# **ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 16**

# **Работа с журналом аудита базы данных**

**Цель и задачи работы**

Целью данной работы является получение практических навыков работы с журналами аудита базы данных.

Для достижения цели работы необходимо решить следующие задачи.

1. Изучить основные журналы, используемые для отображения событий, происходящих с сервером и с его окружением.
2. Ознакомиться с основными средствами просмотра данных этих журналов, изучить их возможности.
3. Выполнить практическое задание по работе с журналами сервера изученными средствами.

**Краткие теоретические сведения**

При работе сервера необходимо отслеживать события, связанные с его работой. Главная цель при этом – как можно быстрее обнаруживать проблемы, возникающие на сервере, и оперативно реагировать на них.

Самое простое средство мониторинга работы MS SQL Server – журналы сервера. Считается, что рабочий день администратора на предприятии должен начинаться с просмотра журналов событий на всех серверах. Для MS SQL Server начиная с версии 2005 выделяются 4 журнала:

* журнал событий самого SQL Server;
* журнал событий SQL Server Agent;
* журнал событий операционной системы Windows;
* журнал событий приложений Windows.

Журналы можно просматривать разными способами. Самый простой и рекомендованный – использовать просмотрщик, который встроен в SQL Server Management Studio. Запустить его можно из контейнера Management | SQL Server Logs (Управление) | Журналы SQL Server. В списке журналов нужно щелкнуть правой кнопкой мыши по требуемому журналу и в контекстном меню выбрать View SQL Server Log (Просмотреть журнал SQL Server). Откроется окно про- смотрщика журналов (рисунки 1,2).

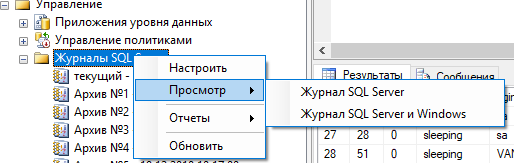


Рисунок 1 - Открытие окна просмотра журналов

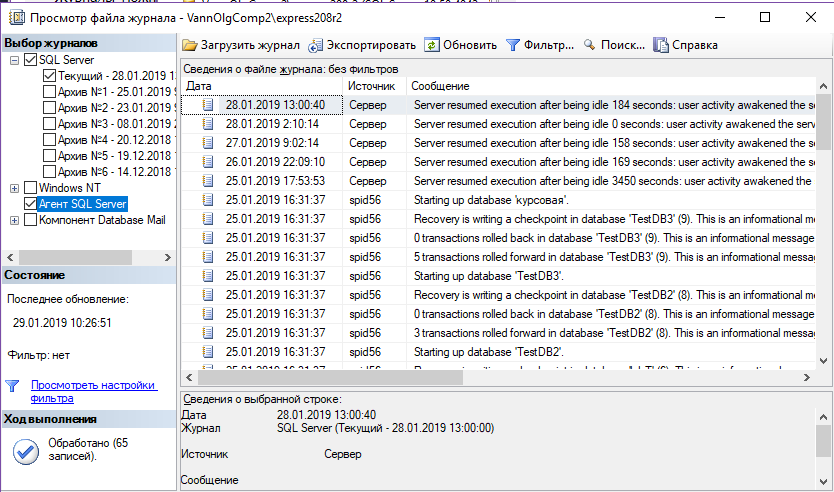


Рисунок 2 - Окно просмотра журналов

При помощи просмотрщика журналов можно просматривать не только журналы SQL Server, но и журналы SQL Server Agent, Windows и Database Mail, можно экспортировать данные из журналов при помощи кнопки Export (Экспортировать), в том числе и в очень удобный для загрузки в базу данных формат CSV, можно настраивать фильтрацию и производить поиск нужной информации.

Журналы событий SQL Server можно просматривать и «вручную», при помощи любого текстового редактора. По умолчанию они находятся в каталоге C:\Program Files\Microsoft SQL Server\MSSQL\LOG. Там же находятся и журналы SQL Server Agent.

Если вам нужен более подробный протокол событий, происходящий на сервере, можно воспользоваться параметром C2 Audit Tracing. Его можно установить на вкладке Security (Безопасность) свойств сервера в Management Studio. В этом режиме в каталоге Data (Данные) для данного экземпляра сервера будут автоматически создаваться текстовые файлы с очень подробной информацией, которая может потребоваться для аудита в соответствии со стандартом безопасности C2.

**Порядок выполнения работы**

1. Открыть журнал сервера.

Журнал событий SQL Server был открыт через SQL Server Management Studio (SSMS).

**Действия:**

* Перейти в **Управления → Журналы SQL Server;**
* Щёлкнуть правой кнопкой мыши по журналу и выбрать **Просмотр журнала SQL Server**.

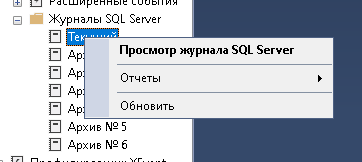


Рисунок 3 – Просмотр журнала SQL Server

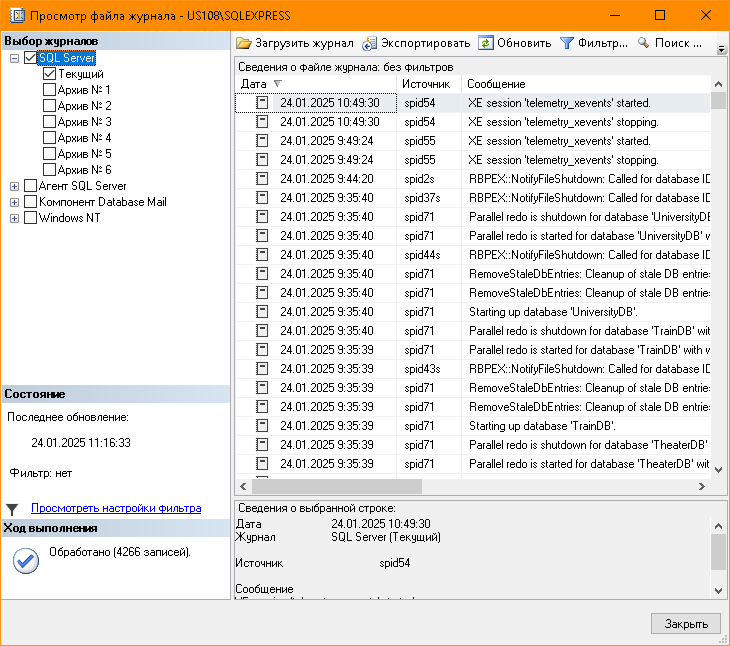


Рисунок 4 – Журнал SQL Server

1. Выявить основные события сервера за последние 12 часов.

Были применены фильтры для отображения событий за последние 12 часов.

**Действия:**

* В окне просмотра журнала нажать Фильтр.
* Установить диапазон времени на последние 12 часов.

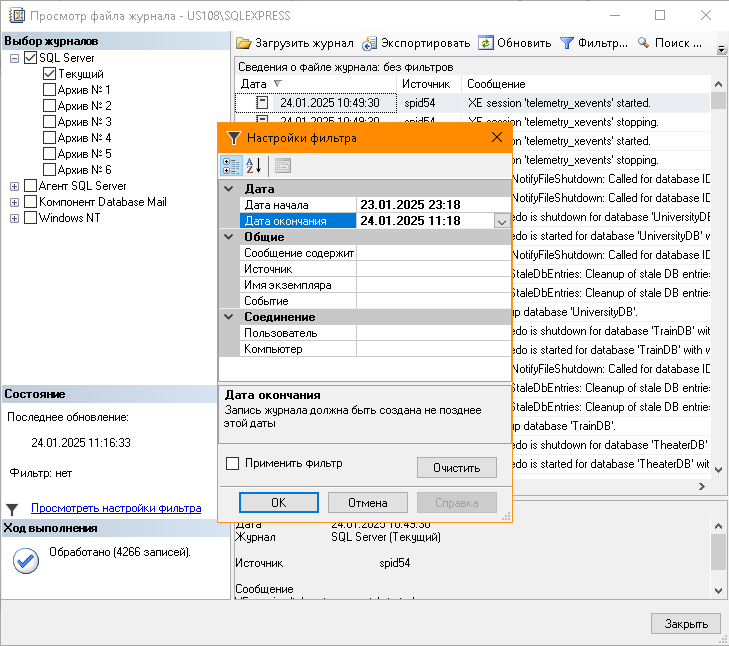


Рисунок 5 – Фильтрация по времени

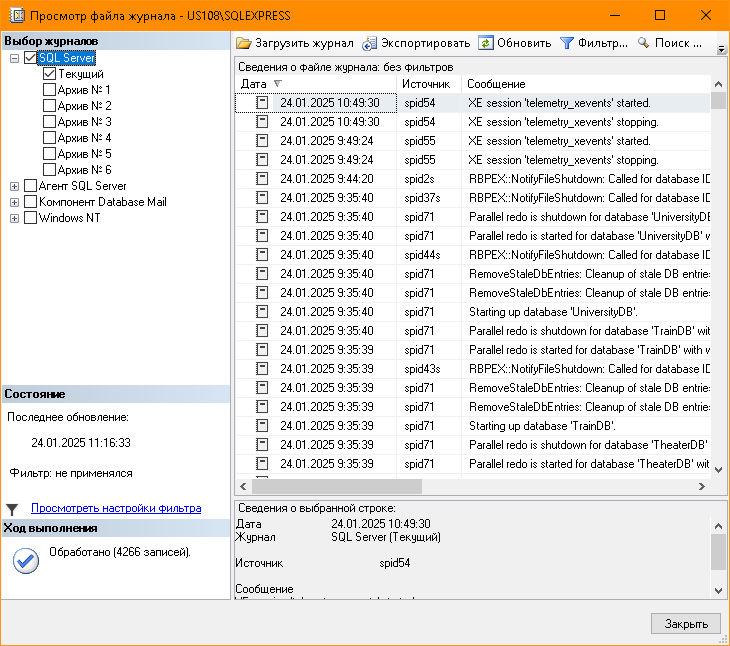


Рисунок 6 – Фильтрация по времени

1. Отобразить события в виде отчёта.
2. Выгрузить журнал в текстовый файл и файл «.csv».

События были экспортированы в файл формата CSV для дальнейшей обработки.

**Действия:**

* В окне просмотра журнала нажать Экспортировать.
* Сохранить файл в формате CSV.
* Данные представлены в табличной форме с указанием времени, типа события и описания.

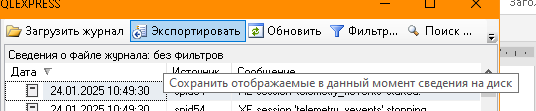


Рисунок 7 – Кнопка экспорта

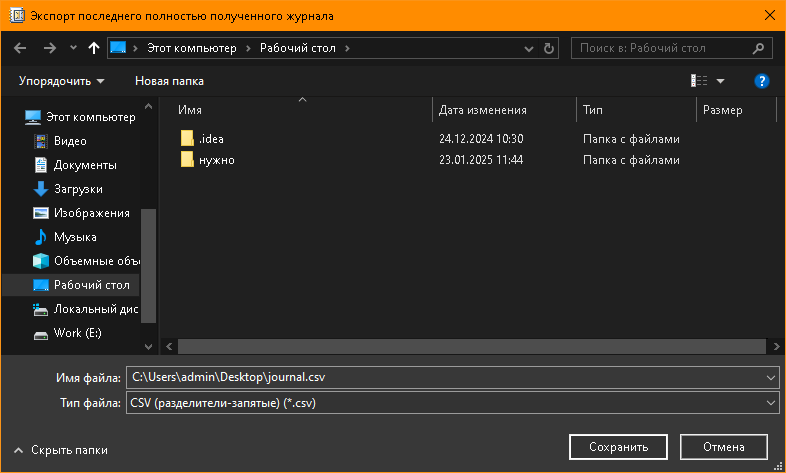


Рисунок 8 – Выбор пути и формата cvs сохранения файла

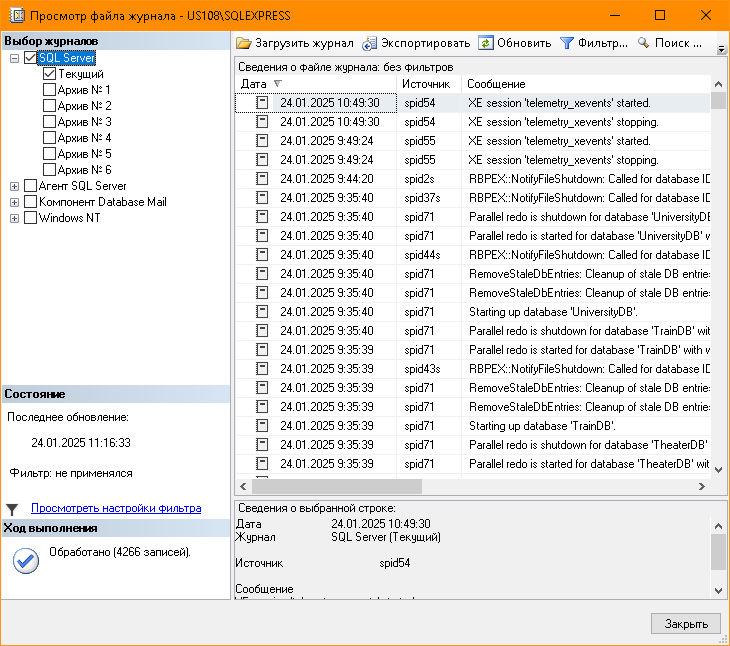


Рисунок 9 – Успешное сохранение

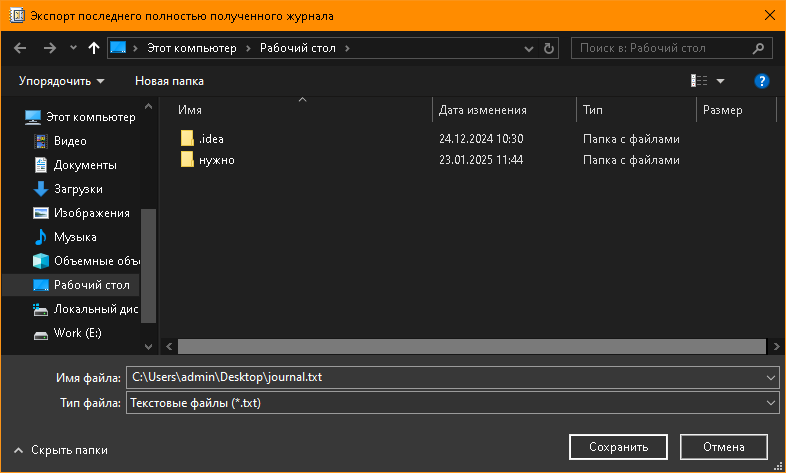


Рисунок 10 – Выбор пути и формата txt сохранения файла

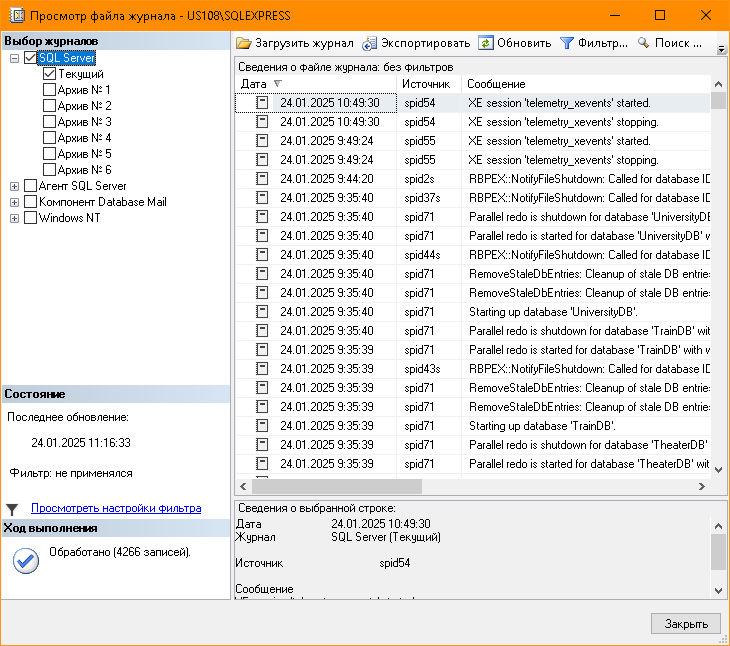


Рисунок 11 – Успешное сохранение

1. Определить положение и открыть с помощью текстового редактора файл, соответствующий журналу.



Рисунок 12 – Иконка журнала в формате cvs



Рисунок 13 – Открытый в блокноте файл cvs



Рисунок 14 – Иконка журнала в формате txt



Рисунок 15 – Открытый в блокноте файл txt

1. Этапы выполнения каждого задания и ответы на контрольные вопросы оформить в отчете о выполнении ПЗ. Прикрепить отчет о ПЗ, файлы из задания 4.

**Контрольные вопросы**

1. **Какие события могут происходить при работе сервера? Зачем их отслеживать?**

При работе сервера могут происходить следующие события:

* Ошибки соединения.
* Изменение конфигурации сервера.
* Ошибки выполнения запросов.
* Аварийные завершения работы служб.

Отслеживание событий необходимо для обеспечения стабильности работы сервера, выявления и устранения ошибок, а также для аудита безопасности.

1. **Каким образом сохраняются данные о событиях сервера?**

Данные о событиях сервера сохраняются в логах, которые хранятся в текстовых файлах или базах данных, обеспечивая доступ к информации о произошедших событиях.

1. **Какие типы журналов сервера выделяются?**

Выделяют следующие типы журналов:

* Журнал событий SQL Server.
* Журнал событий SQL Server Agent.
* Журнал событий операционной системы Windows.
* Журнал событий приложений Windows.

1. **Какие средства просмотра журналов существуют? Каковы их возможности?**

Средства просмотра:

* **SQL Server Management Studio** — встроенный просмотрщик журналов, позволяет фильтровать, искать и экспортировать данные.
* **Просмотр журналов Windows** — для работы с системными и приложенческими журналами.
* **Текстовые редакторы** — для просмотра логов, сохранённых в текстовом формате.
* **Сторонние утилиты** — для анализа данных из журналов (например, Splunk).

1. **Как запустить просмотрщик событий сервера?**

Просмотрщик запускается через SQL Server Management Studio:

* Перейти в **Management → SQL Server Logs**.
* Щёлкнуть правой кнопкой мыши по журналу и выбрать **View SQL Server Log**.