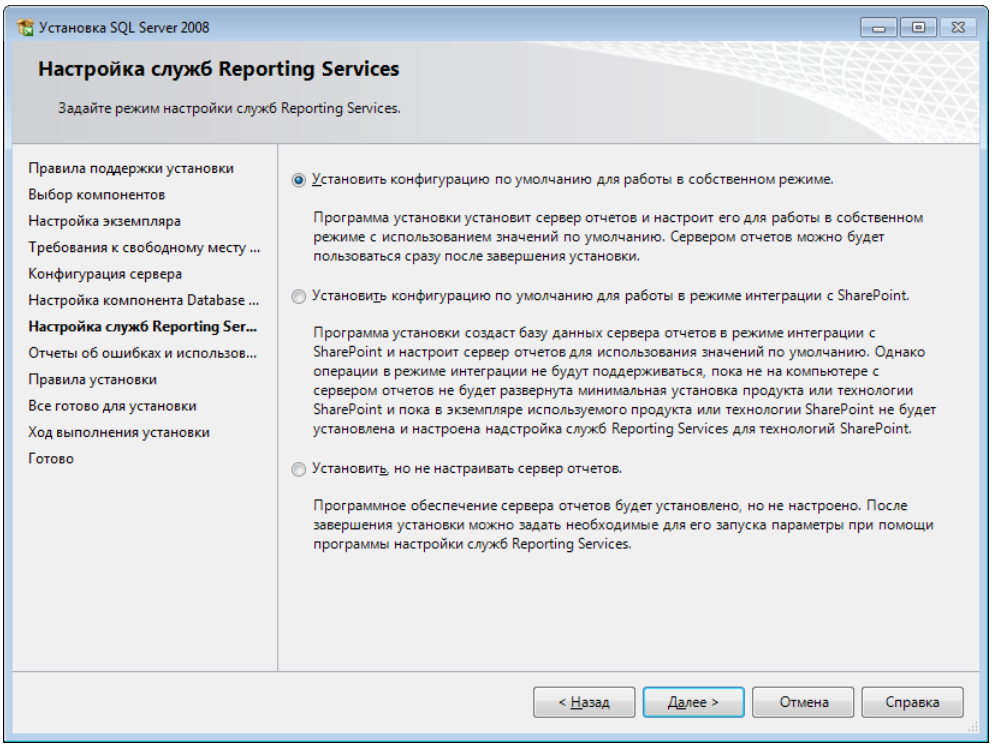

Рис. 17. Настройка служб Reporting Services

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

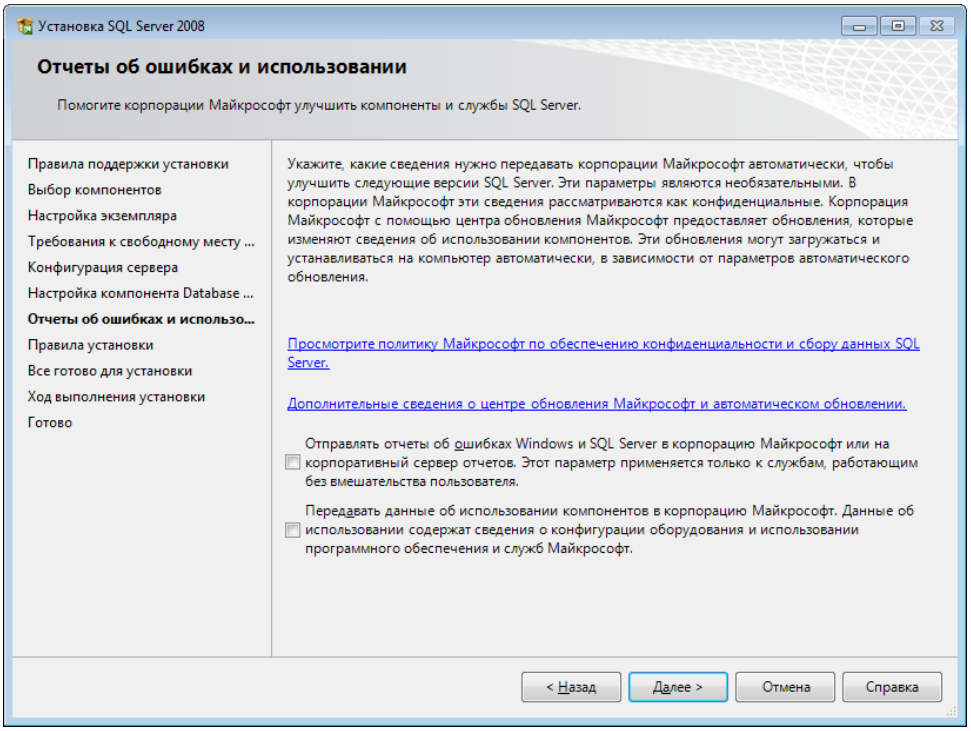

Рис. 18. Отчеты об ошибках и использовании

25. 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» (рис. 19).

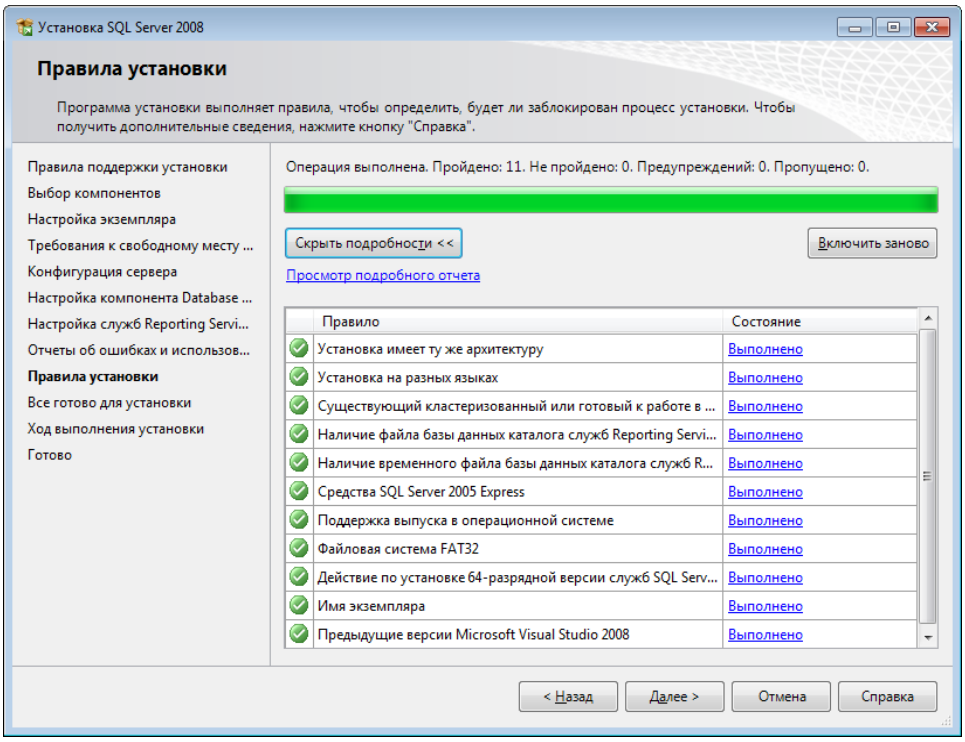

Рис. 19. Проверка правил установки

26. Для продолжения установки нажать кнопку «Далее».

27. Нажать кнопку «Установить» (рис. 20).

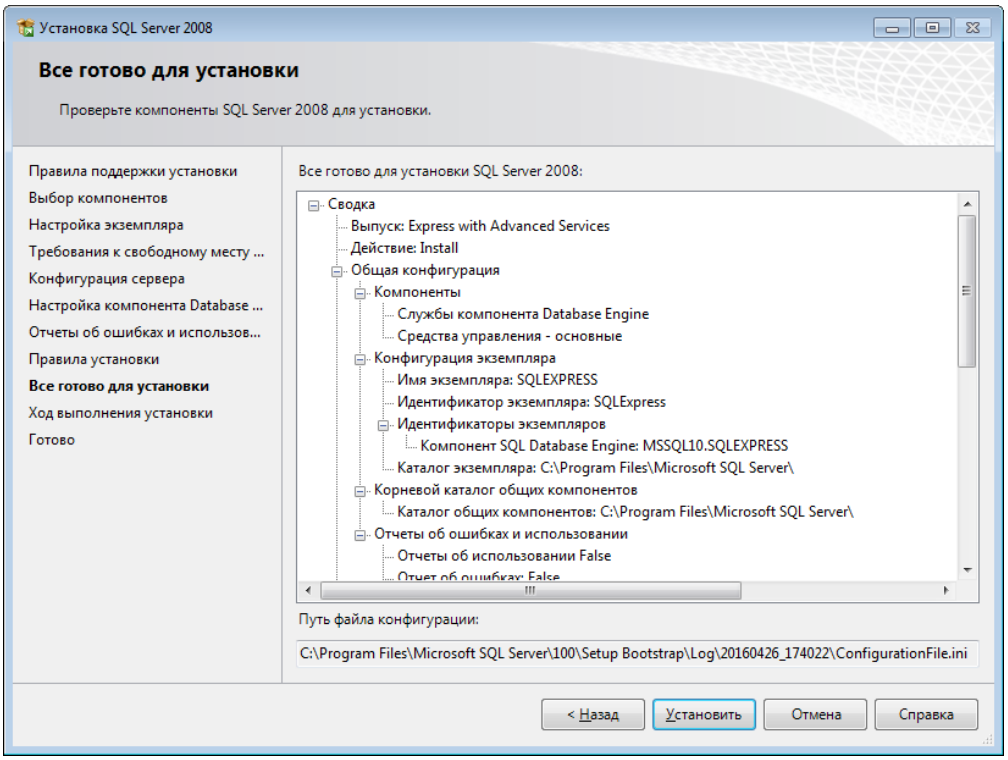

Рис. 20. Сводка компонентов SQL Server 2008

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

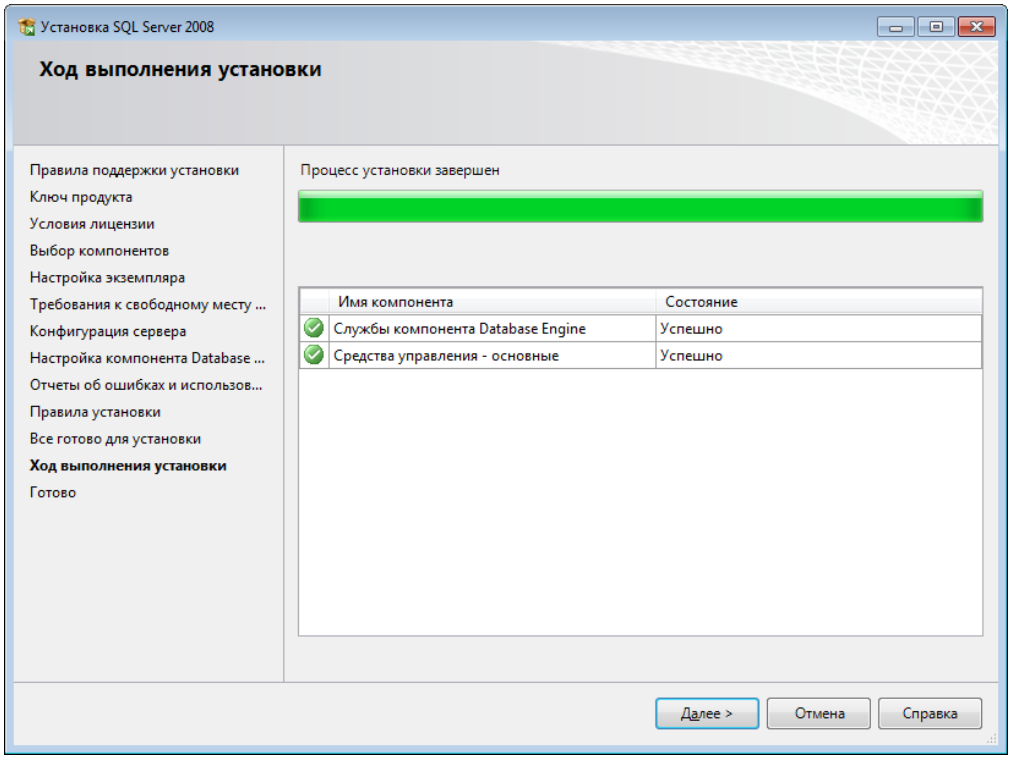

Рис. 21. Ход выполнения установки

29. Нажать кнопку «Закрыть» (рис. 22).

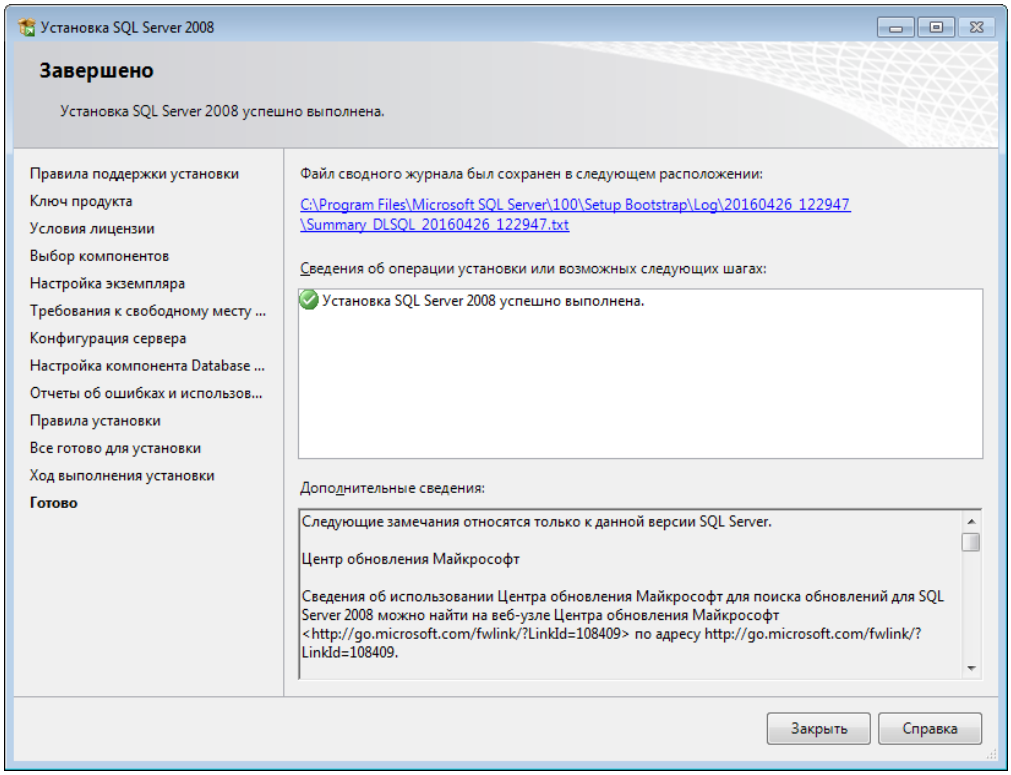

Рис. 22. Завершение установки

30. 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).

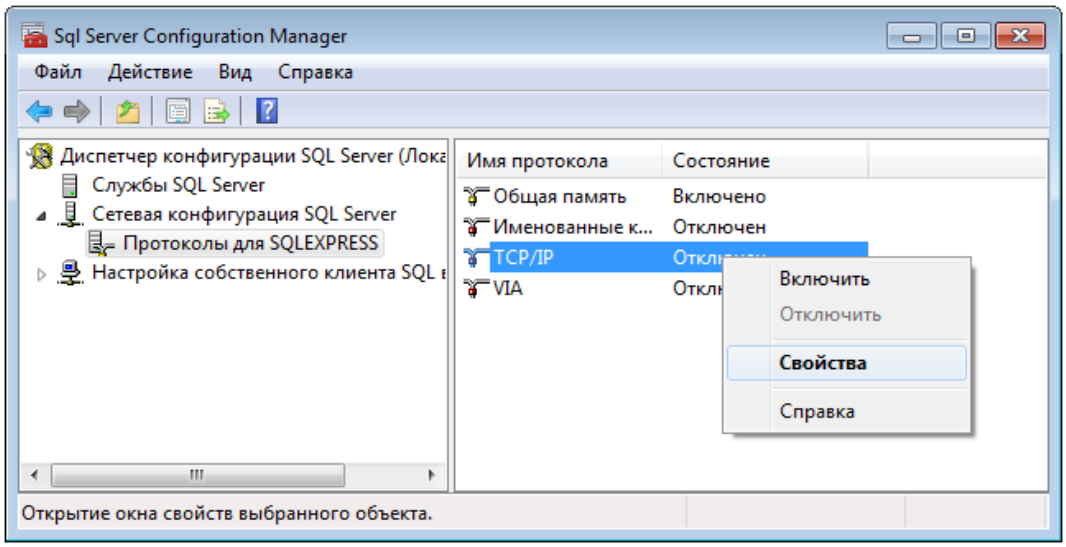

Рис. 23. Вызов свойств протокола TCP/IP

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

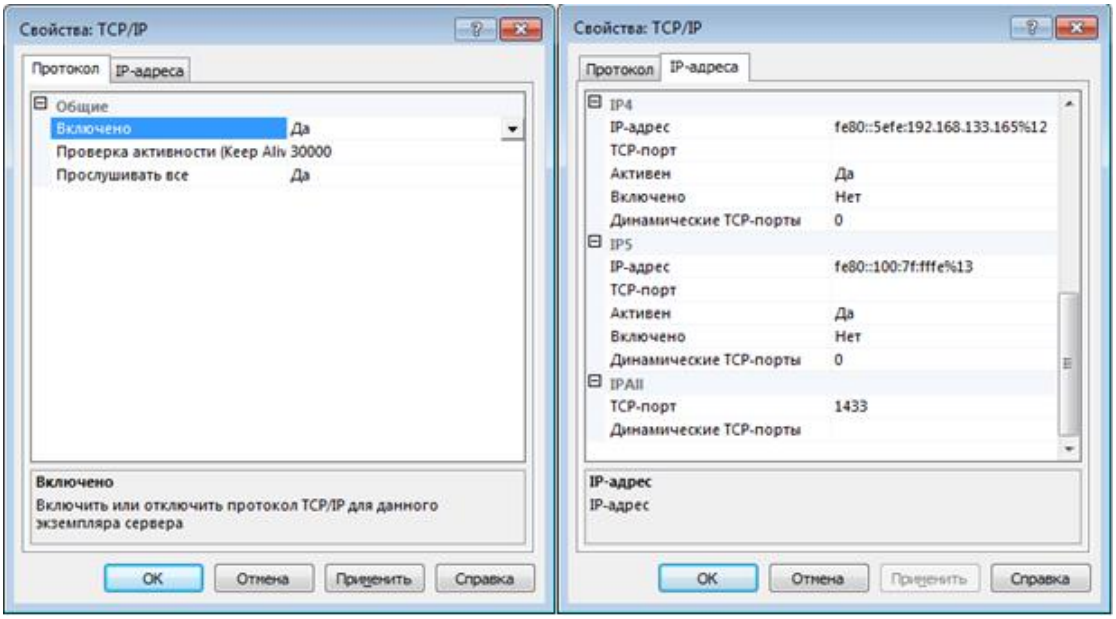

Рис. 24. Настройка свойств протокола TCP/IP

32. 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).

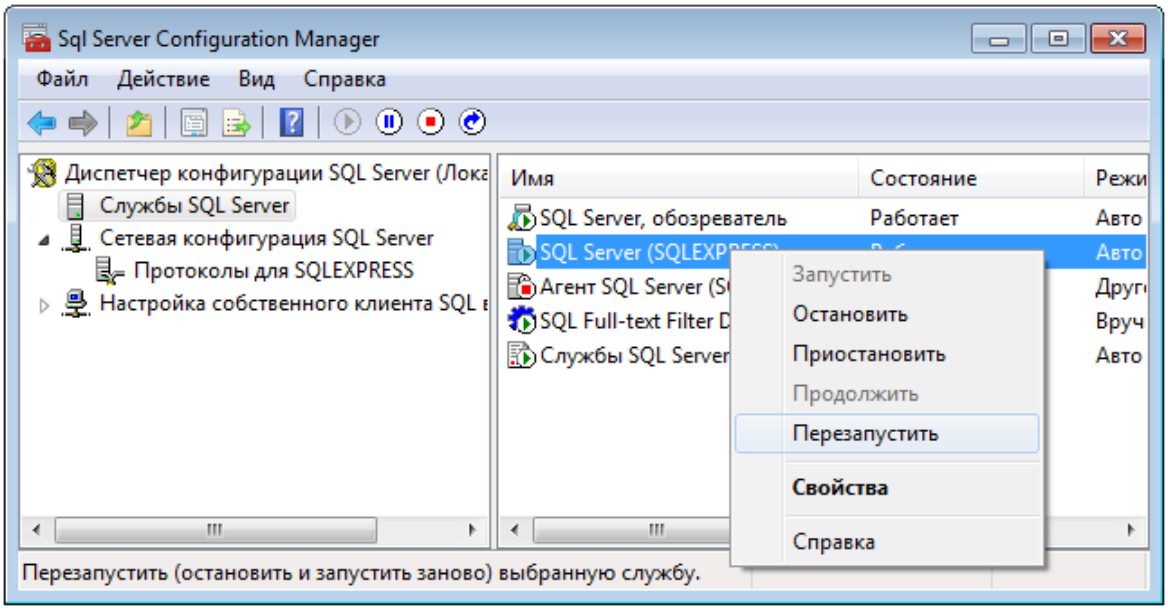

Рис. 25. Перезапуск службы SQL Server

3 ПОДКЛЮЧЕНИЕ БД К СБ

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

Для корректного взаимодействие сервера безопасности и СУБД MS SQL необходимо следующее:

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. При установке: При установке: «Конфигурация сервера» → «Учетные записи служб» → «Обозреватель SQL Server» → выбрать в поле «Тип запуска» значение «Авто» (рис. 26).

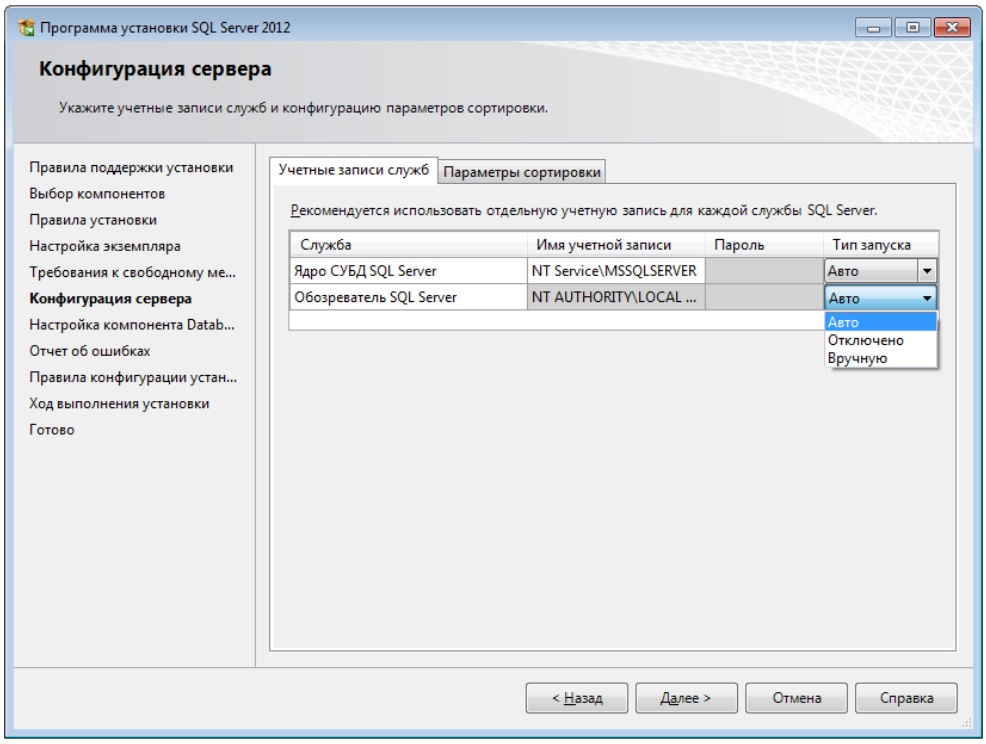

Рис. 26. Включение обозревателя SQL Server в процессе установки MS SQL

После установки: «Пуск» → «Microsoft SQL Sever 2008» → «Средства настройки» → «Диспетчер конфигураций SQL Server» → раздел «Службы SQL Server» → «SQL Server, обозреватель» → после нажатия правой кнопкой мыши в контекстном меню выбрать пункт «Свойства» → вкладка «Служба» → параметру «Режим запуска» присвоить значение «Авто» (рис. 27).

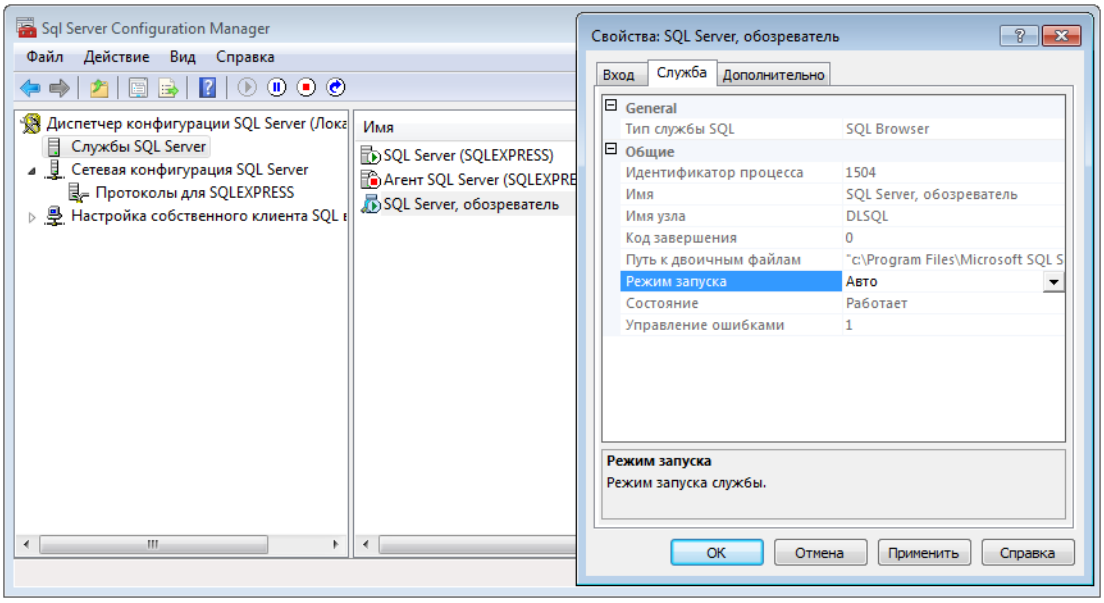

Рис. 27. Включение обозревателя в диспетчере конфигураций SQL Server

2. Включить поддержку 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).

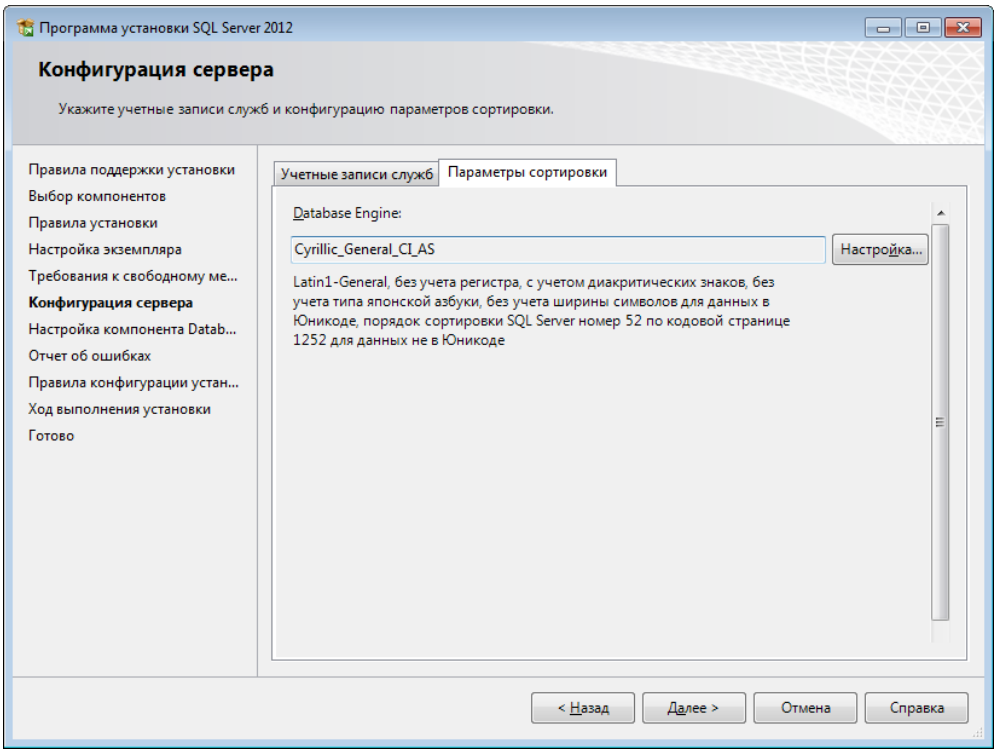

Рис. 28. Параметры сортировки

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

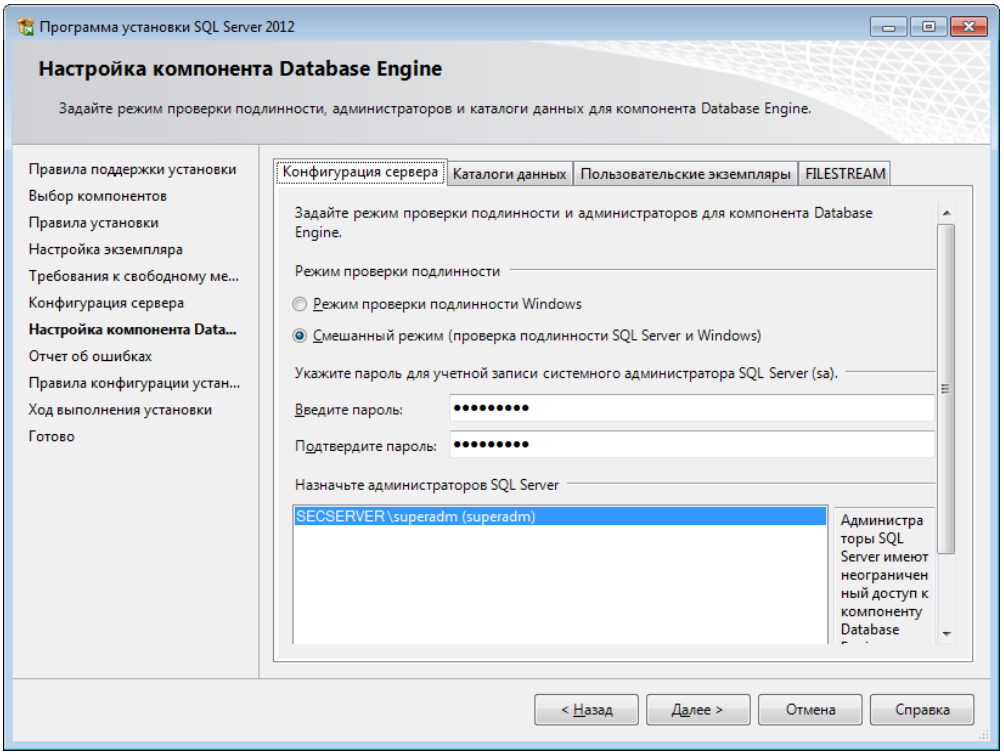

Рис. 29. Режим проверки подлинности

4. Включить протокол TCP/IP для необходимого экземпляра сервера. При использовании SQL Server Express протокол отключен по умолчанию. 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).

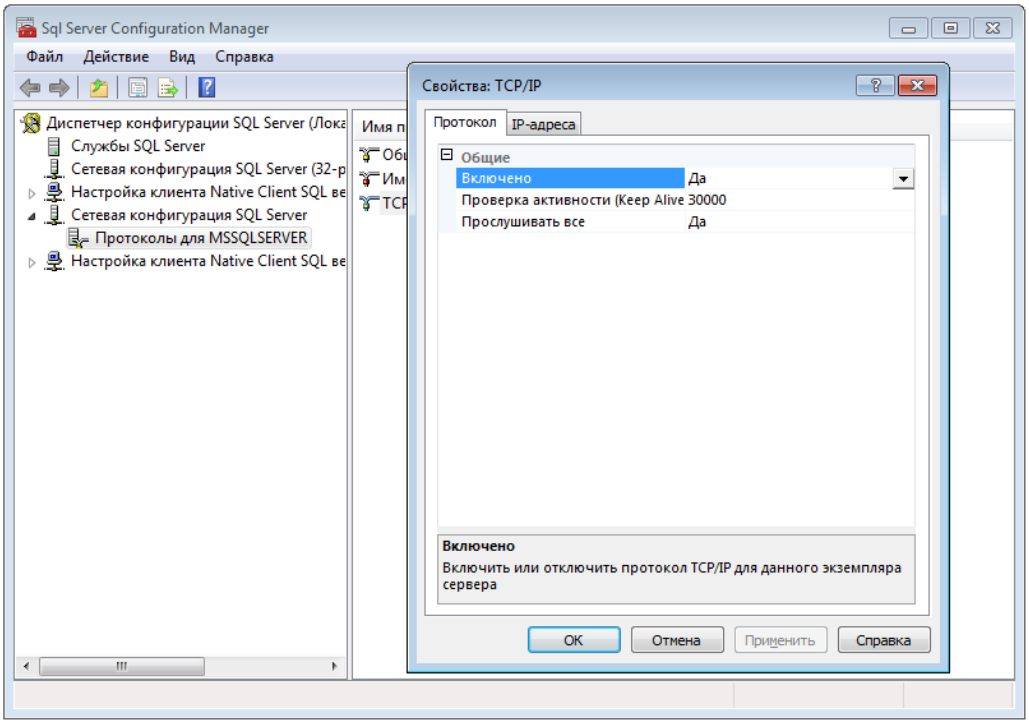

Рис. 30. Включение протокола TCP/IP

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).

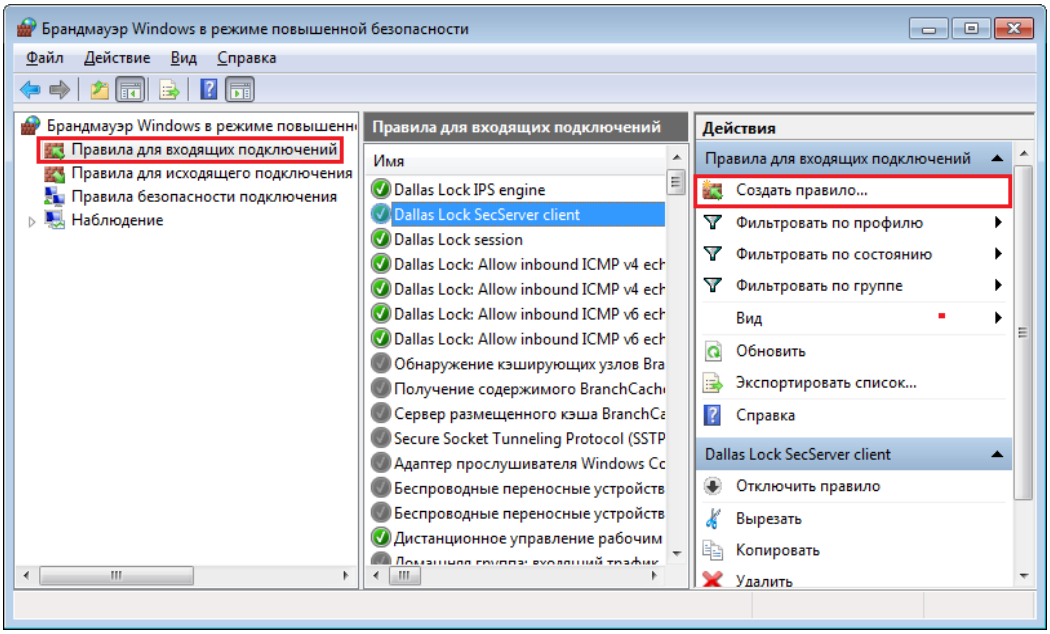

Рис. 31. Создание правила для выходящего соединения

Далее необходимо, выбрать тип правила «Для порта» и нажать кнопку «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.

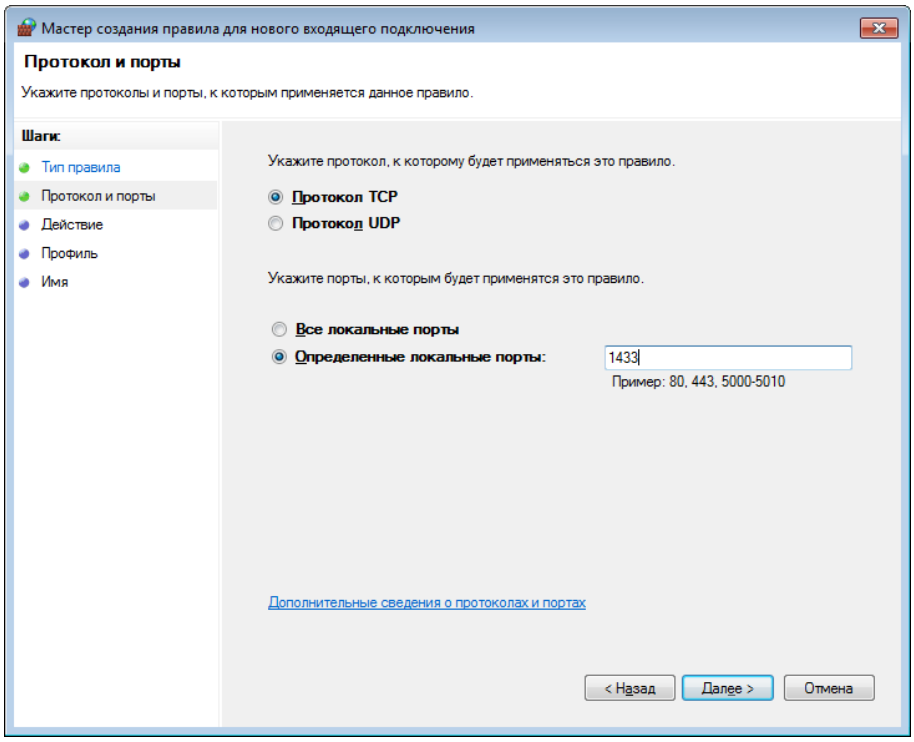

Рис. 32. Создание правила для входящего подключения по протоколу TCP

6. На Сервере УД в Консоли перейти на уровень агента Windows. В категории «Состояние» нажать на кнопку «Сессии-исключения» (рис. 33). В случае, если данная кнопка неактивна, необходимо подключиться к клиенту, нажав на панели «Действия» кнопку «Подключиться».

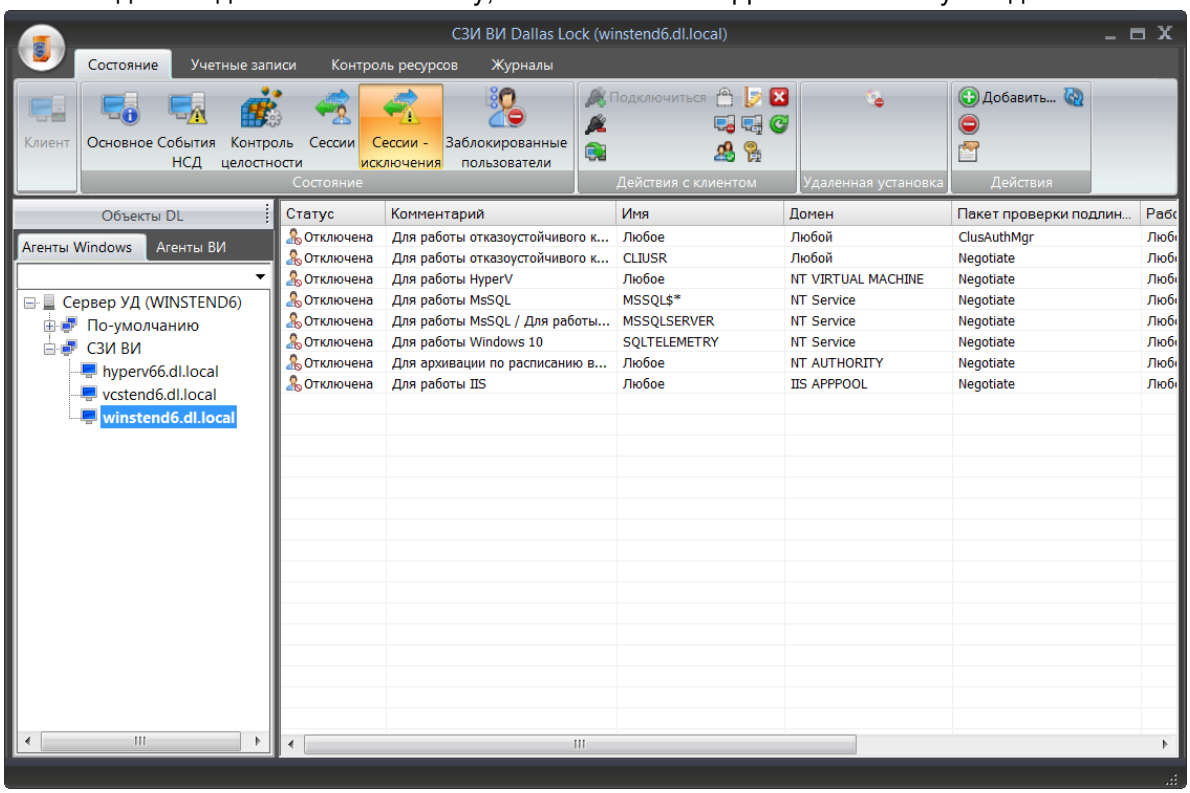

Рис. 33. Необходимые сессии-исключения для работы с SQL-сервером

7. Затем необходимо активировать 2 сессии-исключения «Для работы MsSQL», переводом соответствующих параметров в статус «Включена». Для этого необходимо двойным щелчком на сессии-исключении вызвать окно с настройкой параметров и установить флаг в поле «Исключение активно», после чего нажать кнопку «ОК». (рис. 34).

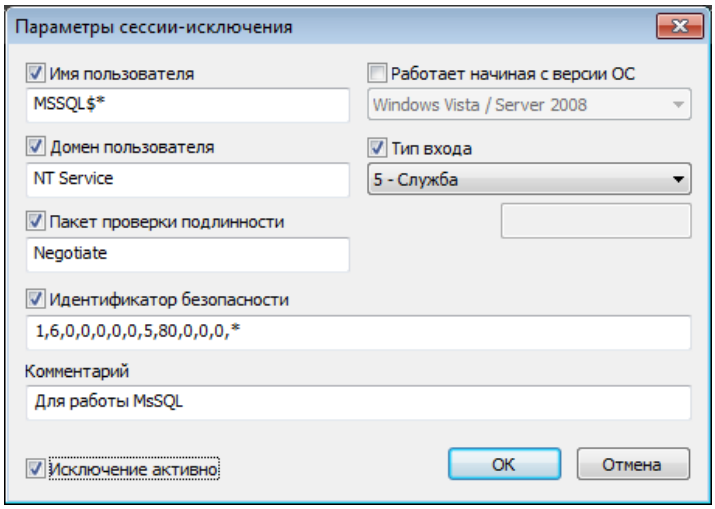

Рис. 34. Настройка сессий-исключений

3.1 Подключение БД в процессе установки Центра управления СЗИ ВИ Dallas Lock

В процессе установки Центра управления СЗИ ВИ Dallas Lock, возможно подключить существующую БД, либо создать новую.

3.1.1 Подключение к существующей БД в процессе установки

Для этого необходимо:

1. В окне «Параметры хранения журналов» поставить флаг «Использовать базу данных MS SQL Server».
2. Заполнить поля подключения к БД (рис. 35):
   - имя или IP-адрес ПК, на котором расположен сервер базы данных;
   - порт подключения;
   - имя базы данных;
   - логин и пароль пользователя базы данных.

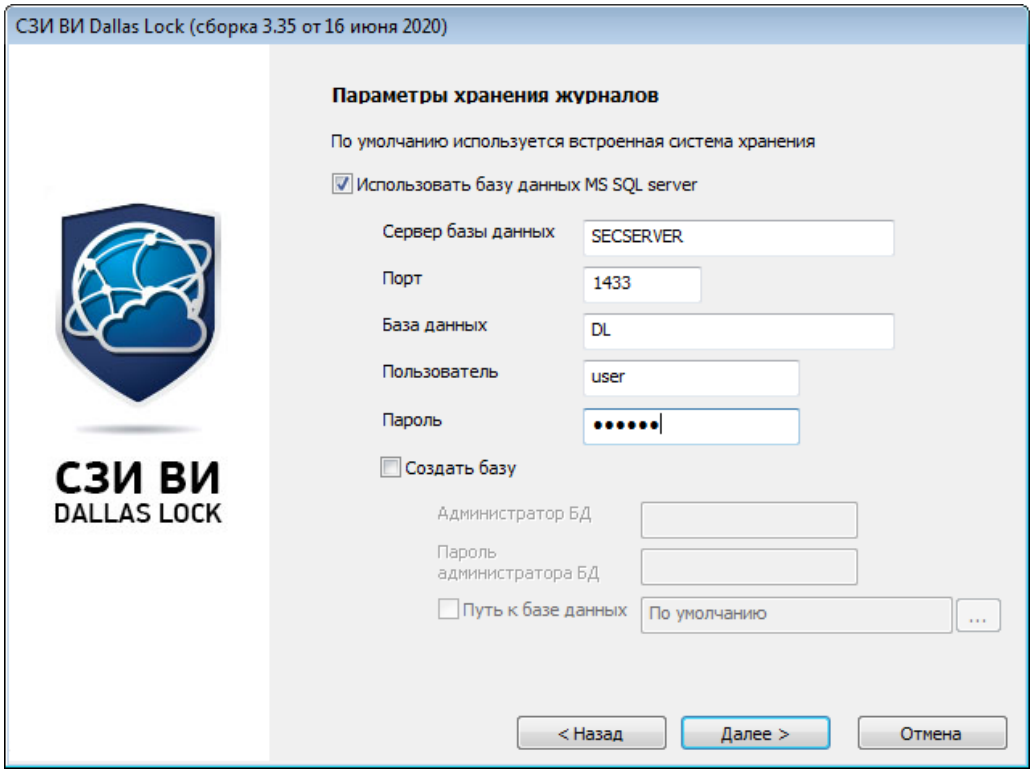

Рис. 35. Подключение к существующей БД в процессе установки СБ

3. Нажать кнопку «Далее» и выполнить дальнейшие действия для установки Центра управления СЗИ ВИ Dallas Lock.

3.1.2 Создание новой БД и пользователя в процессе установки

Для этого необходимо:

1. В окне «Параметры хранения журналов» поставить флаг «Использовать базу данных MS SQL Server».
2. Поставить флаг у параметра «Создать базу».
3. Указать логин и пароль администратора БД, от имени которого будет создана БД.
4. Заполнить поля подключения к БД (рис. 36):
   - имя или IP-адрес ПК, на котором расположен сервер базы данных;
   - порт подключения;
   - имя новой базы данных;
   - логин и пароль для нового пользователя базы данных.

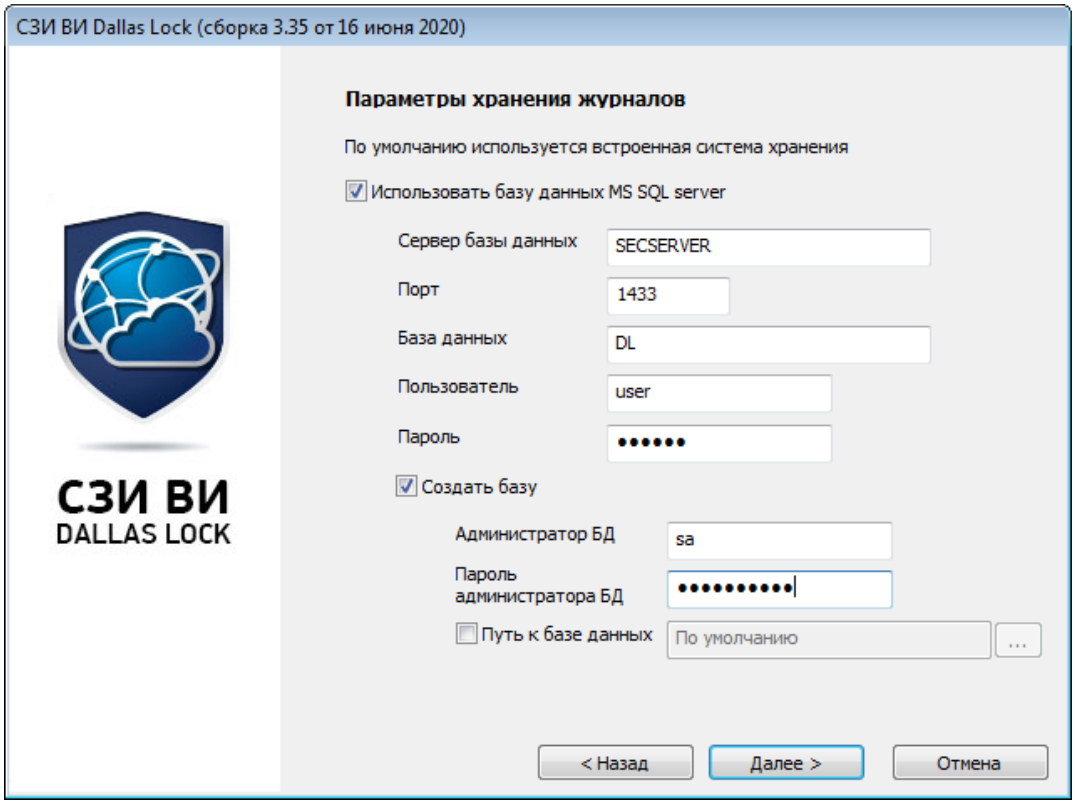

Рис. 36. Создание новой БД и пользователя

5. Нажать кнопку «Далее» и выполнить дальнейшие действия для установки Центра управления СЗИ ВИ Dallas Lock. В случае ввода неверных данных, появится окно с описанием ошибки (рис. 37).

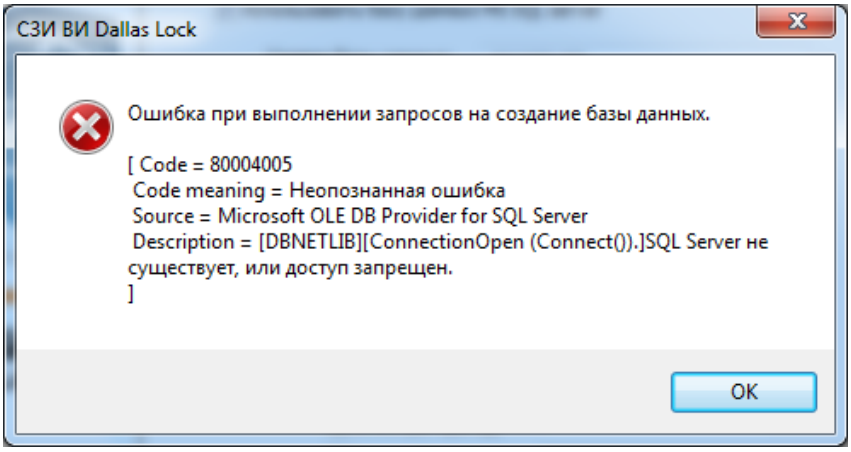

Рис. 37. Ошибка при вводе неверных данных

6. Выполнить перезагрузку системы после окончания установки.

3.2 Подключение к существующей БД из Консоли

Для этого необходимо:

1. Открыть дополнительное меню Консоли → «Параметры хранения журналов…».
2. В окне «Параметры хранения журналов» поставить флаг «Использовать базу данных MS SQL Server».
3. Заполнить поля подключения к БД (рис. 38):
   - имя или IP-адрес ПК, на котором расположен сервер базы данных;
   - порт подключения;
   - имя базы данных;
   - логин и пароль пользователя базы данных.

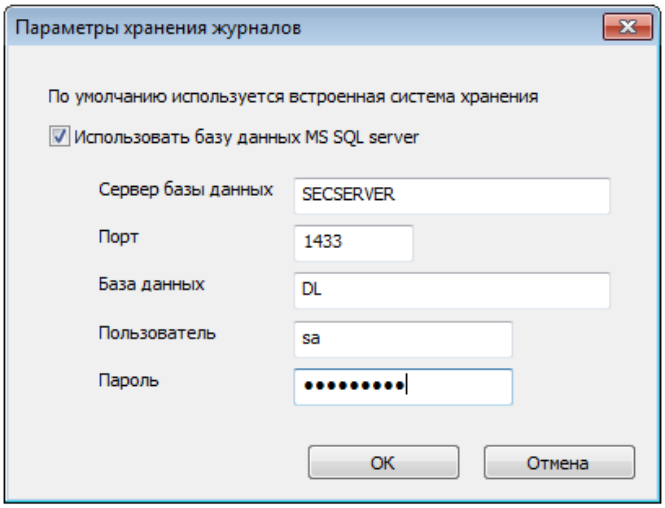

Рис. 38. Параметры хранения журналов

4. Нажать кнопку «ОК».

Для сохранения журналов в файлы, необходимо снять флаг «Использовать базу данных MS SQL Server» и нажать кнопку «ОК».

4 ЭКСПЛУАТАЦИЯ

4.1 Изменение размера БД

При использовании внешней БД в Центре управления СЗИ ВИ Dallas Lock 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. 39).

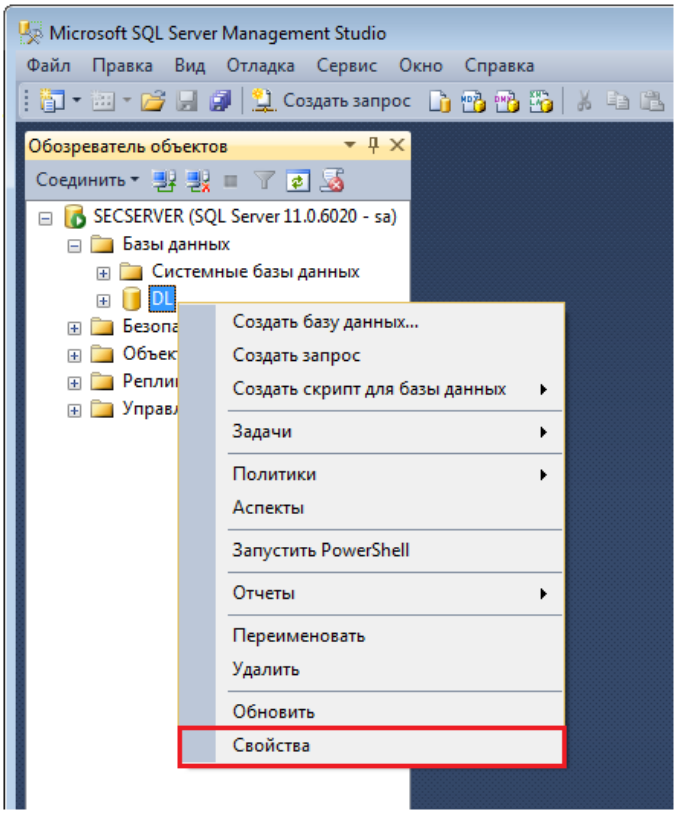

Рис. 39 – Обозреватель объектов

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. 40).

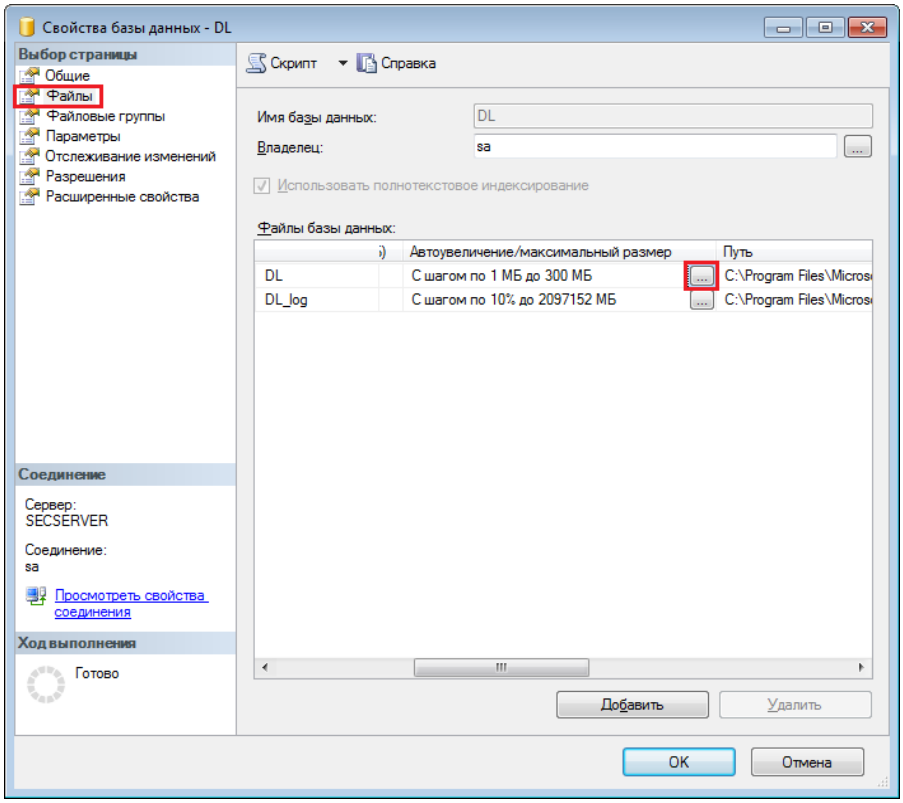

Рис. 40 – Свойства базы данных

4. Откроется окно, в котором возможно задать предельный размер БД (рис. 41).

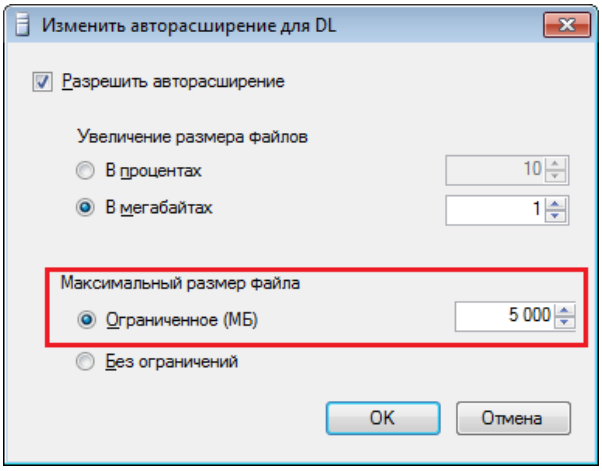

Рис. 41 – Изменение предельного размера БД

4.2 Регистрация событий

События, связанные с БД, фиксируются в «Журнал СУД». Для более детального просмотра события, необходимо щелкнуть по нему два раза левой кнопкой мыши (рис. 42).

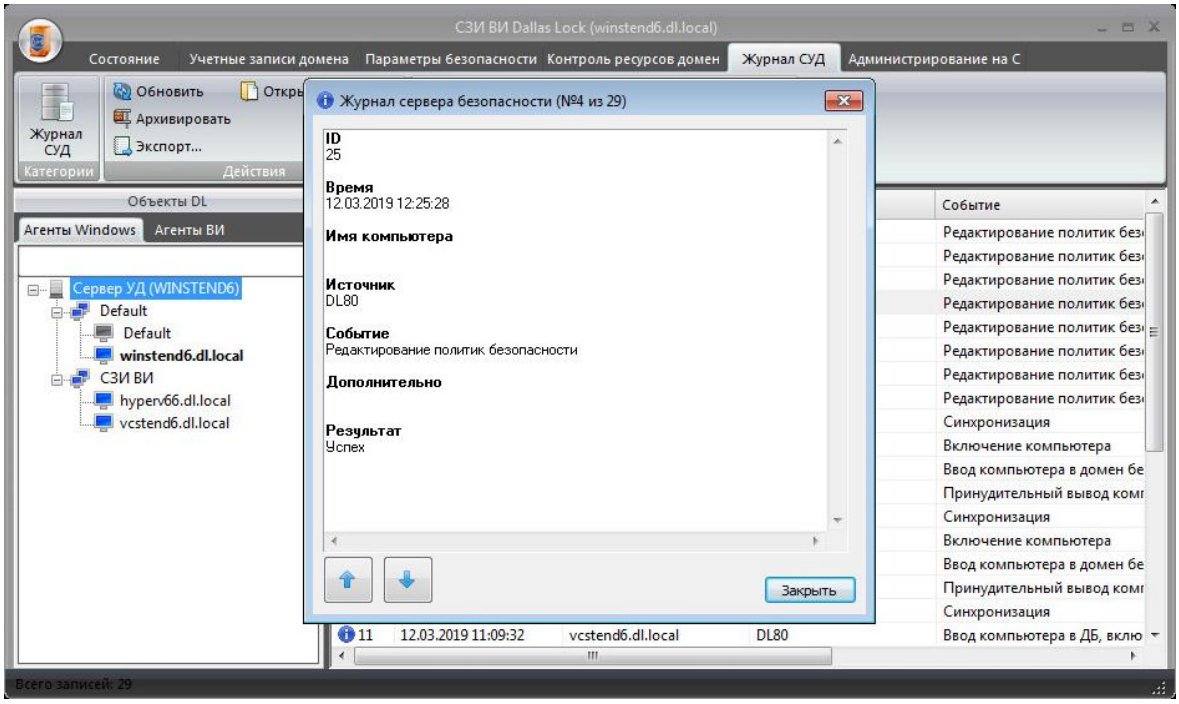

Рис. 42 – Окно детального просмотра события

Во внешней БД сохраняются данные журналов клиентов, с установленными агентами DL, а также журнала Сервера УД.

Для того, чтобы собрать журналы со всех клиентов, необходимо открыть дерево «Агенты Windows», выбрать Сервер УД в дереве объектов, перейти на вкладку «Состояние» → «Основное» и нажать на кнопку «Собрать журналы» (рис. 43).

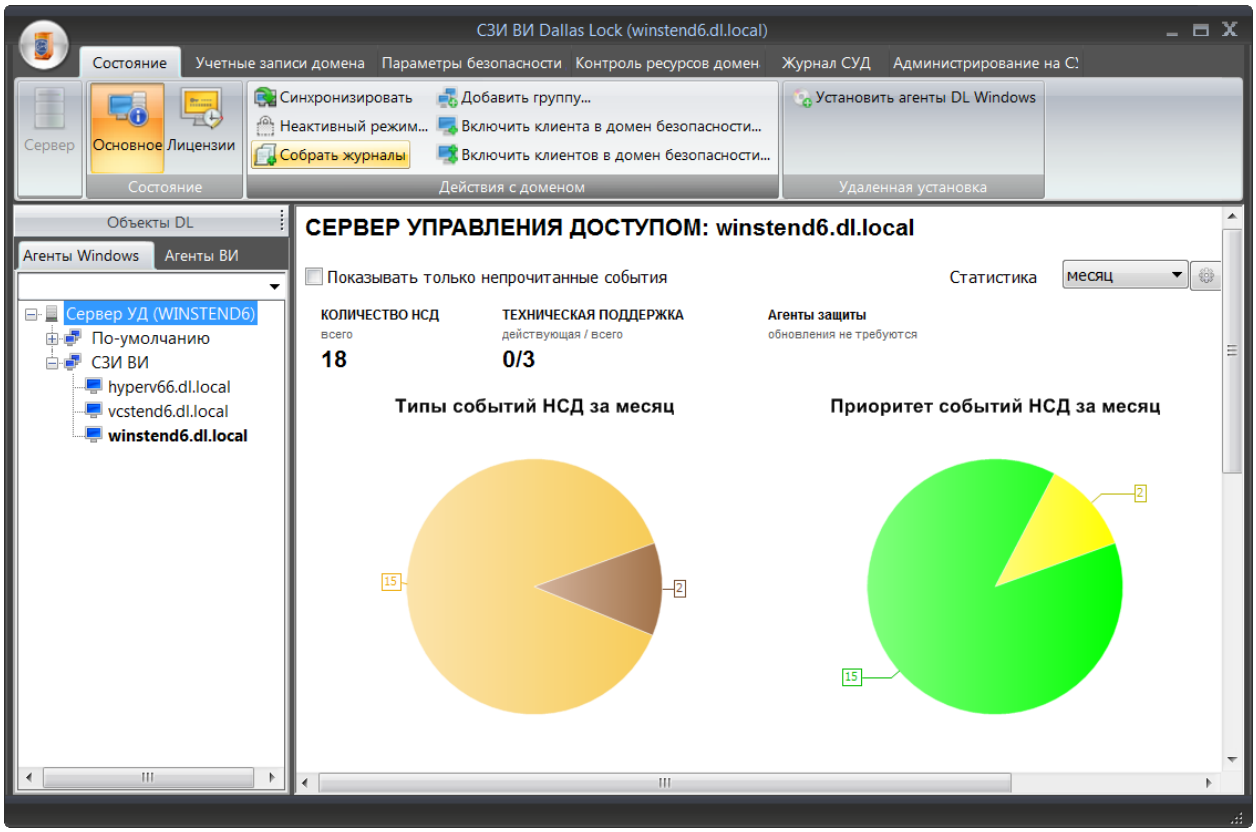

Рис. 43 – Собрать все журналы всех Windows клиентов

Также возможно собрать журнал у определенного клиента, для этого необходимо открыть дерево Windows, выбрать нужного клиента в дереве объектов и перейти на вкладку «Журналы». Далее на панели «Действия с журналами» нажать на кнопку «Собрать журналы» (рис. 44).

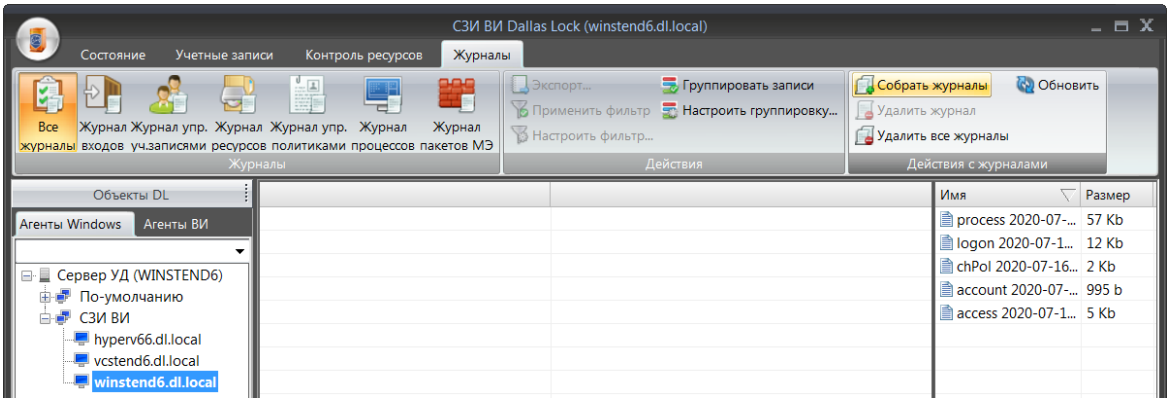

Рис. 44 – Собрать журналы клиента

В случае возникновении сбоя при сохранении данных аудита, собранные файлы журналов хранятся на Сервере УД 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 с каждого отдельного клиента, необходимо во вкладке Windows перейти на уровень клиента и выбрать вкладку «Журналы» (рис. 45). 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.

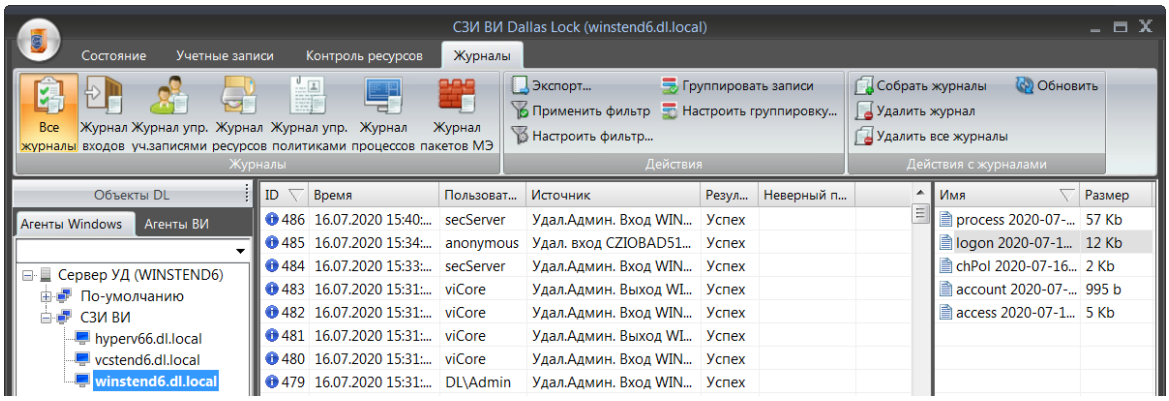

Рис. 45 – Журналы всех Windows клиентов

Взаимодействие с журналами подробно описано в разделе 8.2, документа «Руководство по эксплуатации» ПФНА.501410.001 РЭ.

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

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

Термины и сокращения

Некоторые термины, содержащиеся в тексте руководства, уникальны для СЗИ ВИ, другие используются для удобства, третьи выбраны из соображений краткости.

Сокращение	Полная формулировка
АИБ	администратор информационной безопасности
АУД	агент управления доступом. Компонент Центра управления СЗИ ВИ Dallas Lock, устанавливаемый также на объекты ВИ — сервер vCenter for Windows и гипервизор Hyper-V для обеспечения выполнения политик безопасности
СУБД	система управления базами данных
БД	база данных
Консоль	Консоль Центра управления СЗИ ВИ Dallas Lock. Средство администрирования СЗИ ВИ
ОС	операционная система
ПК	персональный компьютер
ПО	программное обеспечение
Сервер УД	сервер управления доступом. Компонент Центра управления СЗИ ВИ Dallas Lock, обеспечивающий защиту серверов виртуализации, посредством взаимодействия с АУД
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах