МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт кибернетики и информационных технологий

Кафедра “Кибербезопасность, обработка и хранение информации”

Идришев Әділ Мұратұлы

Организация мониторинга и аудита в MS SQL Server

ДИПЛОМНЫЙ ПРОЕКТ

Специальность 5В100200 – Системы информационной безопасности

Алматы 2021

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени К.И. САТПАЕВА
ИНСТИТУТ КИБЕРНЕТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА КИБЕРБЕЗОПАСНОСТЬ, ОБРАБОТКА И ХРАНЕНИЕ ИНФОРМАЦИИ

«Допущен к защите»
Заведующий кафедрой КОиХИ
канд. техн. наук, доцент
_____ Н.А.Сейлова
“ 25 ” 05 2021г.

ДИПЛОМНЫЙ ПРОЕКТ

на тему: «Организация мониторинга и аудита в MS SQL Server»

по образовательной программе 5В100200 – «Системы информационной безопасности»

Выполнил Идришев Ә.М.

Научный руководитель к.т.н., ассоц. проф. Айтхожаева Е.Ж.

10.05.2021 г.

Алматы 2021

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт кибернетики и информационных технологий

Кафедра “Кибербезопасность, обработка и хранение информации”

5В100200 - Системы информационной безопасности

УТВЕРЖДАЮ
Заведующий кафедрой КОиХИ
канд. техн. наук, доцент
_____ Н.А.Сейлова
“ 25 ” 05 20 21 г.

ЗАДАНИЕ
на выполнение дипломного проекта

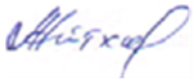
Обучающемуся *Идришев Әділ Мұратұлы*
Тема: *Организация мониторинга и аудита в MS SQL Server*
Утверждена *приказом Ректора Университета № 2131-б* от “*24” 11 2020 г.*
Срок сдачи законченной работы “*04” 05 2021г.*
Исходные данные к дипломному проекту:
механизмы мониторинга и аудита в MS SQL Server, CASE-средство проектирования баз данных CA ERwin Modeling Suite, утилита SQL Server Profiler.
Перечень подлежащих разработке в дипломном проекте вопросов:
а) обзор механизмов мониторинга и аудита в MS SQL Server;
б) проектирование базы данных MS SQL Server в CASE-средстве проектирования БД;
в) организация мониторинга и аудита базы данных;
г) приложения.
Перечень графического материала (с точным указанием обязательных чертежей):
механизмы мониторинга и аудита в MS SQL Server – 1А3; логическая и физическая модели данных в Erwin – 1А3; схема базы данных в MS SQL Server – 1А3; шаблоны и файлы трассировки – 2А3.
Рекомендуемая основная литература: *из 10 наименований*

ГРАФИК
подготовки дипломного проекта

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Мониторинг и аудит в MS SQL Server	01.03.2021 г.	выполнено
Проектирование базы данных MS SQL Server в CASE-средстве	26.03.2021 г.	выполнено
Организация мониторинга и аудита базы данных	26.04.2021 г.	выполнено

Подписи
консультантов и нормоконтролера на законченный дипломный проект с указанием относящихся к ним разделов проекта

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	подпись
Нормоконтроль	магистр техн.наук, ассистент Кабдуллин М.А.	10.05.2021	

Научный руководитель  Айтхожаева Е.Ж.

Задание принял к исполнению обучающийся  Идришев Ә.М.

Дата “_24”11 2020 г.

АҢДАТПА

Бұл жұмыс дерекқордың кең таралған және сұранысқа ие серверлерінің бірі болып табылатын MS SQL Server-де мәліметтер қорын қорғауды ұйымдастыру кезінде қылмыстар мен теріс пайдаланушылықтарды анықтау мәселелеріне арналған. Деректер базасын жобалауға арналған CASE - ERWin құралында жасалған «Дүкен» мәліметтер базасының аудиті мен мониторингін ұйымдастыру туралы мәселе қарастырылды. MS SQL Server 2014-те SQL Profiler графикалық утилитасын пайдалану технологиясы, сондай-ақ сервер мен мәліметтер базасын бақылауға және тыңдауға арналған SQL Audit көрсетілген. Мақалада іздеу профилінің шаблондарын құру, іздік файлды құру, деректер базасының серверіндегі оқиғаларды бақылау және бақылау үшін трек-файлды іске қосу қарастырылған. Іздеу файлы талданды.

АННОТАЦИЯ

Данная работа посвящена проблеме выявления преступлений и злоупотреблений при организации защиты баз данных в MS SQL Server, являющимся одним из самых распространенных и востребованных серверов баз данных. Рассматривается вопрос организации аудита и мониторинга базы данных «Магазин», спроектированной в CASE-средстве проектирования БД - ERWin. Показана технология использования в MS SQL Server 2014 графической утилиты SQL Profiler, а также SQL Audit, предназначенные для мониторинга активности и аудирования сервера и БД. Рассмотрено создание шаблонов профиля трассировки, создание файла трассировки, запуск файла трассировки для аудита и мониторинга событий в сервере БД. Выполнен анализ файла трассировки.

ANNOTATION

This work is devoted to the problem of detecting crimes and abuse when organizing database protection in MS SQL Server, which is one of the most widespread and demanded database servers. The article deals with the organization of audit and monitoring of the "Shop" database, designed in the CASE-database design tool - ERWin. The technology of using the graphical utility SQL Profiler in MS SQL Server 2014 is shown, as well as SQL Audit intended for monitoring the activity and listening of the server and the database. Creation of trace profile templates, creation of a trace file, launching a trace file for auditing and monitoring events in the database server are considered. The trace file has been analyzed.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Обеспечение безопасности данных - один из важнейших моментов любого предприятия: в банках, в медицине и во множестве других сферах жизнедеятельности человека в современном мире.

Большинство данных хранится в базах данных (БД). Безопасность баз данных обеспечивается применением широкого диапазона средств, механизмов и методов для защиты информации, хранящейся в базах данных. Безопасность БД – это отдельная специализированная область в более широких сферах компьютерной безопасности, информационной безопасности и управления рисками.

Росс Андерсон часто говорил, что «по своей природе большие базы данных никогда не будут свободны от злоупотреблений в результате нарушений безопасности; Если большая система предназначена для облегчения доступа, она становится небезопасной; Если сделана водонепроницаемая, становится невозможно использовать». Это называется «Правилом Андерсона».

MS SQL Server является одной из наиболее известных систем управления базами данных. Для организации баз данных в MS SQL Server используется реляционная модель. Данная модель баз данных была разработана еще в 1970 году Эдгаром Коддом. И на сегодняшний день она практически считается стереотипом для организации баз данных [1].

Одной из основных характеристик информационной безопасности, наряду с конфиденциальностью, целостностью и доступностью, считается учет. Способы и средства учета и исследования обеспечивают вероятность выявления и регистрации значимых действий, связанных с защищённостью, или же всевозможных попыток получения доступа, а также уничтожения системных ресурсов.

Контрольное слежение за выполняемыми действиями в системе при работе с конфиденциальными данными или же при выполнении критичных операций, называется аудитом.

Очень близким к понятию аудита является понятие мониторинга. Мониторинг используется для исследования работы ОС, её служб, служб сервера базы данных, хранимых процедур и т.д. Итоги мониторинга применяются для оптимизации работы сервера базы данных, для отслеживания тенденций повышения или же понижения производительности системы и выявления их причин.

Аудит и мониторинг снижают риск внутренних опасностей от легальных пользователей. Осуществление аудита и мониторинга в всевозможных SQL-серверах производится собственными встроенными механизмами.

Целью дипломной работы является организация мониторинга и аудита в MS SQL Server базы данных для предметной области «Магазин», включая этап разработки и проектирования БД, а также внедрение и использование механизмов мониторинга и аудита в сервер MS SQL SERVER.

1 Мониторинг и аудит в MS SQL Server

1.1 Механизмы мониторинга и аудита

На этапе функционирования, сервер баз данных обрабатывает запросы, поступающие от пользователей. Для обработки запросов сервер использует средства, выделенные ему операционной системой. Для того, чтобы узнать, насколько сервер базы данных в данный момент загружен, какие ресурсы ему сейчас доступны, существуют специальные средства мониторинга, встроенные в сервера баз данных.

Мониторинг вводится для исследования за работой операционной системы, ее служб, служб сервера баз данных, хранимых процедур, времени нахождения пользователя в системе и т.д. Итоги мониторинга используются для улучшения работы сервера баз данных.

К средствам мониторинга относятся: специальные встроенные утилиты, системные процедуры сервера баз данных. А также внутри сервера БД имеются специальные системные таблицы, в которые автоматически заносится информация о текущем состоянии системы.

Мониторинг позволяет определить:

- пользователей, работающих с сервером базы данных;
- объем памяти, используемый сервером БД;
- объем свободной памяти, доступной серверу БД;
- что ожидает некоторый запрос;
- причины понижения производительности сервера БД [2];

Аудит представляет собой контрольное слежение за выполняемыми действиями в сервере БД, что особенно необходимо при работе с конфиденциальными данными или же при выполнении критичных операций. Контрольный след поможет выявить нарушителя, если произошло нарушение характеристик информационной безопасности (конфиденциальность, целостность, доступность данных), имеется подозрение, что совершено несанкционированное вмешательство в базу данных.

Для хранения контрольного следа, как правило, применяется определенный файл, в который система автоматически записывает все произведенные пользователем операции при работе с обычной базой данных. Обычно запись в файле содержит следующую основную информацию: запрос (исходный текст); терминал, с которого была вызвана операция; пользователь, задавший операцию; дату и время запуска операции; базовые отношения, кортежи и атрибуты, используемые в операции; старые значения и новые значения данных [3].

В сервере MS SQL SERVER имеется несколько встроенных средств аудита и мониторинга, которые представлены ниже.

SQL Trace. В SQL Trace с помощью системных хранимых процедур создается файл трассировки, в котором регистрируются события, если они являются экземплярами классов событий, перечисленных в определении трассировки при ее создании. Эти события возможно отфильтровать из трассировки

или поставить в очередь для их назначения. Местом назначения могут быть файлы или объекты управления SQL Server (SMO), которые могут использовать информацию трассировки в приложениях, управляющих SQL Server.

C2 Audit. Режим аудита C2 настраивается с помощью SQL Server Management Studio или же с помощью параметра **режима аудита c2** в **sp_configure**. Выбор этого режима настроит сервер на запись неудачных, и успешных попыток доступа к операторам и объектам. Эта информация может помочь профилировать активность системы и отслеживать возможные нарушения политики безопасности.

Триггеры предполагают собой особой тип хранимой процедуры, которая вызывается автоматически при выполнении конкретного действия над объектами, находящимися под управлением сервера БД .

Триггеры DDL автоматически запускаются при выполнении различных событий языка DDL. Эти события в основном соответствуют инструкциям Transact-SQL, которые начинаются с ключевых слов CREATE, ALTER, DROP, GRANT, DENY, REVOKE или UPDATE STATISTICS. Системные хранимые процедуры, выполняющие операции, подобные операциям DDL, также могут запускать триггеры DDL. Применяют триггеры DDL, чтобы:

- предотвращать конкретных изменений в схему базы данных;
- настроить выполнение в базе данных некоторых действий в ответ на изменения в схеме базы данных;
- записать изменения или события схемы базы данных.

Триггеры DDL срабатывают в ответ на событие Transact-SQL, обработанное текущей базой данных или текущим сервером. Область триггера зависит от события. Например, триггер DDL, созданный для срабатывания на событие CREATE TABLE, может срабатывать каждый раз, когда в базе данных или в экземпляре сервера возникает событие CREATE_TABLE.

Триггеры DML позволяют контролировать целостность сущностей или же целостность домена. Они автоматически запускаются при выполнении команд INSERT, DELETE, UPDATE. Целостность сущностей обычно контролируется на самом нижнем уровне с помощью индексов, являющихся частью ограничений PRIMARY KEY и UNIQUE или создаваемых независимо от ограничений. Целостность домена контролируется через ограничения CHECK, а ссылочная целостность — через ограничения FOREIGN KEY. Триггеры DML полезны в случаях, когда функции ограничений не удовлетворяют функциональным потребностям приложения.

Change Tracking – это отслеживание изменений. Эффективный механизм отслеживания изменений для приложений. Используется, чтобы приложения могли запрашивать изменения данных в базе данных и получать доступ к информации. Для настройки отслеживания изменений можно использовать операторы DDL или SQL Server Management Studio.

Change Data Capture (CDC) представляет собой механизм ограничения влияния на исходные данные при загрузке свежих данных в оперативные хранилища данных и хранилища данных, CDC дополняет инструменты интеграции корпоративной информации.

Perfomance monitor (монитор производительности)**,** используется для настройки производительности. Дает информацию о том, как работает SQL Server, и как работает Windows Server.

Монитор производительности определяет статистику производительности сквозь определенные промежутки времени и сохраняет данную статистику в файле. Администратор базы данных избирает временной интервал, формат файла и отслеживаемую статистику. После того, как статистика будет собрана за конкретный промежуток времени (часы или же дни), ее можно использовать для выполнения анализа производительности.

SQL Audit. Аудит среды SQL Server Database Engine или отдельной базы данных включает в себя отслеживание и фиксацию (запись) событий, происходящих в ядре SQL Server - Database Engine. Аудит среды SQL Server разрешает проводить аудит сервера, который имеет возможность подключать в себя спецификации аудита сервера для мероприятий на уровне сервера, а еще спецификации аудита базы данных для мероприятий на уровне базы данных. Действия аудита могут записываться в журналы событий или файлы аудита [4].

1.2 Утилита SQL Server Profiler

SQL Server Profiler отслеживает действия обработки ядра, к примеру, начало пакета или же транзакции, и регистрирует данные о происходящих событиях в таблице SQL Server или же в файле. Этим самым обеспечивая учет (аудит и мониторинг) операций серверов и баз данных. Включение в аудит какой-либо из категорий событий приведет к сохранению следующей информации о событиях:

- дата и время события;
- учетная запись пользователя;
- тип события;
- результат выполнения действия (успешно или нет);
- место события (к примеру, имя компьютера);
- имя объекта, к которому осуществлялся доступ;
- текст SQL-запроса (за исключением паролей).

SQL Profiler позволяет фиксировать фактически все события, которые имеют место в SQL Server, включая:

- действия конечных пользователей (все SQL команды, вход/выход из системы, использование ролей приложений);
- действия DBA (действия отличные от Grant/Revoke/Deny, а также события безопасности и конфигурирования (БД или сервера));
- события безопасности (Grant/Revoke/Deny, добавление/удаление /изменение логина пользователя/роли);
- сервисные события (резервирование/восстановление/bulk insert/bcp/ DBCC команды);
- события сервера (завершение, пауза, запуск);
- события аудита (добавление, изменение, отключение аудита)

Эта информация полезна, в случае если нужно установить, кто и когда выполнял, и какие, действия в базе данных. При аудите и мониторинге SQL Profiler разделяет регистрируемую информацию на категории по типу событий. Комплект зарегистрированных событий именуется профилем трассировки (trace). Файл, содержащий профиль трассировки именуется трассировочным файлом, а таблица с профилем трассировки - трассировочной таблицей. Подлежащие трассировке (регистрации) данные можно определить в шаблоне профиля трассировки.

В системе есть интегрированные шаблоны SQL Profiler, но пользователь имеет возможность поменять любой из имеющихся шаблонов или же сделать собственный [5].

Механизмы мониторинга и аудита MS SQL Server приведены в Приложении Б на листе 1.

2 Проектирование базы данных MS SQL Server в CASE-средстве

ERWIN является одним из CASE средств. Главное назначение ERWIN это моделирование данных. Он разрешает делать различные модели данных, выполнять автоматическое преобразование данных моделей, генерировать схемы баз данных и описание данных на уровне программного кода. В ER-методе применяется терминология, в которой определены сущность, связь, атрибут [6].

Сущность - это объект, представляющий интерес для пользователя: студенты, договора, машины, банковские счета, товар, продавцы и т.д.

Атрибут - это свойство сущности. Например, у сущности Товар есть свои атрибуты, такие как, дата поставки, поставщик, цена, количество.

Связь – представляет собой соединение между двумя или более экземплярами сущностей. Связи различаются по типу: один к одному (1:1), один к многим (1:M), многие к многим (M:M).

При проектировании с использованием ER-метода используются ER-диаграммы, включающие в себя все сущности (представляющие интерес для пользователя), атрибуты и связи. По построенной ER-диаграмме определяется перечень таблиц и первичный ключ для каждой из таблиц. Вслед за тем подготавливается перечень всех представляющих внимание атрибутов и каждый их них назначается одной из таблиц. В случае, если есть связь M:M то эта связь требует собственной таблицы [7].

2.1 Проектирование логической модели данных

Была спроектирована ER-диаграмма для предметной области «Магазин», которая представлена на рисунке 2.1. В предметной области были определены сущности и атрибуты, а также связи между сущностями. В ER-диаграмме сущности представляются в виде прямоугольников, связи – в виде ромбов, атрибуты – в виде овалов. Для целостности данных были определены связи между сущностями через первичные ключи (Primary Key – PK) и внешние ключи (Foreign Key – FK).

Сущность ПРОИЗВОДИТЕЛЬ (Код производителя (PK), Телефон, E-mail, Страна, Название АО).

Сущность ПРОДАВЦЫ (Код продавца (PK), ФИО, Телефон, Отдел, Адрес, Должность).

Сущность ПОСТАВЩИК (Код поставщика (PK), Название АО, Телефон, Контактное лицо, Код производителя(FK), Адрес).

Сущность ТОВАРЫ (КОД ТОВАРА(PK), Цена, Название, Количество, Код поставщика(FK), Срок годности).

Сущность ПРОДАЖИ (Код продажи(PK), Дата продажи, Количество, Код товара (FK), Код продавца (FK)).

Связь между ПРОИЗВОДИТЕЛЕМ и ПОСТАВЩИКОМ (1:M), один производитель продвигает товар многим поставщикам.

Связь между ПОСТАВЩИКОМ и ТОВАРОМ (1:M), один поставщик поставляет много товаров.

Связь между ТОВАРОМ и ПРОДАЖЕЙ (1:M), один тип товара продается много раз.

Связь между ПРОДАЖАМИ и ПРОДАВЦАМИ (M:1), много продаж выполняет один продавец.

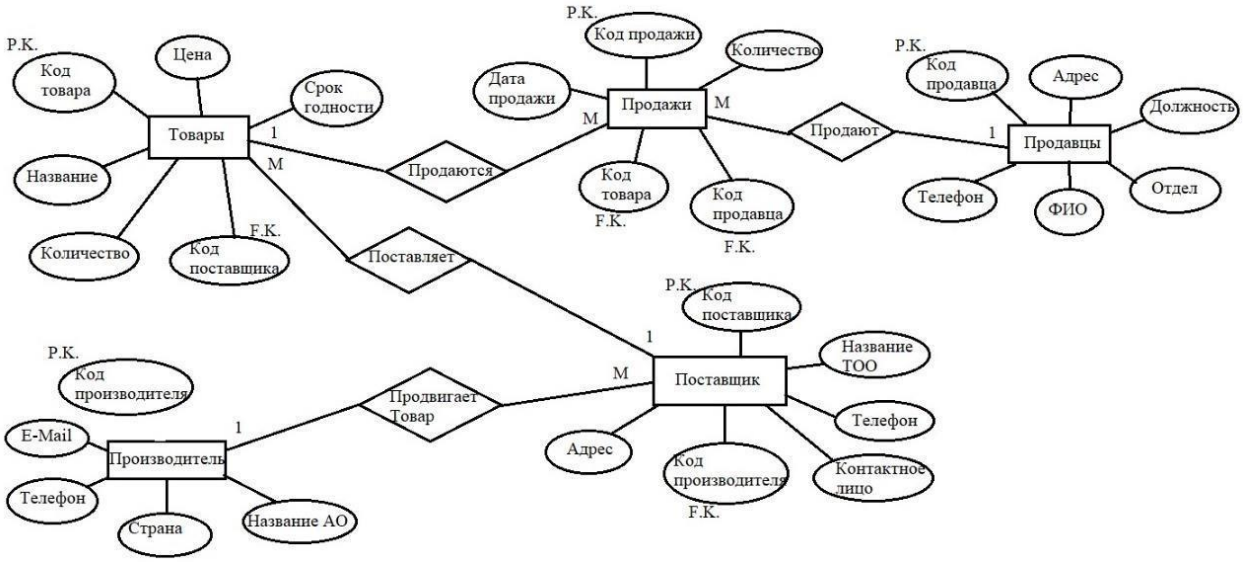


Рисунок 2.1 - ER-диаграмма

Модель на логическом уровне ERWIN – это логическая модель, которая является информационной и не связана с определенной реализацией в СУБД.

Логическая модель предметной области «Магазин» представлена на рисунке 2.2 с сущностями и атрибутами а также со связями и первичными и внешними ключами.

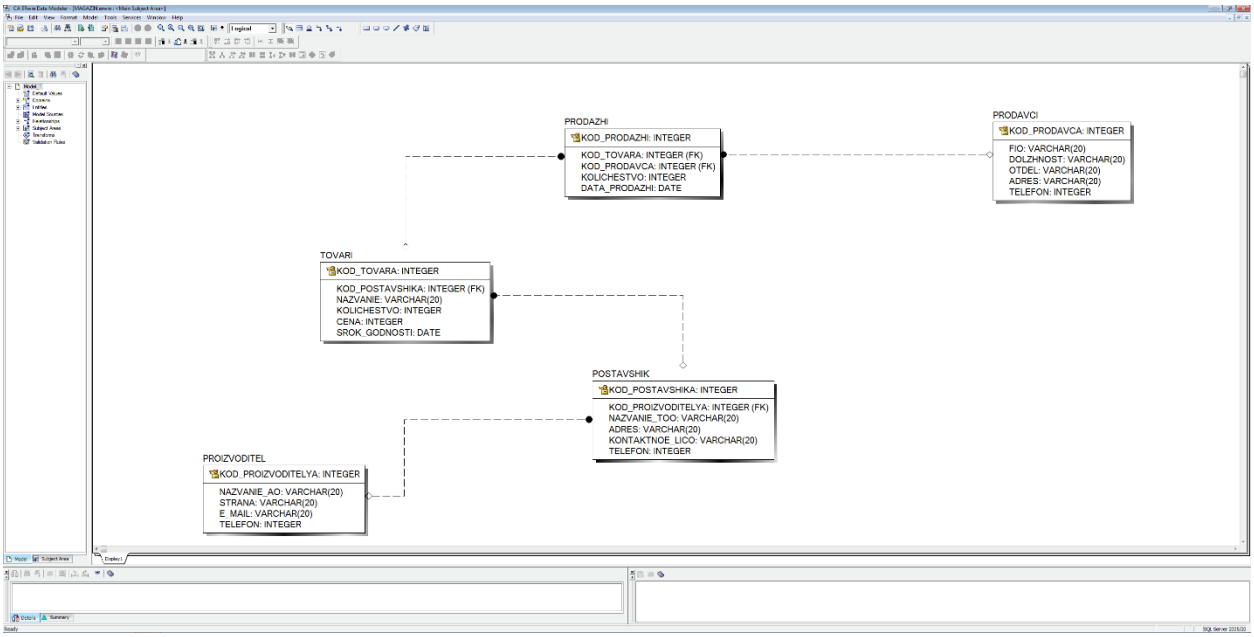


Рисунок 2.2 - Логическая модель данных

2.2 Проектирование физической модели данных

Физическая модель данных зависит от определенной СУБД, учитывает все требования конкретной СУБД. В физической модели находится информация обо всех объектах БД. В физической модели данных представлена вся информация об определённых физических объектах: таблицах, колонках, индексах, ограничениях целостности и т.д [8].

Физическая модель предметной области «Магазин» представлена на рисунке 2.3 с типами данных.

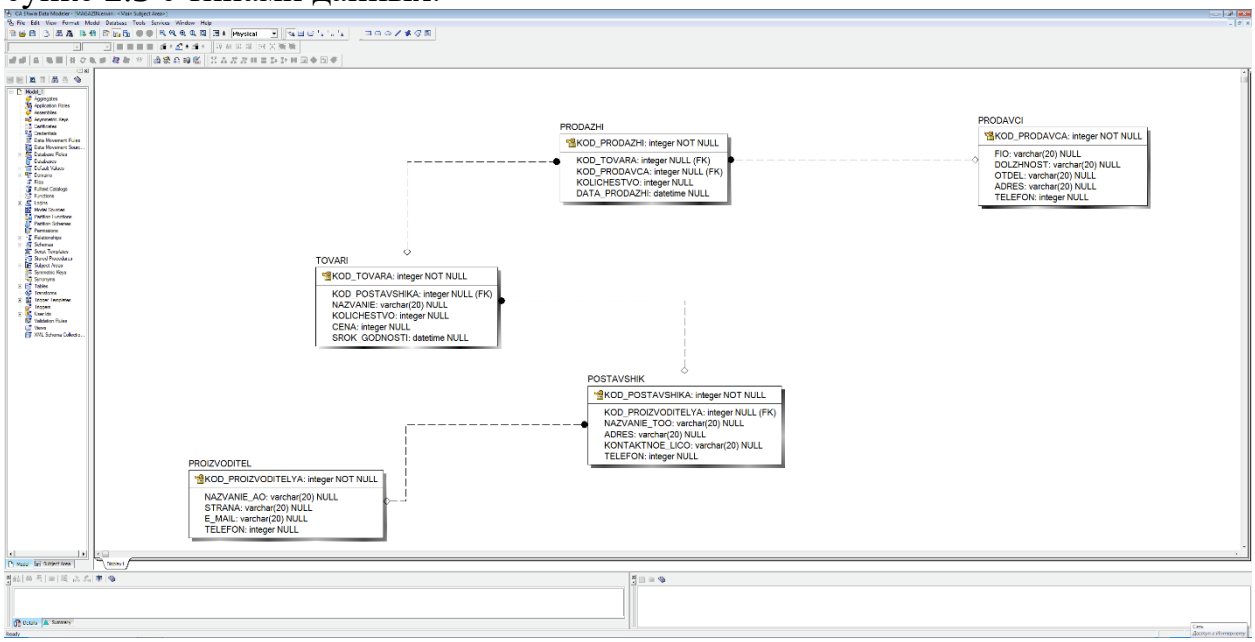


Рисунок 2.3 - Физическая модель данных

На рисунке 2.4 представлено правило ограничения минимального и максимального значения для столбца КОЛИЧЕСТВО для таблицы ТОВАРЫ.

Ограничения - это особые объекты в SQL Server, с помощью которых возможно задать правила допустимости конкретных значений в столбцах с целью обеспечения автоматической целостности базы данных. Ограничения создают некоторое условие на те данные, которые будут вводится в таблицу.

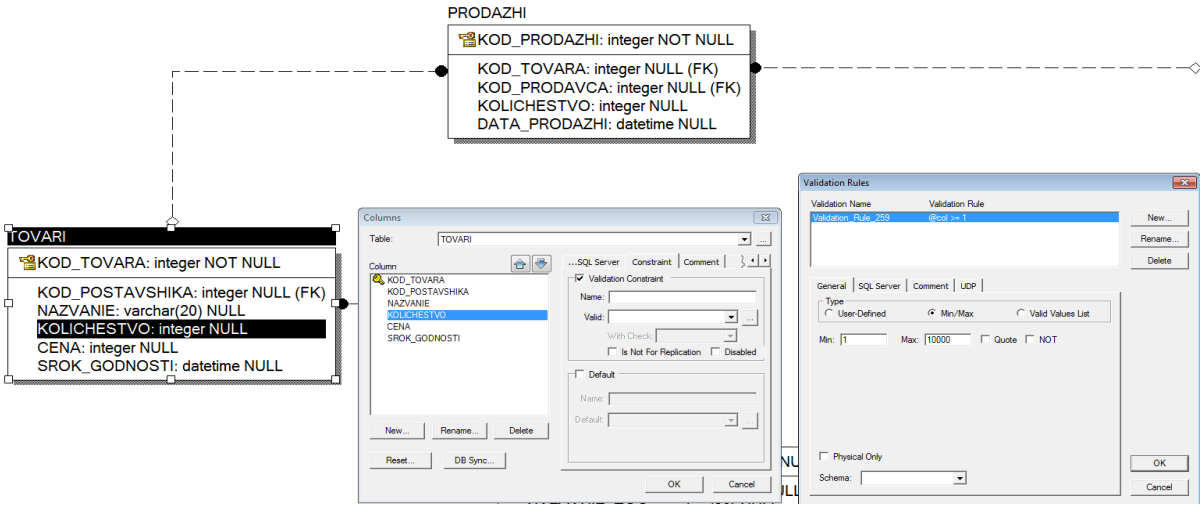


Рисунок 2.4 - Ограничение мин/макс

На рисунке 2.5 представлены ограничения типа Valid Values List в котором возможен ввод данных только допустимых значений.

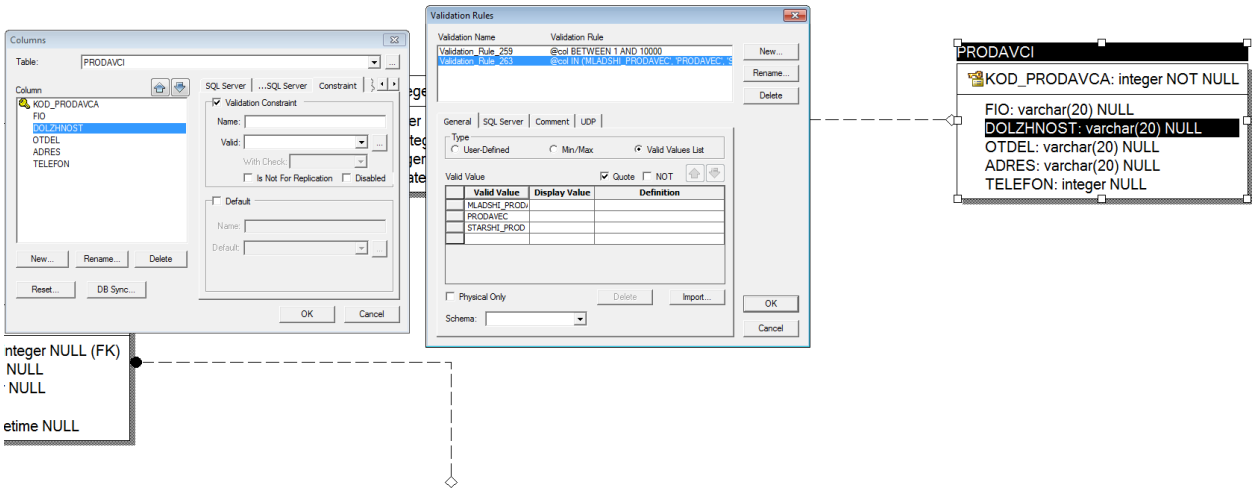


Рисунок 2.5 - Ограничение допустимых значений

Модели БД логического и физического уровня Erwin приведены в Приложении Б на листе 2.

2.3 Реализация базы данных в MS SQL Server

С использованием SQL скриптов, полученных в результате проектирования БД в Erwin, были созданы в БД Magazin таблицы (Proizvoditrel, Postavshik, Tovari, Prodazhi, Prodavci). SQL скрипты приведены в Приложении А. Была создана схема БД, наглядно показывающая связи между таблицами БД, приведённая на рисунке 2.6. Схема БД приведена в Приложении Б на листе 3.

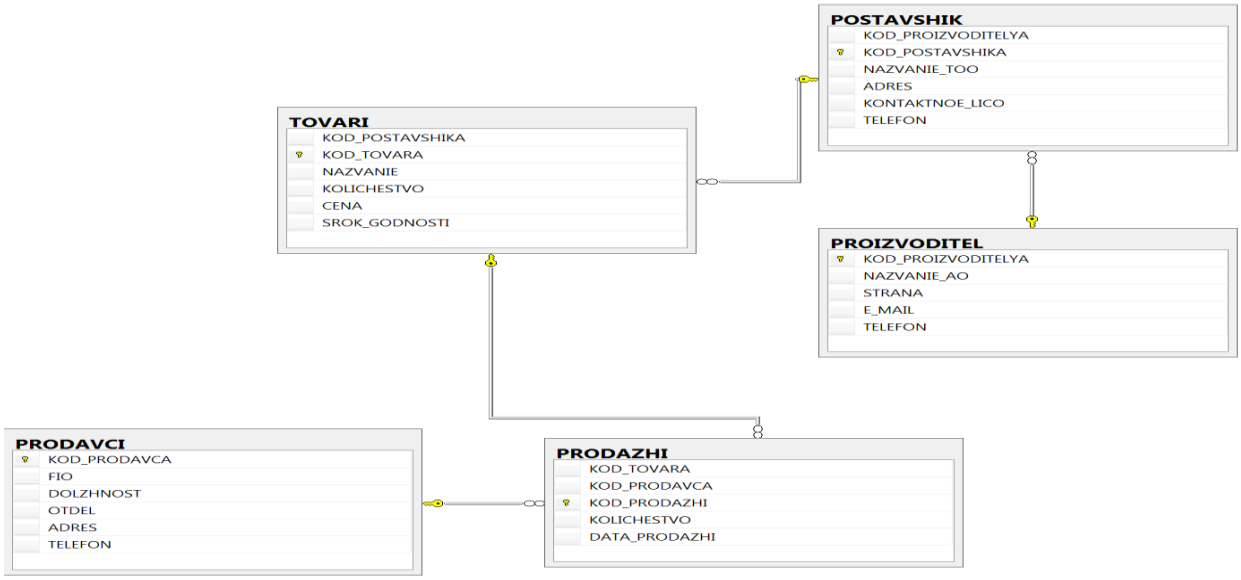


Рисунок 2.6 - Схема БД

Структуры таблиц Proizvoditrel, Postavshik, Tovari, Prodavci, Prodazhi приведены на рисунках 2.7-2.11.

ADIL-ПК\ADIL.MA...dbo.PROIZVODITEL | ADIL-ПК\ADIL.MA...N - dbo.PRODAZHI | ADIL-ПК\ADIL.MA...

Имя столбца	Тип данных	Разрешить значения...
KOD_PROIZVODITELYA	int	☐
NAZVANIE_AO	varchar(20)	☑
STRANA	varchar(20)	☑
E_MAIL	varchar(20)	☑
TELEFON	int	☑
		☐

Рисунок 2.7 - Структура таблицы Proizvoditel

ADIL-ПК\ADIL.MA...- dbo.POSTAVSHIK

Имя столбца	Тип данных	Разрешить значения...
KOD_PROIZVODITELYA	int	☑
KOD_POSTAVSHIKA	int	☐
NAZVANIE_TOO	varchar(20)	☑
ADRES	varchar(20)	☑
KONTAKTNOE_LICO	varchar(20)	☑
TELEFON	int	☑
		☐

Рисунок 2.8 - Структура таблицы Postavshik

ADIL-ПК\ADIL.MAGAZIN - dbo.TOVARI | ADIL-ПК\ADIL.MA...dbo.PROIZVODITEL | ADIL-ПК\ADIL.MA...

Имя столбца	Тип данных	Разрешить значения...
KOD_POSTAVSHIKA	int	☑
KOD_TOVARA	int	☐
NAZVANIE	varchar(20)	☑
KOLICHESTVO	int	☑
CENA	int	☑
SROK_GODNOSTI	datetime	☑

Рисунок 2.9 - Структура таблицы Tovari

ADIL-ПК\ADIL.MA...N - dbo.PRODAVCI | ADIL-ПК\ADIL.MA...- dbo.POSTAVSHIK

Имя столбца	Тип данных	Разрешить значения...
KOD_PRODAVCA	int	☐
FIO	varchar(20)	☑
DOLZHNOST	varchar(20)	☑
OTDEL	varchar(20)	☑
ADRES	varchar(20)	☑
TELEFON	int	☑
		☐

Рисунок 2.10 - Структура таблицы Prodavci

ADIL-ПК\ADIL.MA...N - dbo.PRODAZHI | ADIL-ПК\ADIL.MA...N - dbo.PRODAVCI | ADIL-ПК\ADIL.MA...-

Имя столбца	Тип данных	Разрешить значения...
KOD_TOVARA	int	☑
KOD_PRODAVCA	int	☑
KOD_PRODAZHI	int	☐
KOLICHESTVO	int	☑
DATA_PRODAZHI	datetime	☑
		☐

Рисунок 2.11 - Структура таблицы Prodazhi

Структуры таблиц Proizvoditrel, Postavshik, Tovari, Prodavci, Prodazhi с их свойствами приведены в Приложении Б на листе 3.

3 Организация мониторинга и аудита базы данных

3.1 SQL Server Audit

SQL Server даёт возможность производить аудит пользовательской активности на уровне сервера. SQL Audit довольно мощный инструмент, который позволяет держать под контролем действия пользователей или же разработчиков.

Для начала создается аудит и его базовая настройка. Создание аудита с именем Audit 20210329-184340 и его базовая настройка приведены на рисунке 3.1. Журнал аудита сохраняется в файле в папке Audit на диске C (C:\Audit) и отображается в браузере объектов в папке Аудиты папки Безопасность сервера.

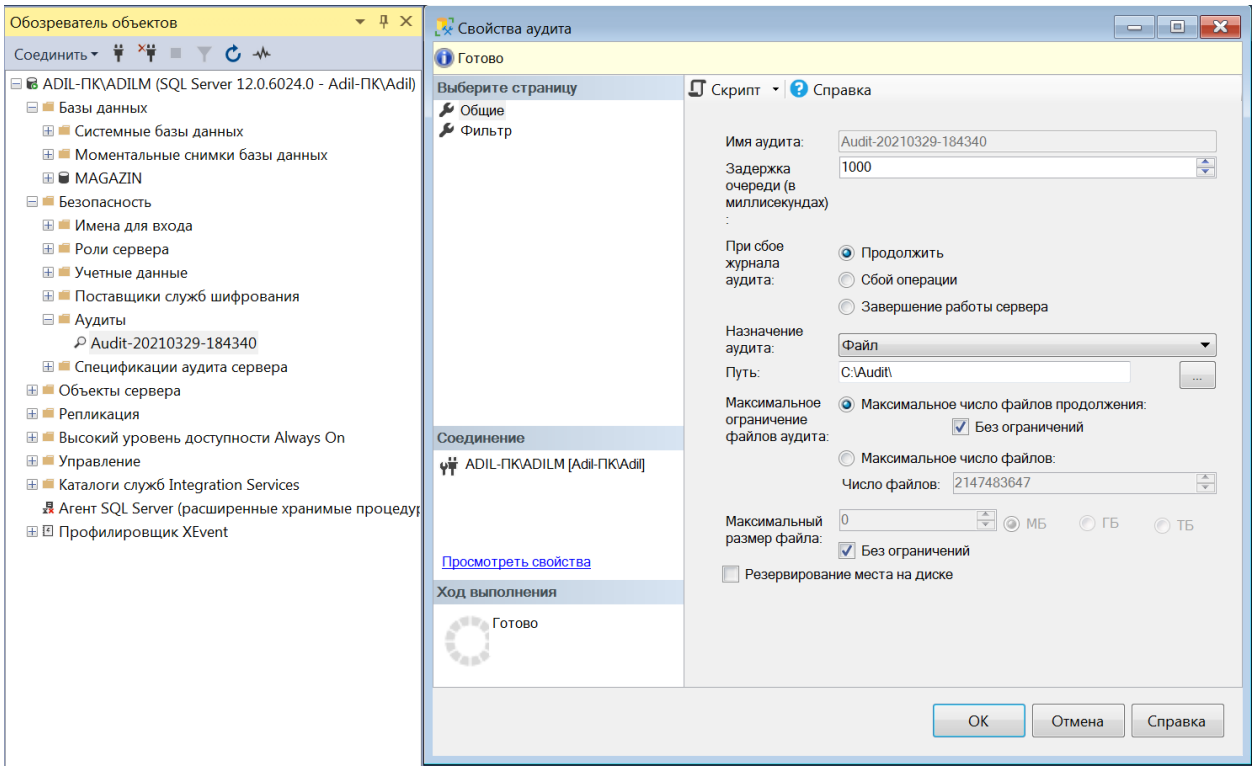


Рисунок 3.1 - Создание аудита и базовая настройка

После создания аудита создается Спецификация Аудита для указания мероприятий или же событий, которые будут отслеживаться на уровне базы данных. Были выбраны типы действий и объекты аудита. Типы действий такие как: Delete, Insert, Select, Update. Объектом аудита выбрана таблица Postavshik. Создание спецификации аудита изображено на рисунке 3.2.

Спецификация Аудита создается в папке Безопасность конкретной БД MAGAZIN для созданного аудита Audit 20210329-184340. Предварительно, перед началом аудита, сам аудит на уровне сервера и его спецификации на уровне базы данных должны быть включены. Включение аудита на уровне сервера показано на рисунке 3.3.

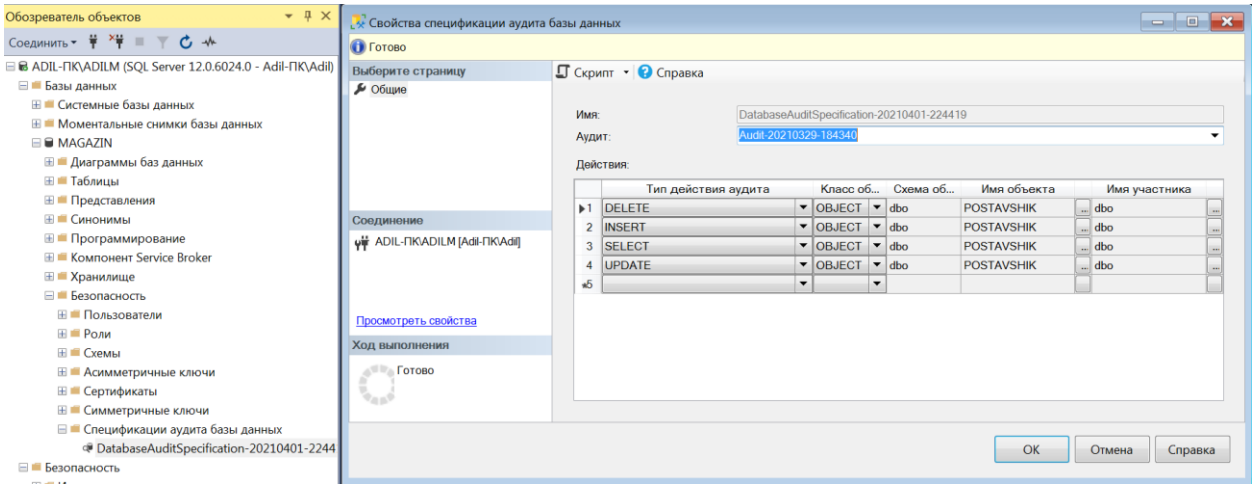


Рисунок 3.2 - Создание спецификации аудита

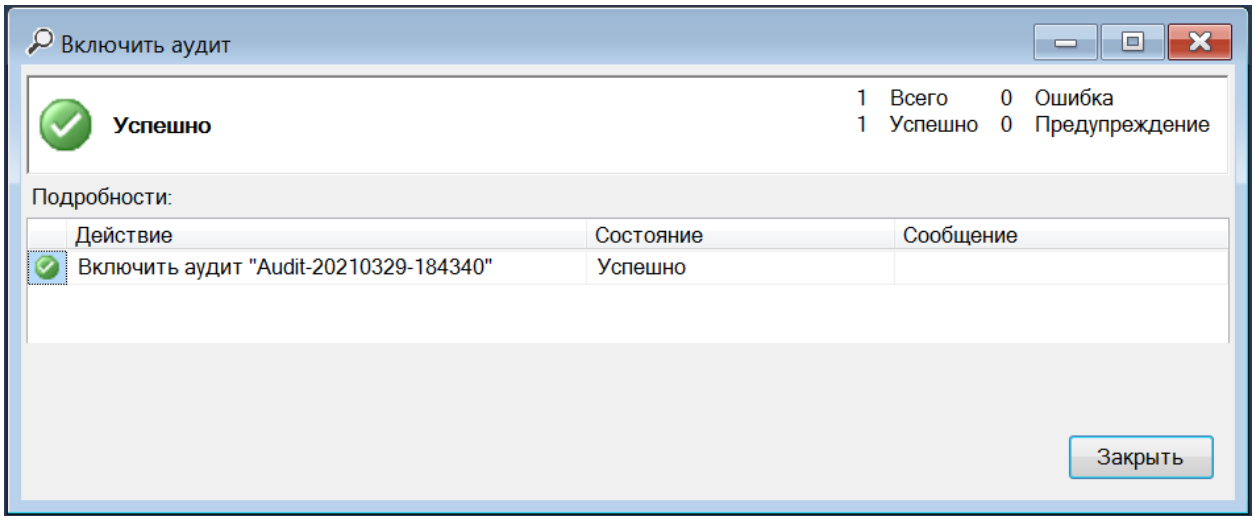


Рисунок 3.3 - Включение аудита на уровне сервера

Включение спецификации аудита на уровне базы данных показано на рисунке 3.4.

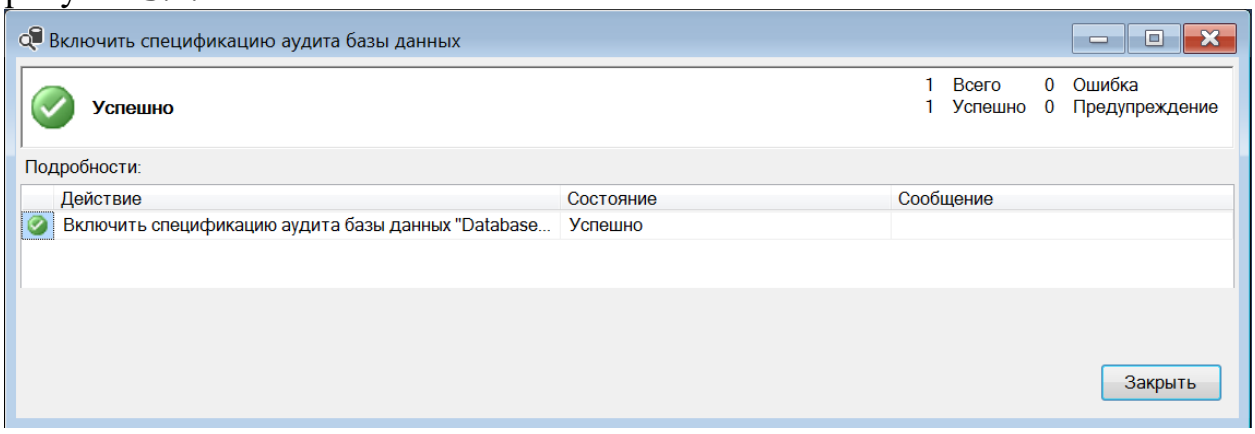


Рисунок 3.4 – Включение аудита на уровне базы данных

После включения аудита можно выполнять непосредственно аудит действий в объекте аудита, определенных в спецификации аудита.
На рисунке 3.5 показаны SQL скрипты выполнения вставки строк, изменения значений, удаления строк и чтения данных в таблице Postavshik.

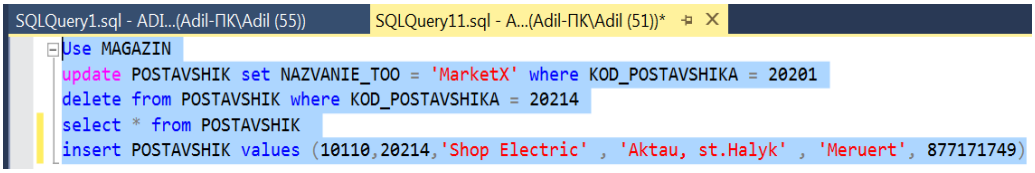
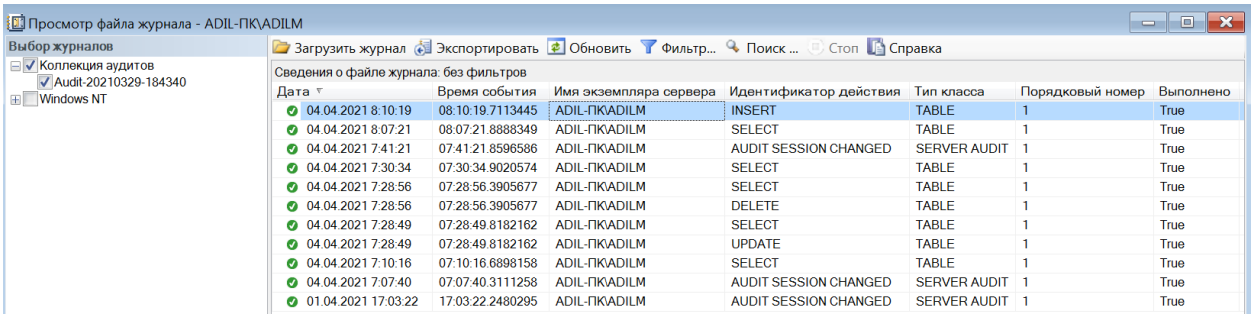


Рисунок 3.5 - Выполненные скрипты

Выполняемые действия регистрируются в журнале аудита, что можно проверить, открыв журнал аудита. Для этого используется команда меню Просмотреть Журнал контекстно-зависимого меню созданного аудита Audit 20210329-184340. Результаты аудита показаны на рисунке 3.6.

В результатах аудита показана: Дата, Время события, Имя экземпляра сервера, Идентификатор действия, Тип класса, Порядковый номер, Выполнение, Имя базы данных, Имя схемы, Имя объекта (Имя таблицы в базе данных), Инструкции (Команды которые были выполнены), Имя файла (Где хранится сам аудит), Источник журнала (Название аудита).



Дата	Время события	Имя экземпляра сервера	Идентификатор действия	Тип класса	Порядковый номер	Выполнено
04.04.2021 8:10:19	08:10:19.7113445	ADIL-ПК\ADILM	INSERT	TABLE	1	True
04.04.2021 8:07:21	08:07:21.8888349	ADIL-ПК\ADILM	SELECT	TABLE	1	True
04.04.2021 7:41:21	07:41:21.8596586	ADIL-ПК\ADILM	AUDIT SESSION CHANGED	SERVER AUDIT	1	True
04.04.2021 7:30:34	07:30:34.9020574	ADIL-ПК\ADILM	SELECT	TABLE	1	True
04.04.2021 7:28:56	07:28:56.3905677	ADIL-ПК\ADILM	SELECT	TABLE	1	True
04.04.2021 7:28:56	07:28:56.3905677	ADIL-ПК\ADILM	DELETE	TABLE	1	True
04.04.2021 7:28:49	07:28:49.8182162	ADIL-ПК\ADILM	SELECT	TABLE	1	True
04.04.2021 7:28:49	07:28:49.8182162	ADIL-ПК\ADILM	UPDATE	TABLE	1	True
04.04.2021 7:10:16	07:10:16.6898158	ADIL-ПК\ADILM	SELECT	TABLE	1	True
04.04.2021 7:07:40	07:07:40.3111258	ADIL-ПК\ADILM	AUDIT SESSION CHANGED	SERVER AUDIT	1	True
01.04.2021 17:03:22	17:03:22.2480295	ADIL-ПК\ADILM	AUDIT SESSION CHANGED	SERVER AUDIT	1	True

Рисунок 3.6 - Результаты аудита

3.2 Создание шаблонов трассировки SQL Server Profiler

Главным понятием SQL Profiler, от которого находятся в зависимости данные для трассировки событий, считаются шаблоны. Шаблон - это сохраненные в особом файле, с расширением tdf, опции сеанса трассировки. Работа с шаблонами (добавление новых, изменение существующих, импорт и экспорт отчетов в иные каталоги) выполняется при помощи меню Файл/Шаблоны в SQL Profiler.

Существуют стандартные встроенные шаблоны в SQL Server:

-SQLProfilerSP_Counts. Сведения о числе произведенных хранимых процедур. Итоги группируются по имени и содержат число запусков каждой процедуры;

-SQLProfilerStandart. Общая информация о произведённых SQL-пакетах и хранимых процедурах, а также об открытых ими подключениях. Итоги выводятся в порядке выполнения процедур и пакетов;

-SQLProfilerTSQL_Duration. Сведения о сгенерированных операторах TSQL. Итоги группируются по длительности выполнения;

-SQLProfilerTSQL_Grouped. Сведения о сгенерированных операторах TSQL. Итоги группируются по пользователям, выполнявшим эти операторы;

-SQLProfilerTSQL_Replay Сведения о сгенерированных операторах TSQL, которые затем возможно воспроизвести;

-SQLProfilerTSQL_SPs. Подробную информацию о всех выполняемых хранимых процедурах в порядке их выполнения, включая команды TSQL каждой процедуры;

-SQLProfilerTuning. Сведения о всех выполненных хранимых процедурах и SQL-пакетах, включая длительность выполнения и двоичные данные. Двоичные данные включают параметры уровня сеанса, тип используемого курсора и тип блокировки [9].

При необходимости можно создать собственный шаблон трассировки. В определение шаблона можно включить любое количество отслеживаемых событий. Все события сгруппированы по категориям, что облегчает выбор нужных при создании шаблона.

Категории событий:

-Cursors (курсоры). Набор событий, связанных с операциями над курсорами;

-Database (база данных). Набор событий, связанных с динамическим изменением размера БД или ее журнала;

-Error and Warnings (ошибки и предупреждения). Набор событий, которые создаются при возникновении ошибки или предупреждения как самим сервером, так и его компонентами, такими как OLE-db;

-Locks (блокировки). Набор событий, связанных с наложением блокировок на объекты;

-Objects (объекты). Набор событий, связанных с созданием, открытием, закрытием, удалением или уничтожением объектов;

-Performance (производительность). Набор событий, связанных с производительностью сервера: события по отображению плана исполнения индивидуальных команд, использовании параллелизма при выполнении запросов;

-Scans (операция сканирования). Набор событий, создаваемых при сканировании таких объектов БД, как таблицы и индексы;

-Security (разграничение доступа). Обширный набор событий, позволяющих фиксировать работу сервера с точки зрения системы разграничения доступа;

-Session (сессии). Набор событий, создаваемых при исполнении хранимых процедур и связанных с началом и окончанием исполнения процедуры в целом, исполнением индивидуальных команд, входящих в состав процедуры и т.д.;

-Transactions (транзакции). Набор событий, связанных с исполнением транзакций, создаваемых координатором распределенных транзакций сервером. В эту категорию также входят события, создаваемые при записи данных в журнал транзакций;

-TSQL (команды Transact SQL). Набор событий, создаваемых при исполнении команд T-SQL, передаваемых серверу от клиентского приложения;

-User Configurable. В эту группу будет помещен созданный пользователем класс событий, который будет отслеживать утилита профилирования [10].

Для отслеживания событий, связанных с изменением объектов в базе данных и выполнением команд TSQL, был создан шаблон с именем First. На рисунке 3.7 показаны общие свойства шаблона (вкладка Общие).

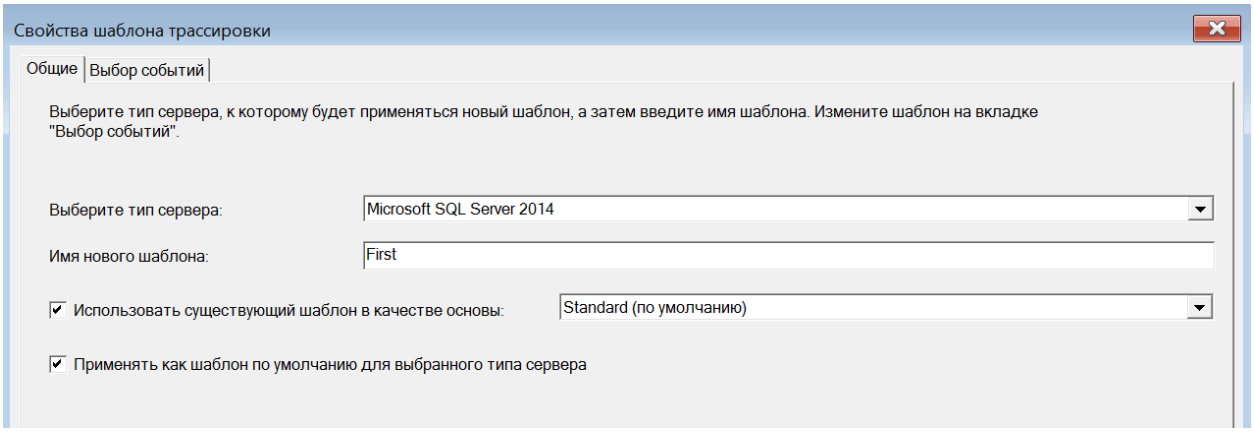


Рисунок 3.7 - Общие свойства шаблона

На рисунке 3.8 показаны события категорий Object и TSQL, включенные в шаблон First (вкладка Выбор событий).

Событие Object в шаблоне будет отслеживать создание, изменение, а также удаление объектов в базе данных.

Событие TSQL в шаблоне отслеживает запуск и завершение выполнения пакета команд TSQL в SQL Server.

На основе этого шаблона в дальнейшем можно создавать файлы трассировки без изменения выбранных событий Object и TSQL или с изменениями указанных событий.

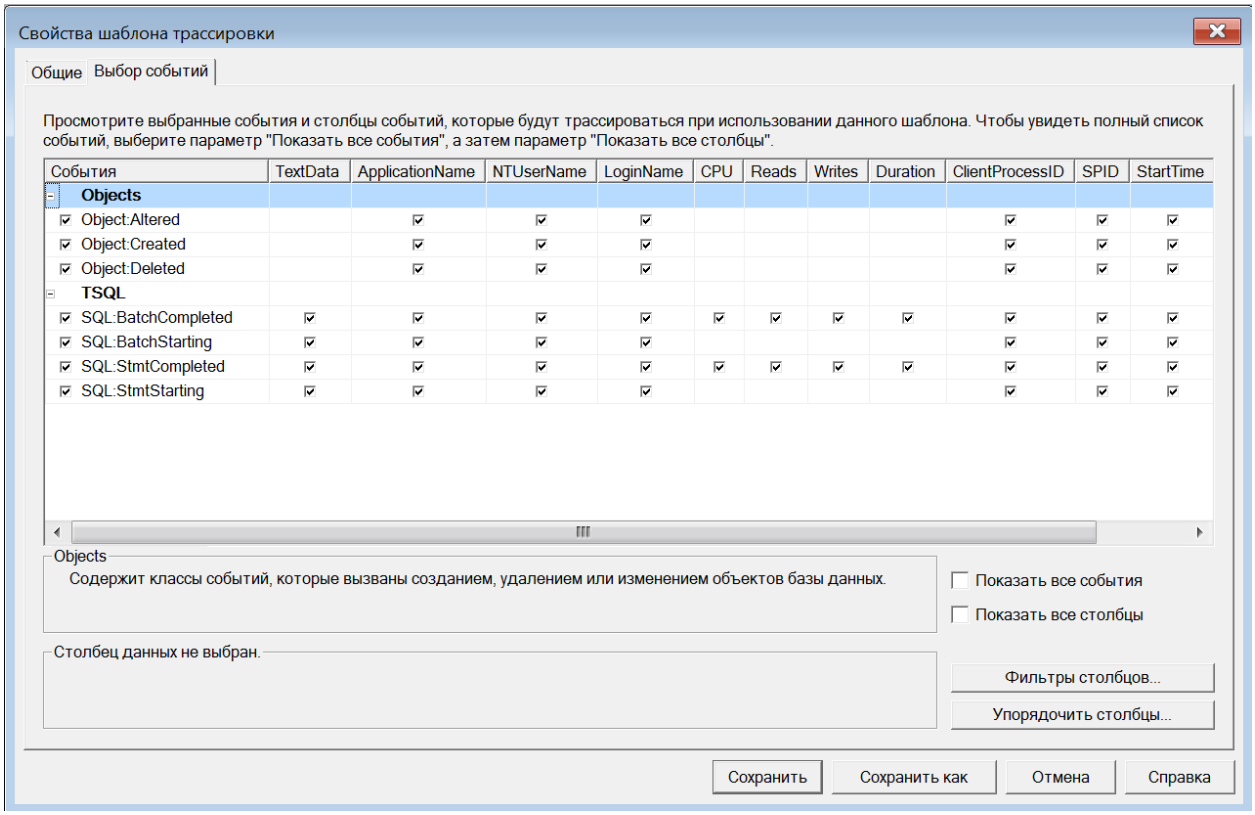


Рисунок 3.8 – События Object и TSQL шаблона First

3.3 Создание файла трассировки SQL Server Profiler

Трассировка, это действие, которое происходит в фоновом режиме в SQL Server. При выполнении трассировки происходит перехватывание конкретных происходящих событий и данных, связанных с этими событиями. Данная информация является очень важной для диагностики задач с производительностью, позволяя обнаруживать тупики, падение производительности и выполнять аудит по информационной безопасности.

На рисунке 3.9 представлена вкладка Общие окна Свойства трассировки, на которой показано создание файла трассировки TraceAdil.trc. Задаются общие свойства для файла трассировки, указывается имя трассировки TraceAdil, шаблон трассировки First, который был создан ранее.

Указание шаблона трассировки при создании файла трассировки определяет также и события, которые будут отслеживаться, так как в шаблоне трассировки они были определены. При необходимости можно изменить перечень событий в отслеживаемых категориях событий, используя вкладку Выбор события окна Свойства трассировки.

На рисунке 3.10 представлена вкладка Выбор события окна Свойства трассировки, на которой показаны события файла трассировки. Перечень событий категорий Object и TSQL, основанный на выбранном шаблоне трассировки First был оставлен без изменения.

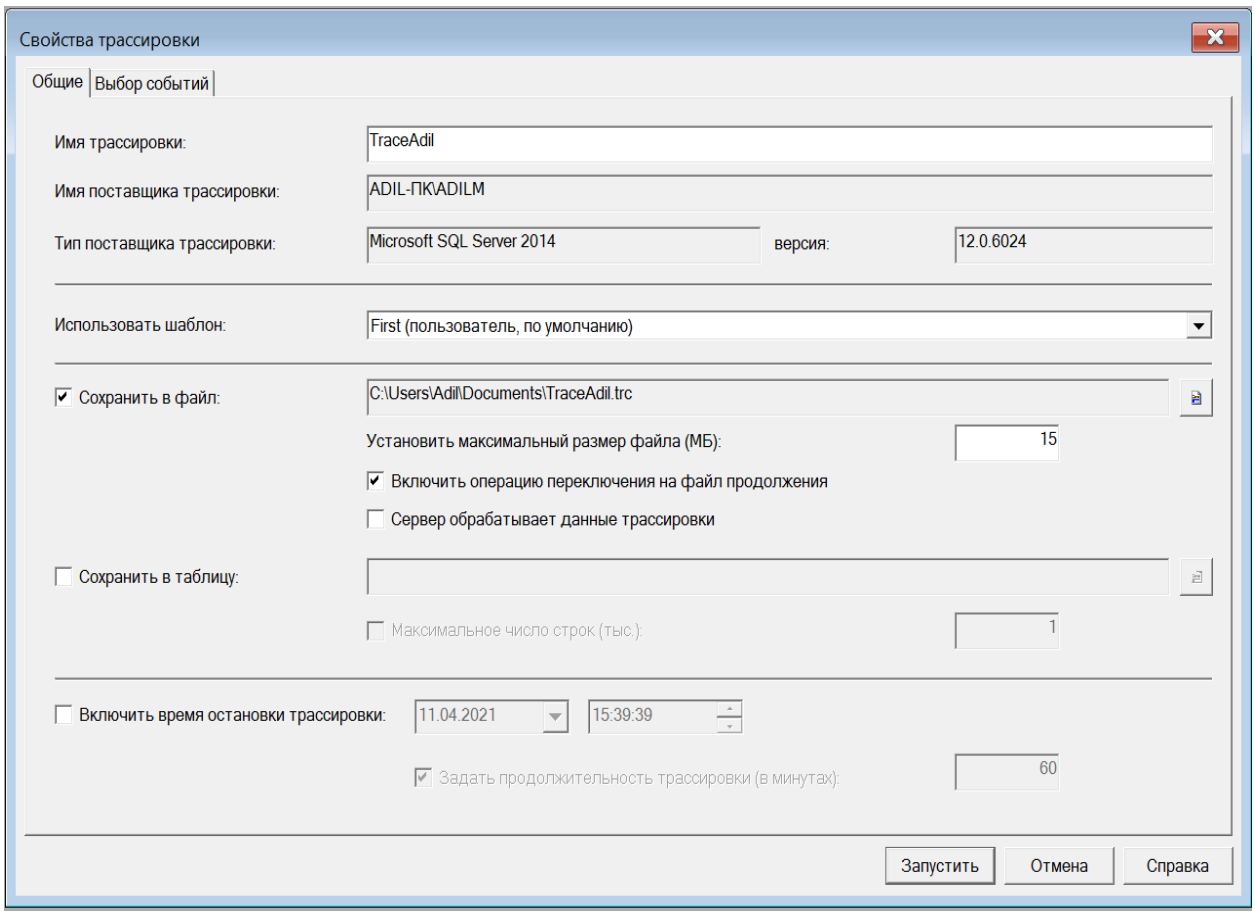


Рисунок 3.9 - Общие параметры создания файла трассировки

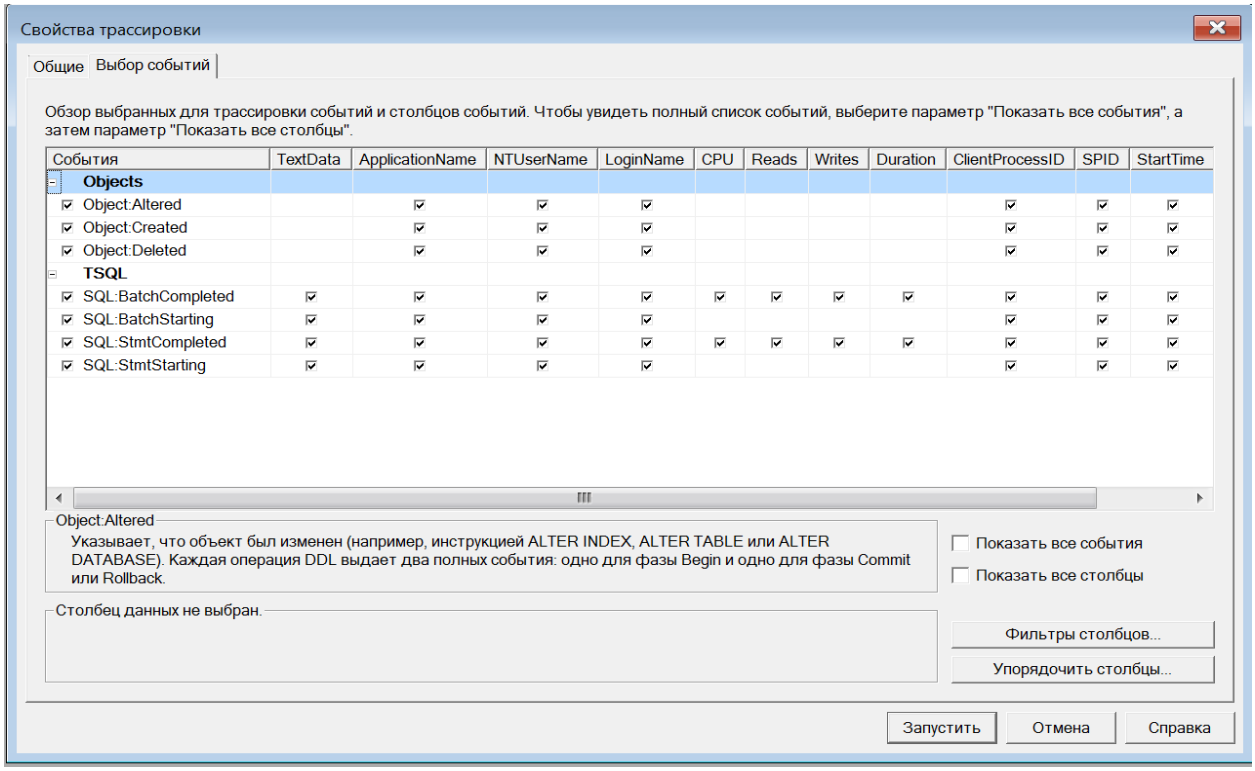


Рисунок 3.10 - События файла трассировки

При создании файла трассировки имеется возможность выбора фиксируемых параметров отслеживаемых событий и задания имени приложения (Application Name), которое будет являться инициатором отслеживаемых событий. Для этого используется кнопка Фильтры столбцов вкладки Выбор события окна Свойства трассировки.

На рисунке 3.11 показаны фильтры столбцов с изменением фильтра Application Name, так как для тестирования файлов трассировки будет использоваться приложение SQL Server Management Studio (имя приложения было вписано в фильтр).

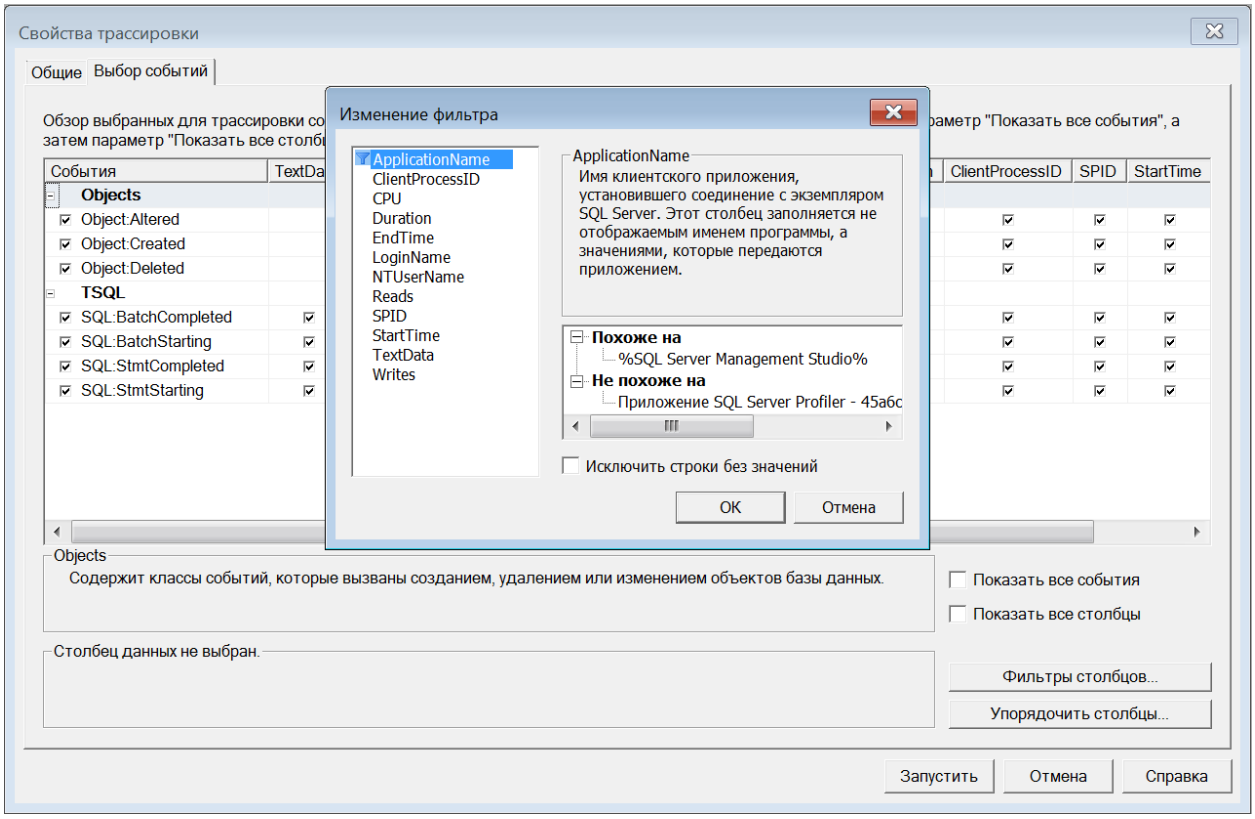


Рисунок 3.11 - Фильтр столбцов

Для запуска файла трассировки используется кнопка Запустить, которая находится на вкладке Выбор события окна Свойства трассировки. На рисунке 3.12 показано содержимое созданного и запущенного файла трассировки TraceAdil.trc, в котором зафиксированы отслеживаемые события для мониторинга и аудита базы данных.

В файле трассировки TraceAdil.trc зафиксированы события, инициированные командой Select * from Postavchik. В столбце Application Name (рисунок 3.12) фиксируется имя приложения SQL Server Management Studio, откуда поступила команда, события которой зарегистрированы в файле трассировки.

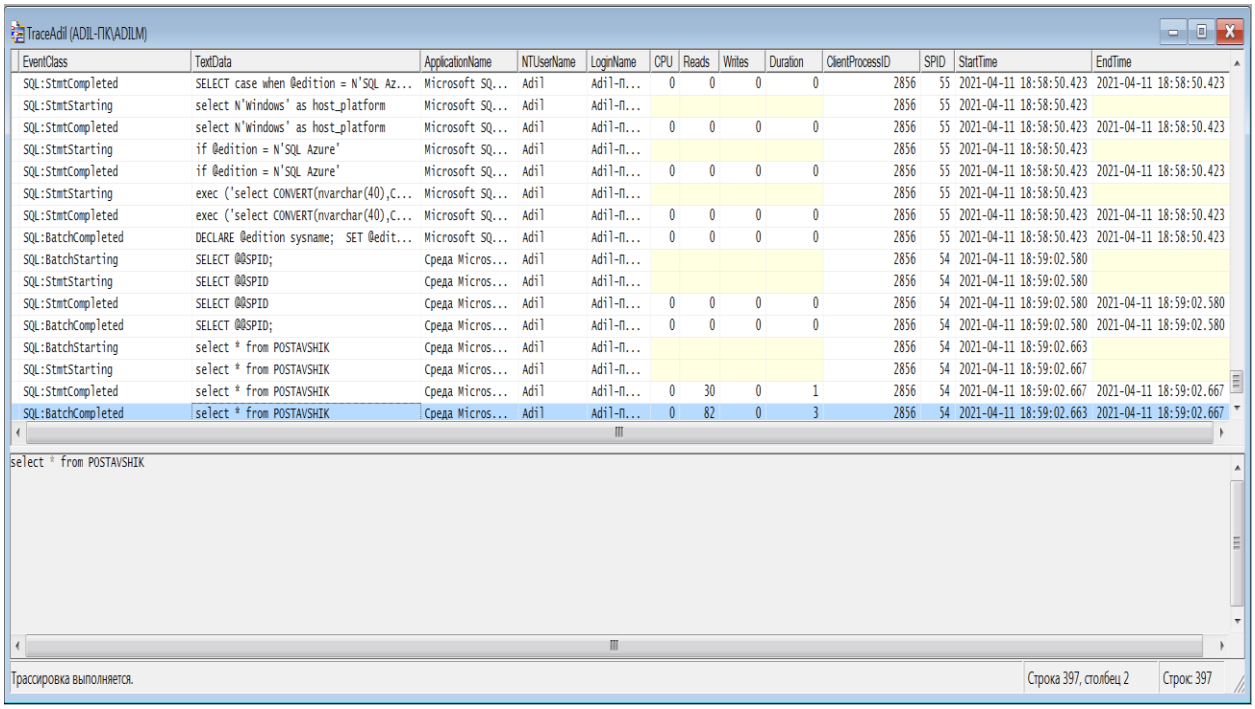


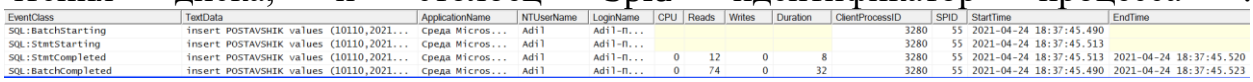
Рисунок 3.12 - Файл трассировки

3.4 Анализ журнала трассировки

Анализ журнала трассировки это поиск медлительных команд и операций, которые происходят в SQL Server. На рисунке 2.23 показан результат трассировки в котором показаны такие столбцы как:

- EventClass (события которые будет проверять и мониторить SQL Profiler);
- TextData (какая команда или же операция была выполнена);
- ApplicationName (приложение или же среда где была выполнена та или иная команда);
- NTUserName (имя пользователя Windows);
- LoginName (имя пользователя SQL Server) ;
- CPU (время центрального процессора в мили секундах);
- Reads (число логических чтений диска);
- Writes (число операций);
- Duration (количество времени в мили секундах использованного событием);
- ClientProcessID (идентификатор процесса);
- SPID (идентификатор серверного процесса);
- StartTime (дата и время начало процесса или же команды);
- EndTime (дата и время конца процесса или же команды).

На Рисунке 3.13 показана операция. Изображены события Bath и Stmt. Событие Stmt показывает более точную информацию по операциям чем Bath. Была выполнена команда Insert POSTAVSHIK values (10110, 20214, 'Shop Electric','Aktau, st.Halyk' 'Meruert', 877171749) В разделе CPU видим что операция не нагружает процессор, в столбце Duration показано время в мили секундах на выполнение события , а так же столбец Reads число логического чтения диска, и столбец Spid идентификатор процесса .



EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration	ClientProcessID	SPID	StartTime	EndTime
SQL:BatchStarting	insert POSTAVSHIK values (10110,2021...	Среда Micros...	Adil	Adil-n...					3280	55	2021-04-24 18:37:45.490	
SQL:StmtStarting	insert POSTAVSHIK values (10110,2021...	Среда Micros...	Adil	Adil-n...					3280	55	2021-04-24 18:37:45.513	
SQL:StmtCompleted	insert POSTAVSHIK values (10110,2021...	Среда Micros...	Adil	Adil-n...	0	12	0	8	3280	55	2021-04-24 18:37:45.513	2021-04-24 18:37:45.520
SQL:BatchCompleted	insert POSTAVSHIK values (10110,2021...	Среда Micros...	Adil	Adil-n...	0	74	0	32	3280	55	2021-04-24 18:37:45.490	2021-04-24 18:37:45.523

Рисунок 3.13 - Операция событий Bath и Stmt

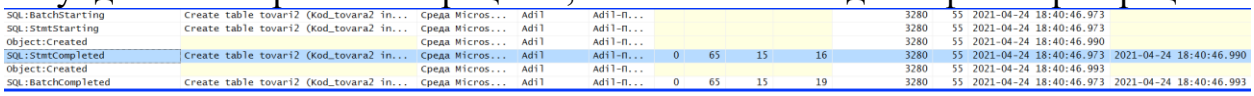
На Рисунке 3.14 показана операция на событие Object. Событие Object распространяется на команды:

- Create;

- Delete;

- Alter.

Была выполнена команда Create table tovari2 (Kod_tovara2 int, nazvanie2 varchar(20)). На рисунке 3.14 видим время запуска и конца процесса, класс событий, команду которая была выполнена, среда или же приложение где была выполнена команда, имя пользователя, в разделе CPU видим значение 0 то есть, операция не нагружает процессор, 65 логических чтений диска, было выполнено 15 операции до конца процесса, событие использовала 16 и 19 мили секунд на завершение процесса, а так же идентификатор процесса.



SQL:BatchStarting	Create table tovari2 (Kod_tovara2 in...	Среда Micros...	Adil	Adil-n...					3280	55	2021-04-24 18:40:46.973	
SQL:StmtStarting	Create table tovari2 (Kod_tovara2 in...	Среда Micros...	Adil	Adil-n...					3280	55	2021-04-24 18:40:46.973	
Object:Created		Среда Micros...	Adil	Adil-n...					3280	55	2021-04-24 18:40:46.990	
SQL:StmtCompleted	Create table tovari2 (Kod_tovara2 in...	Среда Micros...	Adil	Adil-n...	0	65	15	16	3280	55	2021-04-24 18:40:46.973	2021-04-24 18:40:46.990
Object:Created		Среда Micros...	Adil	Adil-n...					3280	55	2021-04-24 18:40:46.993	
SQL:BatchCompleted	Create table tovari2 (Kod_tovara2 in...	Среда Micros...	Adil	Adil-n...	0	65	15	19	3280	55	2021-04-24 18:40:46.973	2021-04-24 18:40:46.993

Рисунок 3.14 - Событие Object

ЗАКЛЮЧЕНИЕ

Данная работа посвящена мониторингу и аудиту MS SQL Server. Обеспечить безопасность можно лишь создав комплекс механизмов защиты. Рассмотрены средства безопасности в серверах баз данных: ограничения целостности, SQL Audit, SQL Profiler.

В результате выполнения работы была создана БД предметной области Магазин. Проанализирована предметная область, определены сущности, атрибуты и связи между ними. Были спроектированы инфологическая и даталогическая модели базы данных в CASE-средстве AllFusion Erwin Data Modeler (Erwin). Для обеспечения характеристики информационной безопасности, как целостность базы данных, в физической модели созданы ограничения целостности, такие как, значения по умолчанию, допустимость пустого значения, первичные и внешние ключи, что предотвращает внесение случайных ошибок.

Была проведена генерация SQL скриптов для реализации баз данных в СУБД MS SQL Server. База Данных была создана в MS SQL Server.

Был создан Аудит и спецификация аудита для отслеживания определенных событий и действий.

В работе был создан шаблон трассировки а так же файл трассировки SQL Server Profiler. Были рассмотрены все шаблоны трассировки, а так же все категории событий. В созданном файле трассировки рассмотрены все выборы фиксируемых параметров отслеживаемых событий.

В ходе дипломного проекта были изучены механизмы и утилиты Мониторинга и Аудита MS SQL Server.

При организации мониторинга и аудита следует учесть, что при этом потребуются дополнительные ресурсы. Поэтому нужно выполнять аудит и детальный мониторинг только тех операций и объектов, информация о которых действительно необходима.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Введение в MS SQL Server // Электронная версия на сайте https://metanit.com/sql/sqlserver/1.1.php
2. Мониторинг в MS SQL Server // Электронная версия на сайте https://aggregate.digital/ru/products/network-manager/database-monitoring/sql-server-monitoring.html
3. Аудит в MS SQL Server // Электронная версия на сайте //https://studbooks.net/2090919/informatika/podsistema_audita_server
4. Механизмы и утилиты Мониторинга и Аудита MS SQL Server // Электронная версия на сайте http://www.t-sql.ru/post/audit.aspx
5. Туриканов Т.С., Айтхожаева Е.Ж. Организация Аудита и Мониторинг в MS SQL Server «Роль и место молодых ученых в реализации новой экономической политики Казахстана» Международных Сатпаевских Чтений Том 4 2015. - Алматы: КазНИТУ
6. ERWIN // Электронная версия на сайте https://www.kpms.ru/Automatization/ERwin.htm
7. Создание Баз Данных с помощью пакета ERWIN // Электронная версия на сайте http://www.pl63.edu.ru/images/doc/study/INF/method/m_erWin.pdf
8. Логическая и Физическая модель данных в ERWIN // Электронная версия на сайте https://studref.com/382616/informatika/logicheskaya_fizicheskaya_modeli_erwin_data_modeler
9. Шаблон трассировк // Электронная версия на сайте http://www.askit.ru/custom/sql2005_admin/m11/11_02_03_profiler.htm
10. Руководство по категориям событий SQL Server Profiler // Электронная версия на сайте https://docs.microsoft.com/ru-ru/sql/relational-databases/event-classes/sql-server-event-class-reference?view=sql-server-ver15

Приложение А

```
CREATE DEFAULT Default_Value_261
	AS GETDATE()
go


CREATE RULE Validation_Rule_259
	AS @col BETWEEN 1 AND 10000
go


CREATE RULE Validation_Rule_263
	AS @col IN ('MLADSHI_PRODAVEC', 'PRODAVEC',
'STARSHI_PRODAVEC')
go


CREATE TABLE POSTAVSHIK
(
	KOD_PROIZVODITELYA   integer  NULL ,
	KOD_POSTAVSHIKA      integer  NOT NULL ,
	NAZVANIE_TOO         varchar(20)  NULL ,
	ADRES                varchar(20)  NULL ,
	KONTAKTNOE_LICO      varchar(20)  NULL ,
	TELEFON              integer  NULL
)
go


ALTER TABLE POSTAVSHIK
	ADD CONSTRAINT XPKPOSTAVSHIK PRIMARY KEY  CLUSTERED
(KOD_POSTAVSHIKA ASC)
go


CREATE TABLE PRODAVCI
(
	KOD_PRODAVCA         integer  NOT NULL ,
	FIO                  varchar(20)  NULL ,
	DOLZHNOST            varchar(20)  NULL ,
	OTDEL                varchar(20)  NULL ,
	ADRES                varchar(20)  NULL ,
```

```
        TELEFON          integer  NULL
)
go


ALTER TABLE PRODAVCI
        ADD CONSTRAINT XPKPRODAVCI PRIMARY KEY  CLUSTERED
(KOD_PRODAVCA ASC)
go


CREATE TABLE PRODAZHI
(
        KOD_TOVARA          integer  NULL ,
        KOD_PRODAVCA        integer  NULL ,
        KOD_PRODAZHI        integer  NOT NULL ,
        KOLICHESTVO         integer  NULL ,
        DATA_PRODAZHI       datetime  NULL
)
go


ALTER TABLE PRODAZHI
        ADD CONSTRAINT XPKPRODAZHI PRIMARY KEY  CLUSTERED
(KOD_PRODAZHI ASC)
go


CREATE TABLE PROIZVODITEL
(
        KOD_PROIZVODITELYA   integer  NOT NULL ,
        NAZVANIE_AO          varchar(20)  NULL ,
        STRANA               varchar(20)  NULL ,
        E_MAIL               varchar(20)  NULL ,
        TELEFON              integer  NULL
)
go

ALTER TABLE PROIZVODITEL
        ADD CONSTRAINT XPKPROIZVODITEL PRIMARY KEY  CLUS-
TERED (KOD_PROIZVODITELYA ASC)
go


CREATE TABLE TOVARI
```

```
(
        KOD_POSTAVSHIKA      integer  NULL ,
        KOD_TOVARA           integer  NOT NULL ,
        NAZVANIE             varchar(20)  NULL ,
        KOLICHESTVO          integer  NULL ,
        CENA                 integer  NULL ,
        SROK_GODNOSTI        datetime  NULL
)
go


ALTER TABLE TOVARI
        ADD CONSTRAINT XPKTOVARI PRIMARY KEY  CLUSTERED
(KOD_TOVARA ASC)
go

exec sp_bindefault 'Default_Value_261', 'TOVARI.SROK_GODNOSTI'
go

ALTER TABLE POSTAVSHIK
        ADD CONSTRAINT R_1 FOREIGN KEY (KOD_PROIZVODITELYA)
REFERENCES PROIZVODITEL(KOD_PROIZVODITELYA)
                ON DELETE NO ACTION
                ON UPDATE NO ACTION
go

exec sp_bindrule 'Validation_Rule_263', 'PRODAVCI.DOLZHNOST'
go

ALTER TABLE PRODAZHI
        ADD CONSTRAINT R_3 FOREIGN KEY (KOD_TOVARA) REFER-
ENCES TOVARI(KOD_TOVARA)
                ON DELETE NO ACTION
                ON UPDATE NO ACTION
go


ALTER TABLE PRODAZHI
        ADD CONSTRAINT R_4 FOREIGN KEY (KOD_PRODAVCA) REFER-
ENCES PRODAVCI(KOD_PRODAVCA)
                ON DELETE NO ACTION
                ON UPDATE NO ACTION
go
```

```
exec sp_bindrule 'Validation_Rule_259', 'TOVARI.KOLICHESTVO'
go

ALTER TABLE TOVARI
	ADD CONSTRAINT R_2 FOREIGN KEY (KOD_POSTAVSHIKA) REF-
ERENCES POSTAVSHIK(KOD_POSTAVSHIKA)
		ON DELETE NO ACTION
		ON UPDATE NO ACTION
Go
```

Приложение Б

Механизмы мониторинга и аудита в MS SQL Server

SQL Trace. В SQL Trace с помощью системных хранимых процедур создается файл трассировки, в котором регистрируются события, если они являются экземплярами классов событий, перечисленных в определении трассировки при ее создании.

C2 Audit. Режим аудита C2 настраивается с помощью SQL Server Management Studio или же с помощью параметра **режима аудита c2** в **sp_configure**. Выбор этого режима настроит сервер на запись неудачных, и успешных попыток доступа к операторам и объектам.

Триггеры предполагают собой особой тип хранимой процедуры, которая вызывается автоматически при выполнении конкретного действия над объектами, находящимися под управлением сервера БД.

Change Tracking – это отслеживание изменений. Эффективный механизм отслеживания изменений для приложений. Используется, чтобы приложения могли запрашивать изменения данных в базе данных и получать доступ к информации.

Change Data Capture (CDC) представляет собой механизм ограничения влияния на исходные данные при загрузке свежих данных в оперативные хранилища данных и хранилища данных, CDC дополняет инструменты интеграции корпоративной информации.

Perfomance monitor (монитор производительности), используется для настройки производительности. Дает информацию о том, как работает SQL Server, и как работает Windows Server.

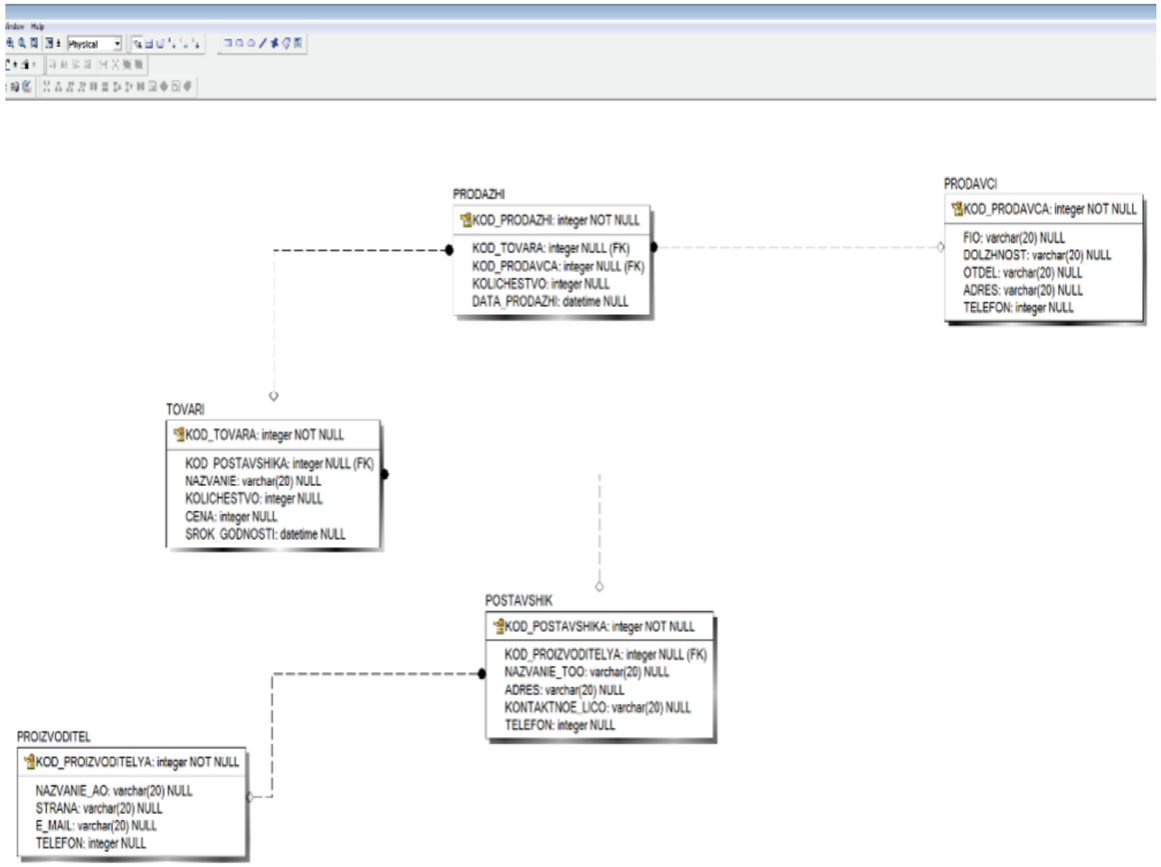
SQL Audit. Аудит среды SQL Server Database Engine или отдельной базы данных включает в себя отслеживание и фиксацию (запись) событий, происходящих в ядре SQL Server - Database Engine. Аудит среды SQL Server разрешает проводить аудит сервера, который имеет возможность подключать в себя спецификации аудита сервера для мероприятий на уровне сервера, а еще спецификации аудита базы данных для мероприятий на уровне базы данных.

SQL Server Profiler отслеживает действия обработки ядра, к примеру, начало пакета или же транзакции, и регистрирует данные о происходящих событиях в таблице SQL Server или же в файле. Этим самым обеспечивая учет (аудит и мониторинг) операций серверов и баз данных.

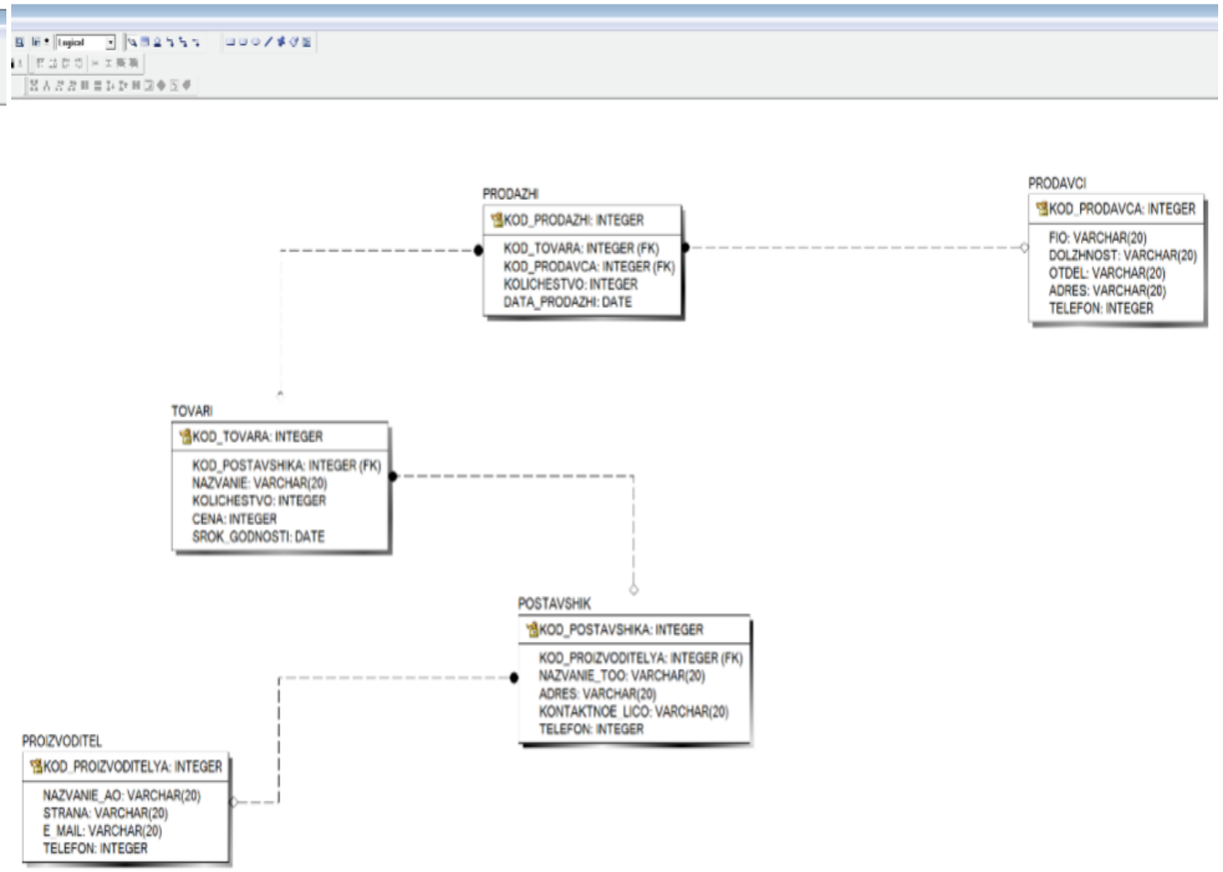
						Дипломный проект	
						Механизмы мониторинга и аудита в MS SQL Server	Лист / Масса / Масштаб
Изм.	Лист	Ф.И.О		Подп.	Дата		
Разраб.		Идришев А.					Лист 1 / Листов 5
Норм.		Кабдуллин М.					
Руков.		Айтхожаева Е				Тема: Организация мониторинга и аудита в MS SQL Server	КазНИТУ ИКиИТ СИБ 5В100200
Зав. каф.		Сейлова Н.					

Приложение Б

Физическая модель данных в Erwin



Логическая модель данных в Erwin



						Дипломный проект
						Лист / Масса / Масштаб
Изм.	Лист	Ф.И.О		Подп.	Дата	
Разраб.		Идришев А.				Логическая и физическая модель данных в Erwin
Норм.		Кабдуллин М.				Лист 2 / Листов 5
Руков.		Айтхожаева Е				
Зав. каф.		Сейлова Н.				Тема: Организация мониторинга и аудита в MS SQL Server
						КазНИТУ ИКиИТ СИБ 5В100200

Приложение Б

Структуры таблиц БД

ADIL-ПК\ADIL.MA...dbo.PROIZVODITEL | ADIL-ПК\ADIL.MA...N - dbo.PRODAZHI | ADIL-ПК\ADIL.MA...

Имя столбца	Тип данных	Разрешить значения...
KOD_PROIZVODITELYA	int	
NAZVANIE_AO	varchar(20)	☑
STRANA	varchar(20)	☑
E_MAIL	varchar(20)	☑
TELEFON	int	☑

ADIL-ПК\ADIL.MA...- dbo.POSTAVSHIK

Имя столбца	Тип данных	Разрешить значения...
KOD_PROIZVODITELYA	int	☑
KOD_POSTAVSHIKA	int	
NAZVANIE_TOO	varchar(20)	☑
ADRES	varchar(20)	☑
KONTAKTNOE_LICO	varchar(20)	☑
TELEFON	int	☑

ADIL-ПК\ADIL.MAGAZIN - dbo.TOVARI | ADIL-ПК\ADIL.MA...dbo.PROIZVODITEL | ADIL-ПК\ADIL.MA...

Имя столбца	Тип данных	Разрешить значения...
KOD_POSTAVSHIKA	int	☑
KOD_TOVARA	int	
NAZVANIE	varchar(20)	☑
KOLICHESTVO	int	☑
CENA	int	☑
SROK_GODNOSTI	datetime	☑

ADIL-ПК\ADIL.MA...N - dbo.PRODAVCI | ADIL-ПК\ADIL.MA...- dbo.POSTAVSHIK

Имя столбца	Тип данных	Разрешить значения...
KOD_PRODAVCA	int	
FIO	varchar(20)	☑
DOLZHNOST	varchar(20)	☑
OTDEL	varchar(20)	☑
ADRES	varchar(20)	☑
TELEFON	int	☑

ADIL-ПК\ADIL.MA...N - dbo.PRODAZHI | ADIL-ПК\ADIL.MA...N - dbo.PRODAVCI | ADIL-ПК\ADIL.MA...-

Имя столбца	Тип данных	Разрешить значения...
KOD_TOVARA	int	☑
KOD_PRODAVCA	int	☑
KOD_PRODAZHI	int	
KOLICHESTVO	int	☑
DATA_PRODAZHI	datetime	☑

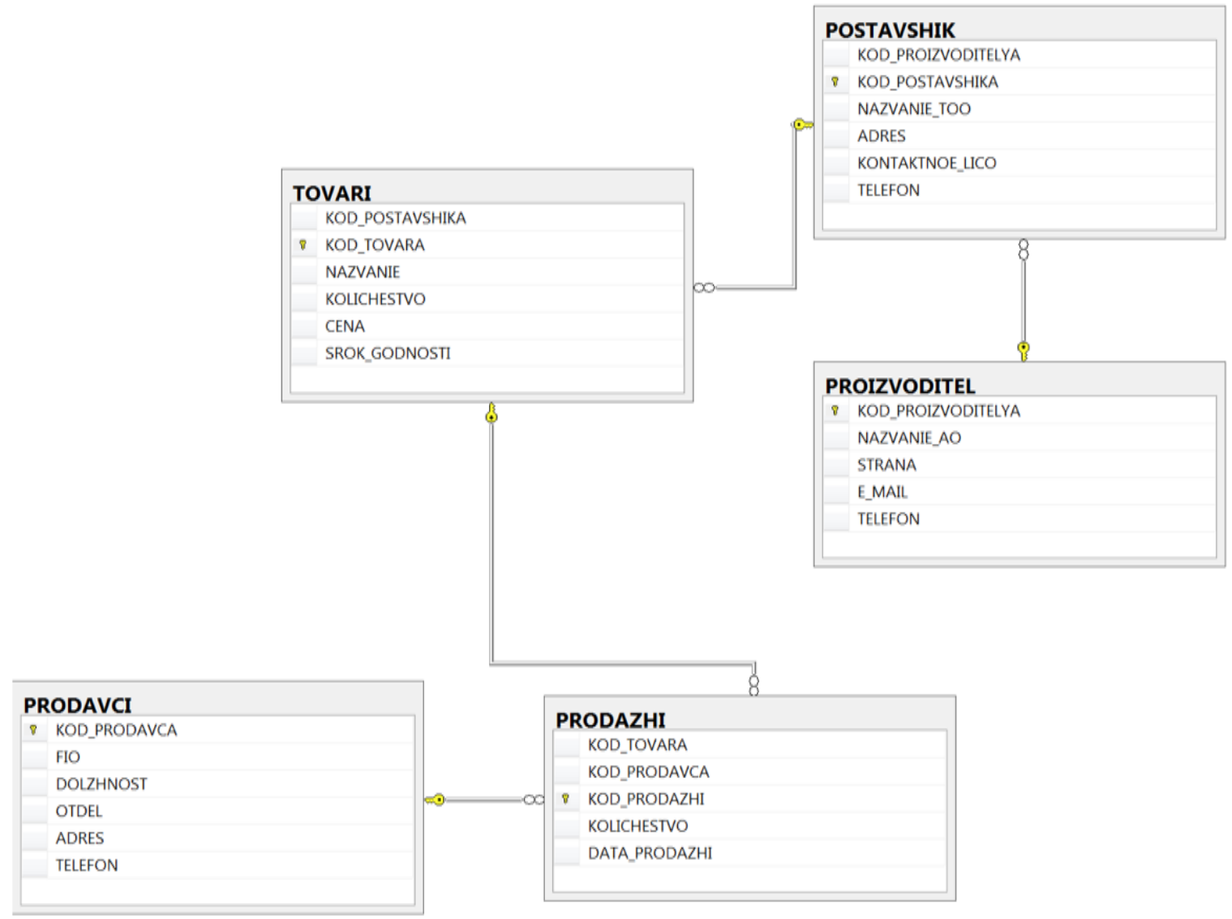


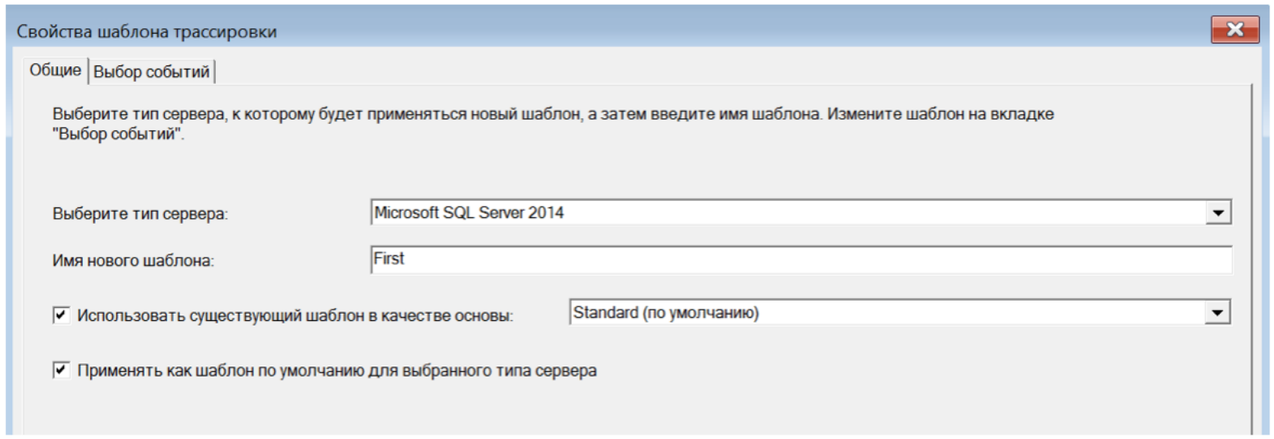
Схема базы данных в MS SQL Server

						Дипломный проект
Изм.	Лист	Ф.И.О		Подп.	Дата	
Разраб.		Идришев А.				Структура таблиц и схема базы данных в MS SQL Server
Норм.		Кабдуллин М.				
Руков.		Айтхожаева Е				
Зав. каф.		Сейлова Н.				Тема: Организация мониторинга и аудита в MS SQL Server

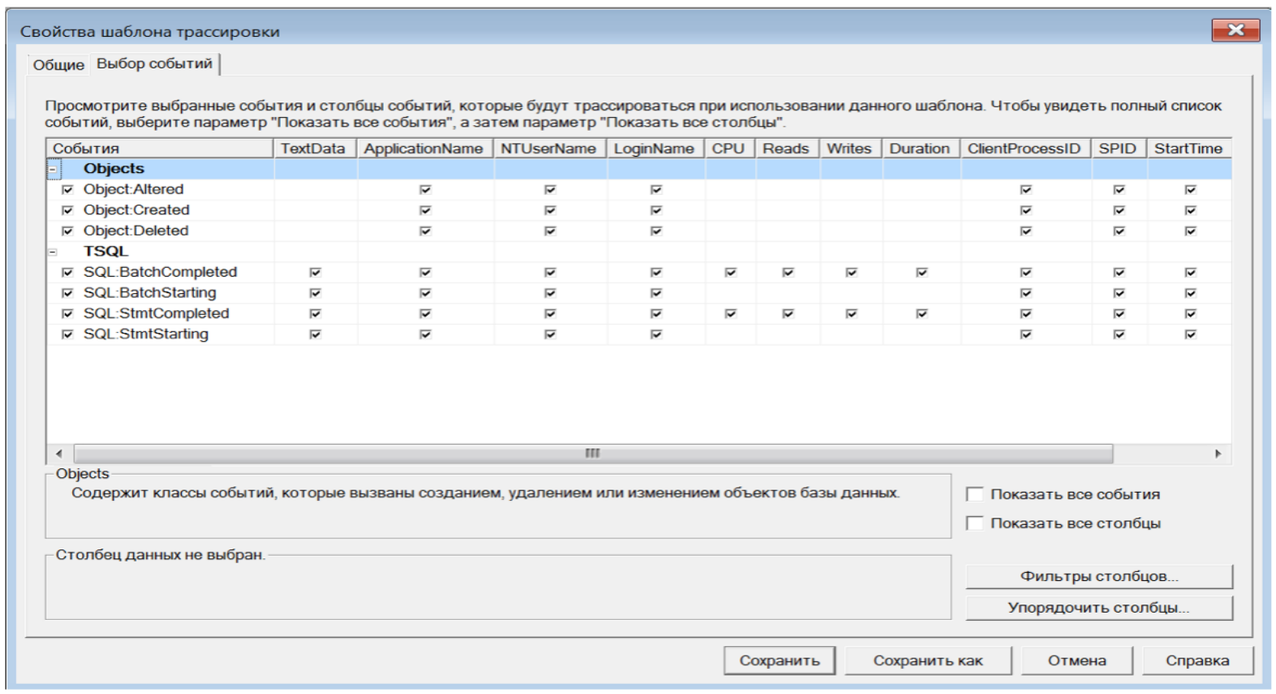
Лист	Масса	Масштаб
Лист 3	Листов 5	

КазНИТУ
ИКиИТ
СИБ
5В100200

Приложение Б



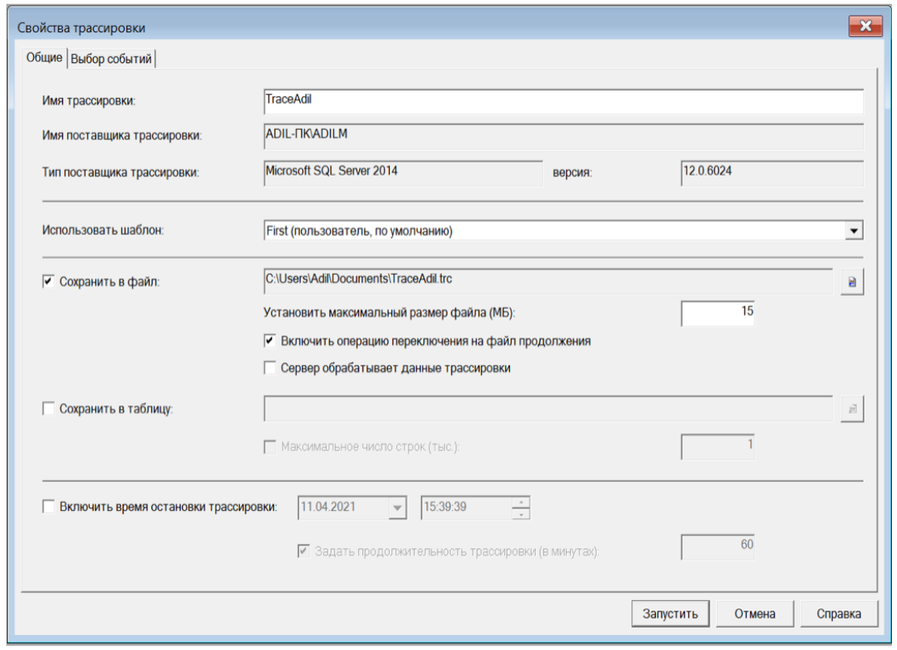
Общие свойства шаблона



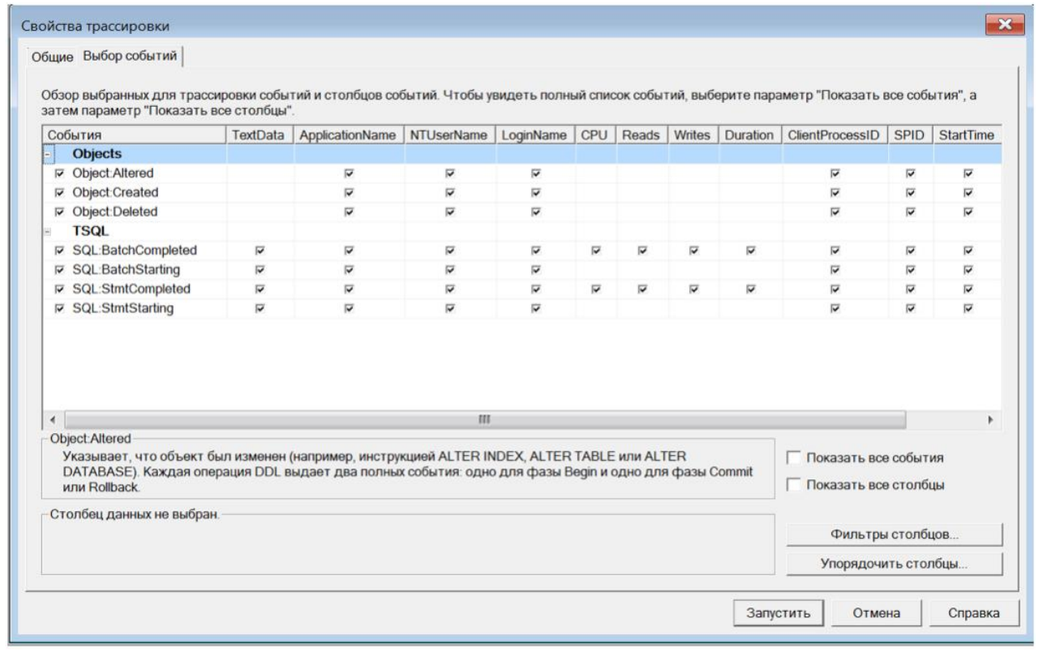
События Object и TSQL шаблона First

						Дипломный проект						
Изм.	Лист	Ф.И.О		Подп.	Дата	Свойства шаблона трассировки		Лист		Масса		Масштаб
Разраб.		Идришев А.										
Норм.		Кабдуллин М.						Лист 4		Листов 5		
Руков.		Айтхожаева Е										
Зав. каф.		Сейлова Н.				Тема: Организация мониторинга и аудита в MS SQL Server		КазНИТУ ИКиИТ СИБ 5В100200				

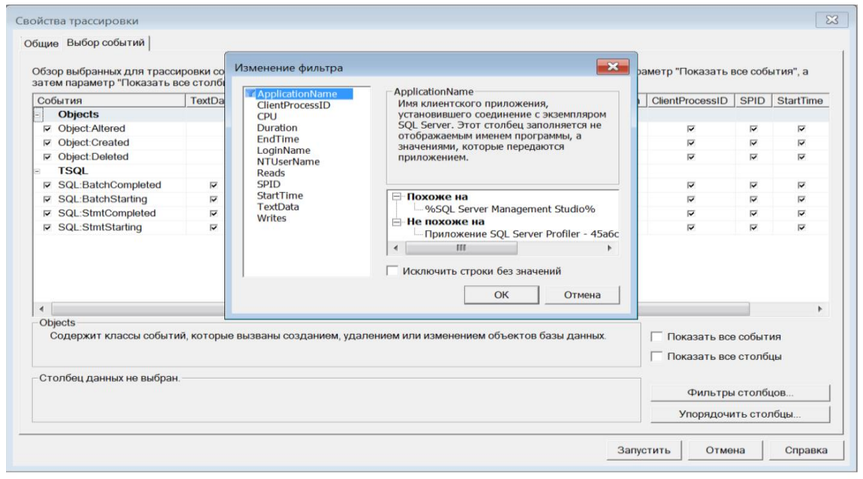
Приложение Б



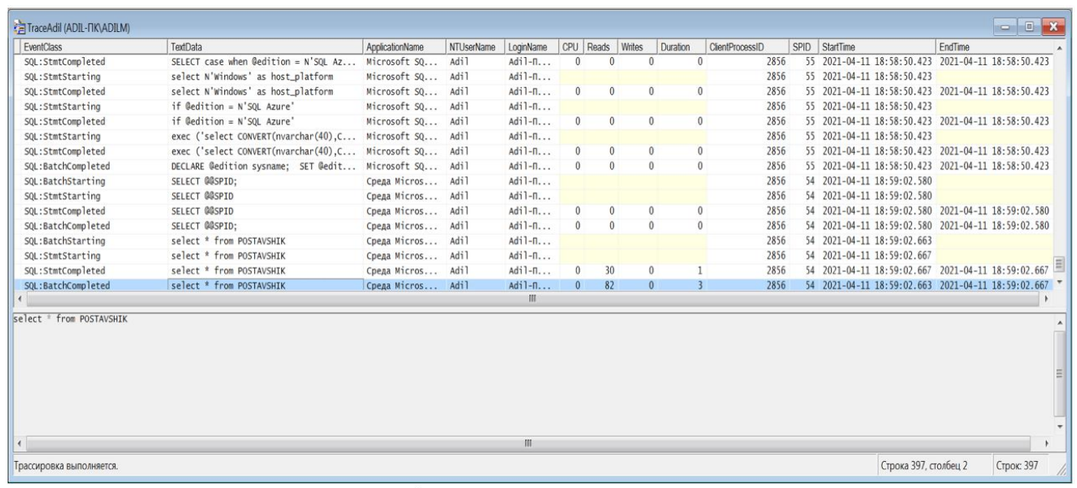
Общие параметры создания файла трассировки



События файла трассировки



Фильтр столбцов



Файл трассировки

						Дипломный проект	
Изм.	Лист	Ф.И.О		Подп.	Дата	Свойства файла трассировки	Лист / Масса / Масштаб
Разраб.		Идришев А.					
Норм.		Кабдуллин М.					Лист 5 / Листов 5
Руков.		Айтхожаева Е					
Зав. каф.		Сейлова Н.				Тема: Организация мониторинга и аудита в MS SQL Server	КазНИТУ ИКиИТ СИБ 5В100200

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

на дипломный проект
(наименование вида работы)
Идришев Әділ Мұратұлы
(Ф.И.О. обучающегося)

5В100200 - Системы информационной безопасности
(шифр и наименование специальности)

Тема:
«Организация мониторинга и аудита в MS SQL Server»

В дипломном проекте студента Идришева Ә.М. «Организация мониторинга и аудита в MS SQL Server» ставится и решается актуальная задача проектирования корректной и целостной базы данных и обеспечения ее безопасности с использованием механизмов мониторинга и аудита широко распространенного сервера БД MS SQL Server.

Идришев Ә.М. самостоятельно выполнил все задания по дипломному проекту. Выполнил рассмотрение механизмов мониторинга и аудита MS SQL Server, анализ предметной области «Магазин». Для проектирования базы данных был использован ER-метод, созданы информационная и логическая модели предметной области, определены ограничения целостности.

Сгенерированы SQL скрипты для реализации базы данных в СУБД MS SQL Server. База данных была реализована в MS SQL Server 2014 для учета, товара, сотрудников, поставщиков, производителей со всеми необходимыми компонентами.

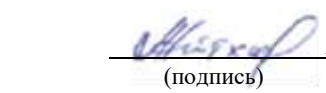
Показана технология использования в MS SQL Server 2014 графической утилиты SQL Profiler, а также SQL Audit, предназначенных для мониторинга активности и аудирования сервера и БД. Рассмотрено создание шаблонов профиля трассировки, создание файла трассировки, запуск файла трассировки для аудита и мониторинга событий в сервере БД. Выполнена трассировка заданных категорий событий и анализ полученных результатов.

В процессе дипломирования Идришев Ә.М. показал практическое умение работать с сервером баз данных MS SQL Server и его механизмами мониторинга и аудита, хорошие инженерные навыки как в области анализа, проектирования и реализации баз данных, так и умение работать с технической литературой.

Работа выполнена с использованием современных IT-технологий: CASE-средство проектирования баз данных AllFusion Erwin Data Modeler, сервер MS SQL Server 2014, утилита SQL Profiler, SQL Audit.

Дипломный проект на тему «Организация мониторинга и аудита в MS SQL Server» выполнен Идришевым Ә.М. на хорошем уровне и может быть допущен к защите.

Научный руководитель
ассоц.профессор, к.т.н.
(должность, ученая степень, звание)


Айтхожаева Е.Ж.
(подпись)
« 10 » 05 2021 г.

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился (-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Идришев Э.М.
Название: Организация мониторинга и аудита в MS SQL Server
Координатор: Айтхожаева Е.Ж.
Коэффициент подобия 1: 9.47%
Коэффициент подобия 2: 8.22%
Тревога: 0.97%

После анализа Отчета подобия констатирую следующее:

✓ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

□ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

□ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

Заимствования объясняются использованием специфической терминологии, которая включает несколько подряд идущих слов. Несколько повышенное значение коэффициента подобия 2 обусловлено тем, что в работе приведены правило Росса Андерсона в оригинале и описание механизмов мониторинга и аудита, взятое из разделов официального сайта Microsoft (в списке использованных источников указаны).

«20 » мая 2021 г.
Дата

Подпись Научного руководителя

Протокол анализа Отчета подобия заведующего кафедрой

Заведующий кафедрой заявляет, что ознакомился (-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Идришев Э.М.
Название: Организация мониторинга и аудита в MS SQL Server
Координатор: Айтхожаева Е.Ж.
Коэффициент подобия 1: 9.47%
Коэффициент подобия 2: 8.22%
Тревога: 0.97%

После анализа Отчета подобия констатирую следующее:

✓ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

□ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

□ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

Заимствования объясняются использованием технической терминологии. Повышенное значение коэффициента подобия 2 объясняется тем, что в работе приведены стандартные определения аудита и мониторинга и официальное описание механизмов мониторинга и аудита в MS SQL Server фирмы-производителя Microsoft.

«20» мая 2021 г.
Дата

Сейтова Н.Н.
Ф.И.О., подпись зав.кафедрой

Окончательное решение в отношении допуска к защите, включая обоснование:

Дипломный проект к защите допускается в связи с признанием заимствований добросовестными.

«20» мая 2021 г.
Дата

Сейлова И.А.
Ф.И.О., подпись зав.кафедрой