Министерство образования и науки Российской федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

Кубанский государственный технологический университет

(ФГБОУ ВО «КубГТУ»)

Институт компьютерных систем и информационной безопасности

Кафедра информационных систем и программирования

Отчет к

лабораторной работе №7:

«Настройка безопасности хранилища данных»

по дисциплине «Хранилища данных и аналитические информационные системы»

Выполнил студент

группы 19-КМ-ПИ1

Ручка Артем Алексеевич

**Задание**

Для разработанного ранее хранилища данных выполнить следующее:

1) определить и настроить роли пользователям;

2) ограничить права доступа к хранилищу данных;

3) выполнить резервное копирование хранилища данных;

4) выполнить восстановление хранилища данных.

**Ход работы**

Определяем роль «Обработка базы данных» и настраиваем ее ограничения(рисунок 1).

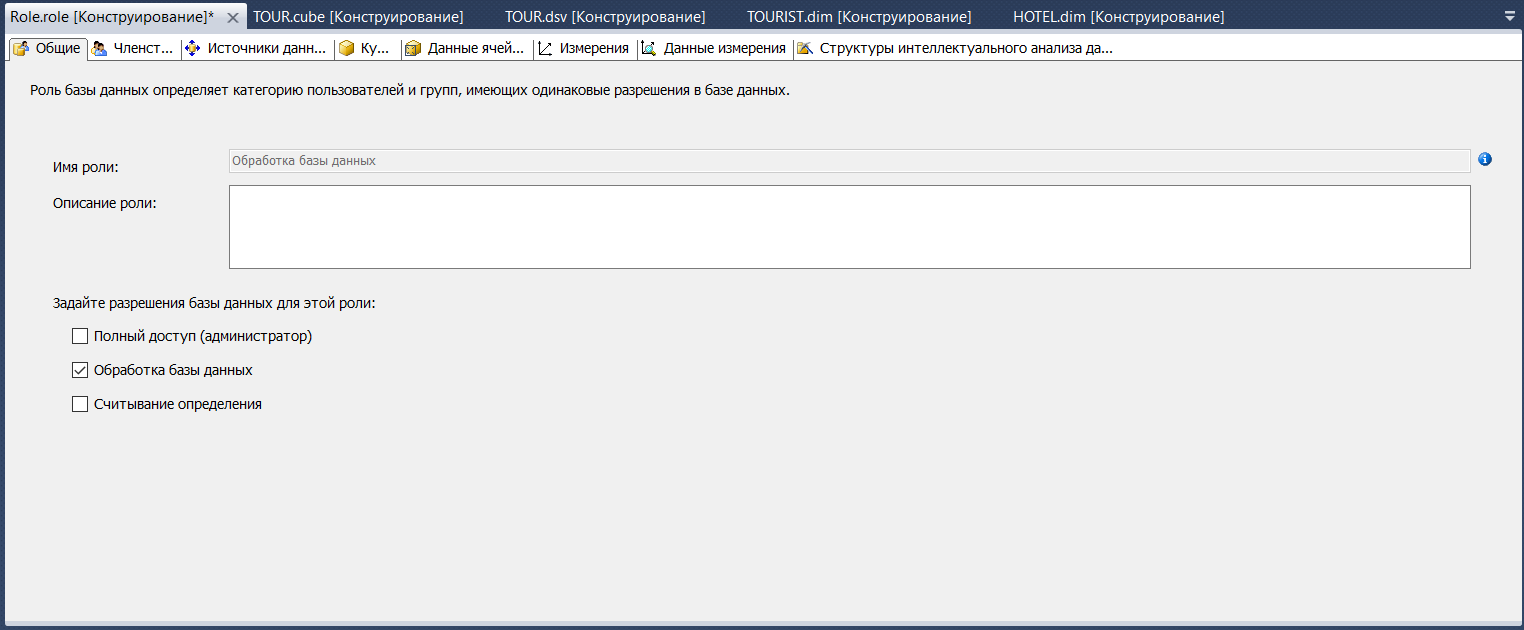


Рисунок 1 – Роль «Обработка базы данных»

Определяем роль «Администрирование» и настраиваем ее ограничения(рисунок 2).

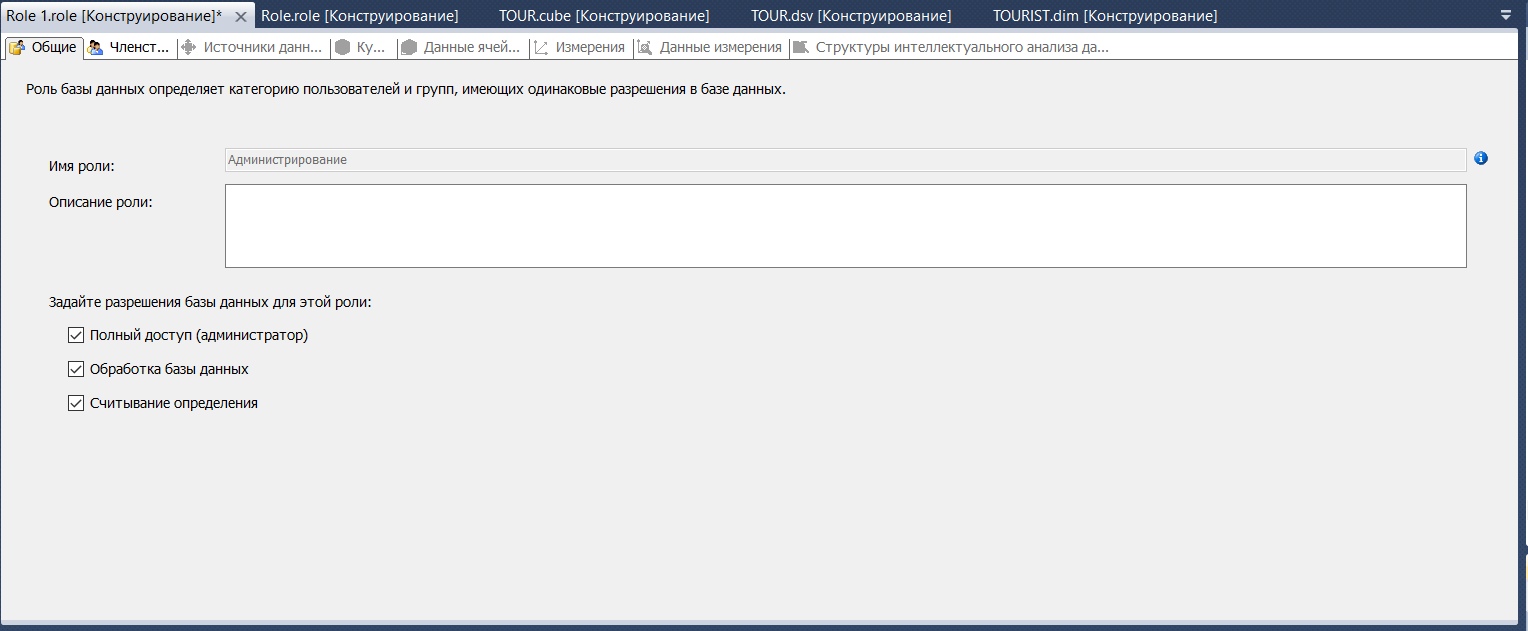


Рисунок 2 – Роль «Администрирование»

Указываем пользователя, который имеет доступ к роли «Обработка базы данных»(рисунок 3).

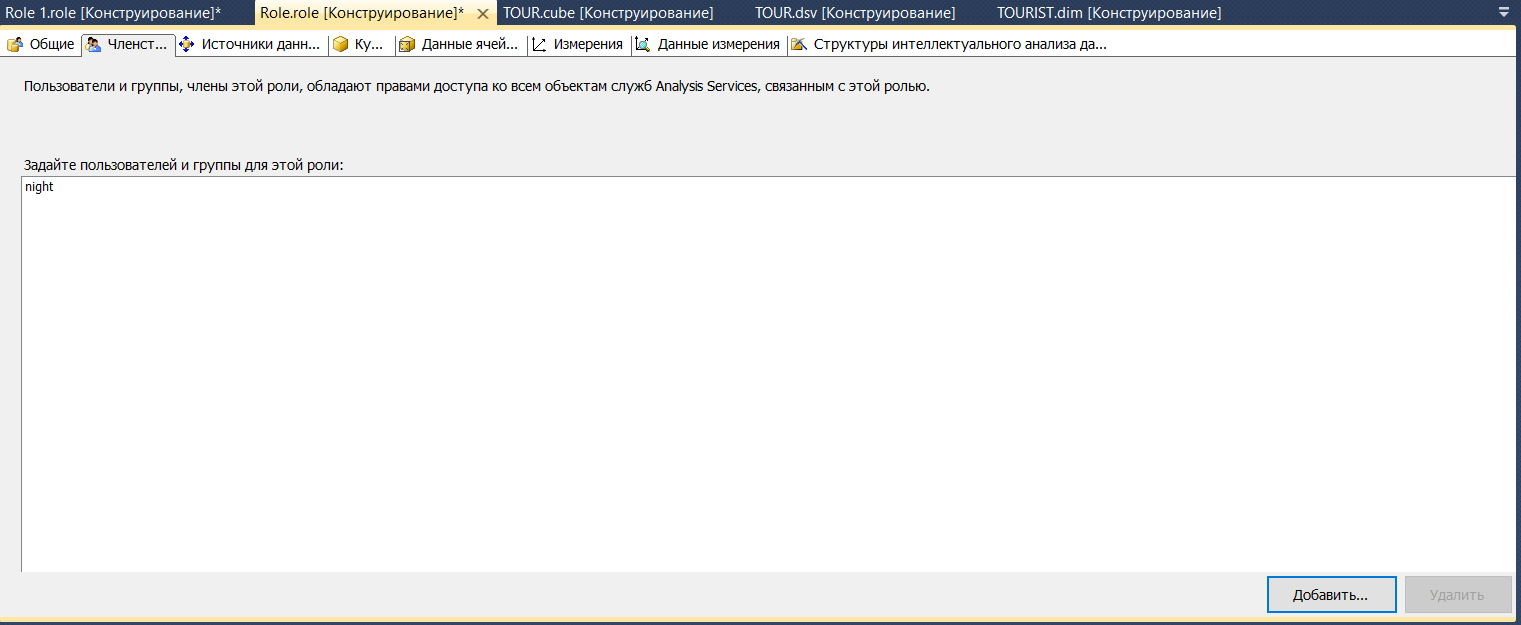


Рисунок 3 – Задание пользователя для роли

Создаем резервную копию базы данных(рисунок 4).

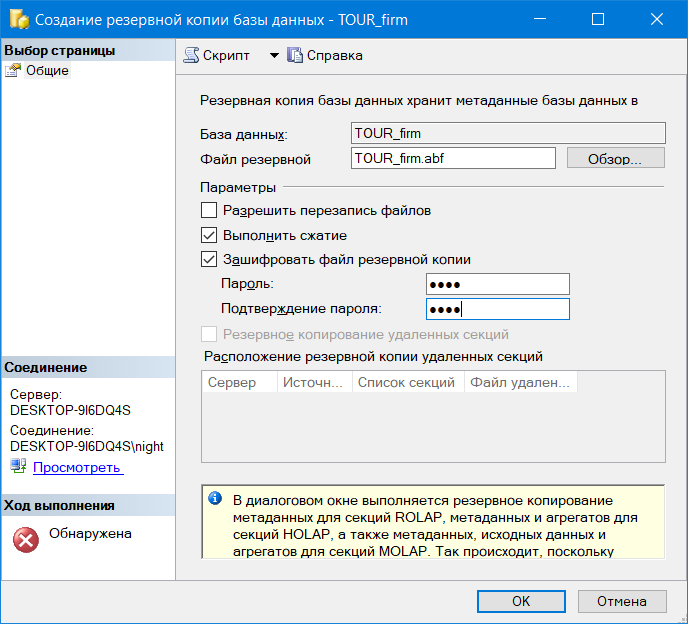


Рисунок 4 – Резервное копирование

Проводим восстановление базы данных(рисунок 5).

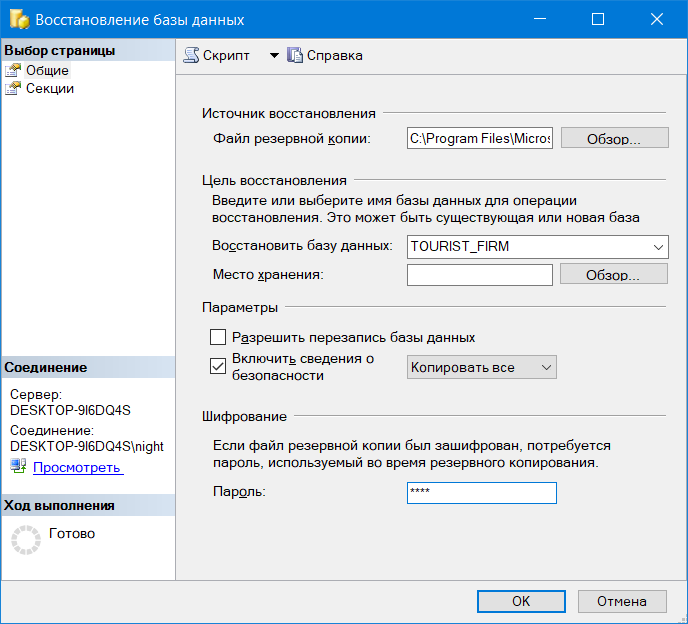


Рисунок 5 – Восстановление базы данных

**Контрольные вопросы**

*1. Перечислите точки доступа к экземпляру SSAS.*

Чтобы обеспечить надлежащую безопасность данных, хранимых в  
службах SSAS, необходимо обеспечить безопасность всех точек доступа к  
экземпляру служб SSAS. Эти точки доступа включают:

1. Защита компьютера со службами SSAS.

2. Защита операционной системы Windows для служб SSAS.

3. Защита программных файлов, общих компонентов и файлов  
данных.

4. Безопасность взаимодействия клиентов с экземпляром служб SSAS,  
что включает шифрование данных, проверку подлинности клиента,  
установку пакетов безопасности, и указание частоты обновления кэша ролей.

5. Защита источников данных, используемых службами SSAS.

6. Обеспечение безопасности доступа с помощью служб SSAS.

*2. Какие мероприятия следует предпринять для обеспечения физической безопасности компьютера?*

Чтобы повысить физическую безопасность компьютера, на котором запущены службы SSAS, выполните следующие шаги:

убедитесь в том, что только санкционированные пользователи имеют физический доступ к компьютеру. По возможности установите компьютер в

запертой комнате с ограниченным доступом;

отключите функцию загрузки с дискеты, если это возможно в настройках BIOS материнской платы, и рассмотрите возможность полного удаления дисковода;

отключите функцию загрузки с CD-ROM, если это возможно в настройках BIOS материнской платы;

увеличьте защиту компьютера путем использования пароля при включении и повысьте защиту настроек BIOS материнской платы, используя пароль доступа к BIOS;

используйте корпус для компьютера, который поддерживает обнаружение проникновения, и который невозможно открыть без ключа;

храните ключ в безопасном месте вдали от компьютера.

*3. Какие мероприятия предназначены для повышения защищенности операционной системы?*

Следующие мероприятия позволят повысить защищенность операционной системы:

* ограничение интерактивного доступа;
* ограничение сетевого доступа;
* отключение ненужных служб;
* указание и ограничение портов.

*4. Каким образом реализуется защита программных файлов, общих компонентов и файлов данных?*

Местоположение по умолчанию для файлов служб SSAS – «\Program  
Files\Microsoft SQL Server\MSAS10.#\OLAP», где # представляет собой номер  
экземпляра. В этой структуре папок имеются четыре вложенные папки:  
Backup, Bin, Data и Log. В этих папках хранятся данные резервного  
копирования, важные файлы для самой службы SSAS, фактические данные  
измерений и кубов, а также данные журналов. Эти данные должны быть  
защищены. Программа установки предоставляет доступ ко всем файлам в  
этой структуре папок только членам локальной группы «Администраторы» и  
учетной записи входа в службы SSAS. Пользователям доступ к файлам в этих  
папках не требуется.

*5. Как повысить безопасность взаимодействия клиентов с экземпляром служб SSAS?*

Безопасность взаимодействия клиентов с экземпляром служб SSAS,  
что включает шифрование данных, проверку подлинности клиента,  
установку пакетов безопасности, и указание частоты обновления кэша ролей.

*6. Каким образом реализуется проверка подлинности пользователей,*

*использующих SSAS?*

Если неавторизованные пользователи получат доступ к источникам данных, из которых службы SSAS загружают данные, эти пользователи будут иметь доступ к сведениям, которые хранятся в экземпляре служб SSAS. Следует ограничить доступ к этим источникам данных. Для просмотра кубов и измерений пользователям служб SSAS не нужны разрешения на эти  
источники данных.

*7. Какие пользователи становятся членами роли сервера служб SSAS по умолчанию? Какими способами можно предоставить другим пользователям доступ к службам SSAS?*

Службы SSAS разрешают устанавливать соединения только пользователям, прошедшим проверку подлинности Windows, если только не разрешены анонимные подключения, и пользователям, которым предоставлены разрешения в экземпляре служб SSAS. Пользователям, не имеющим разрешений, устанавливать соединения запрещено. Службы SSAS не выполняют собственной проверки подлинности пользователей. При проверке подлинности всех пользователей перед авторизацией доступа к данным служб SSAS или перед предоставлением пользователям возможности  
выполнения административных задач службы SSAS полагаются на  
операционную систему Windows.

По умолчанию любой пользователь, не являющийся членом роли  
сервера, не имеет разрешений служб SSAS. Чтобы получить разрешения,  
член роли сервера должен сначала создать пользовательскую роль базы  
данных, а затем предоставить этой роли разрешения.

*8. Какими способами может быть предоставлен административный доступ к объектам в экземпляре служб SSAS?*

Административный доступ к объектам в экземпляре служб SSAS  
предоставляется пользователям и группам Microsoft Windows следующими  
способами:

1. Пользователи и группы могут получить административный доступ  
к службам SSAS на уровне сервера с помощью роли сервера. Члены роли  
сервера на экземпляре службSSAS имеют неограниченный доступ ко всем  
объектам и данным данного экземпляра служб SSAS. Член роли сервера  
служб SSAS может добавлять пользователей и группы Microsoft Windows в  
роль сервера служб SSAS. Для выполнения любых задач на уровне сервера,  
например для создания базы данных, изменения свойств сервера или запуска  
трассировки (кроме обработки событий) пользователь должен входить в  
состав роли сервера служб SSAS. По умолчанию члены локальной группы  
«Администраторы» входят в состав роли сервера служб SSAS. Тем не менее,  
их принадлежность к этой роли сервера не отражается в пользовательском  
интерфейсе.

2. Пользователи и группы могут получить административный доступ  
к определенной базе данных служб SSAS с помощью роли базы данных. В  
службах Microsoft SQL Server члены роли сервера служб SSAS могут  
создавать в базе данных роли базы данных и предоставлять этим ролям  
полные или ограниченные административные разрешения в базе данных.  
Члены роли сервера служб SSAS могут добавлять к этим ролям базы данных  
пользователей и группы Microsoft Windows.

*9. Какие разрешения роль сервера служб SSAS может предоставить роли базы данных?*

Роль сервера служб SSAS может предоставить роли базы данных следующие разрешения:

* полные административные разрешения в базе данных;
* только разрешение на обработку некоторых объектов служб SSAS.

**Заключение**

В результате выполнения данной лабораторной работы были определены и настроены роли пользователей, ограничены права доступа к хранилищу данных, выполнено резервное копирование хранилища данных и восстановление хранилища данных.