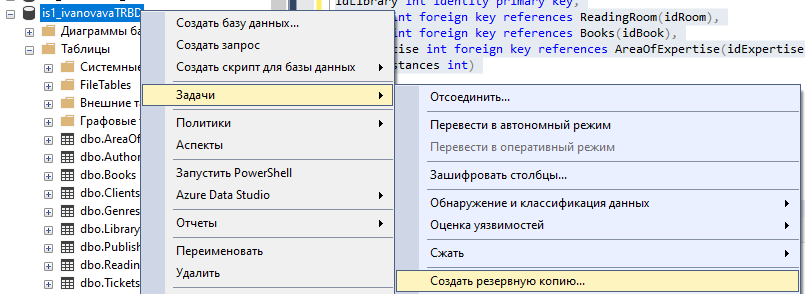
**Обеспечение целостности данных в базе данных**

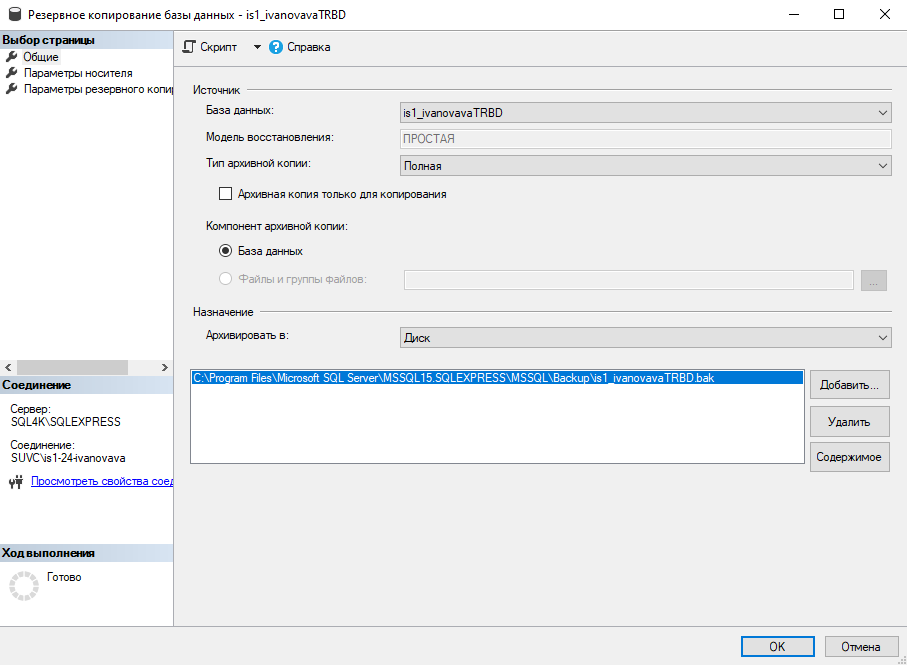
**1 Вариант:**

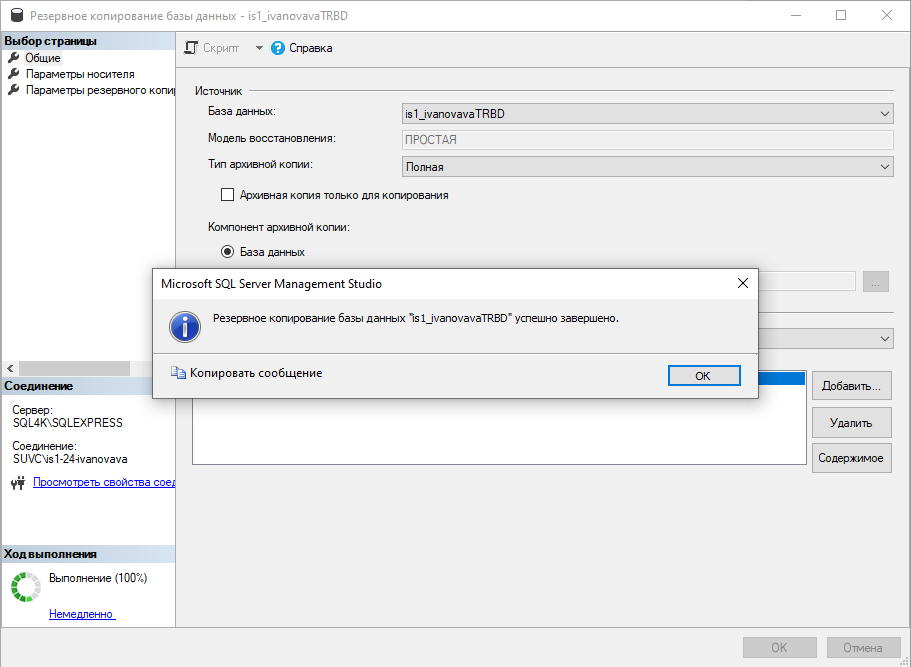
Перед всеми манипуляции нужно создать резервную копию, и в случае возникновения непредвиденных проблем восстановить из ранее созданной резервной копии. (Данный вариант уже проделывался в работах: Отчет по резервному копированию и Отчет по восстановлению резервной копии)

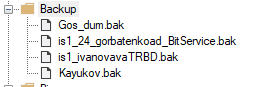
Выбираем нашу базу данных и нажимаем ПКМ 🡪 выбираем пункт «Задачи» 🡪 «Создать резервную копию…»



В открывшемся окне ничего не меняем и нажимаем «ОК»

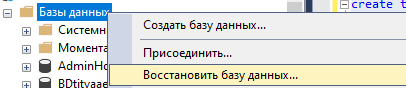


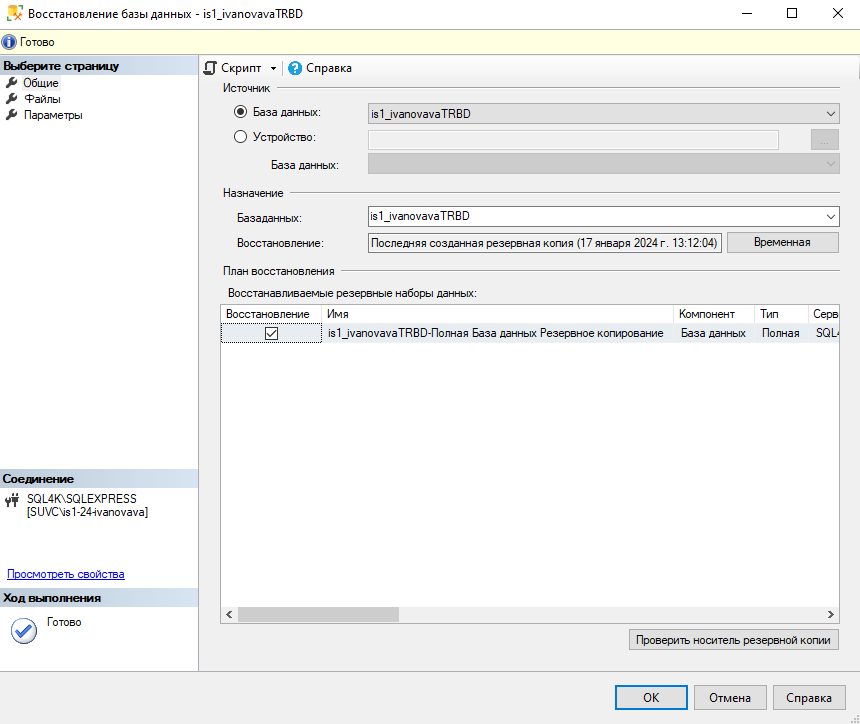


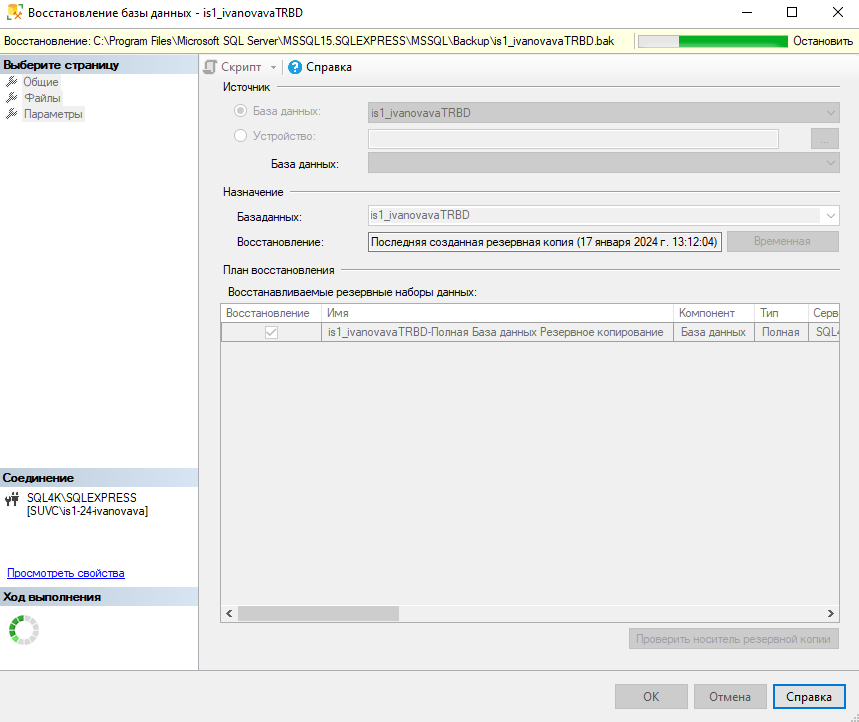


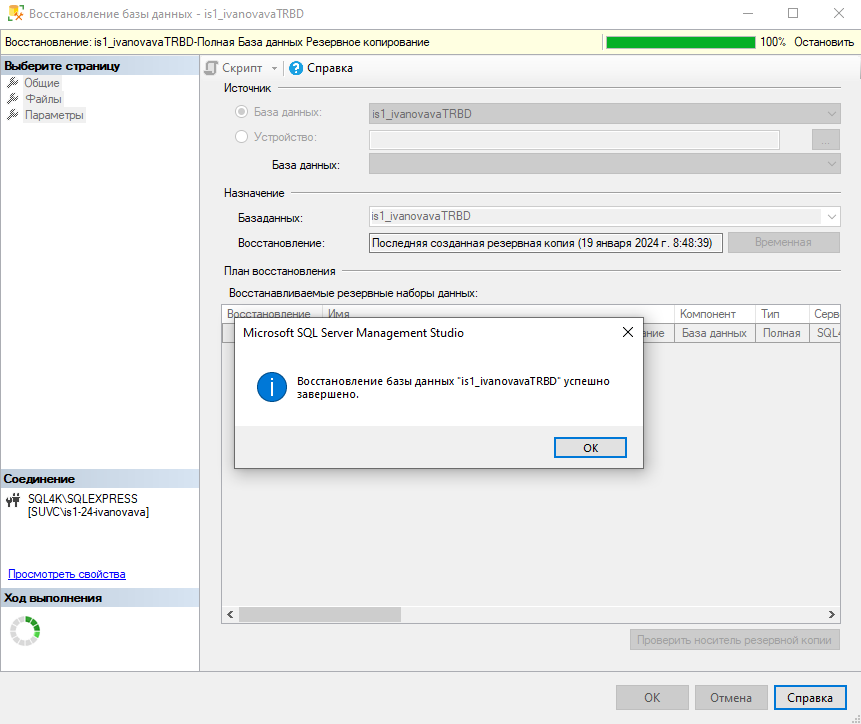
- Восстановление

Нажимаем ПКМ по «Базы данных» 🡪 Восстановить базу данных 🡪 рядом с отмеченным пунктом «Базы данных» в выпадающем списке выбираем нашу ранее созданную нами копию нашей БД 🡪 далее нажимаем «ОК» и ждём восстановления нашей БД









**2 Вариант:**

Почистить всё саморучно.

Примечание: в данном случае есть возможность удалить нужные вещи и таким образом поломать всё БД.

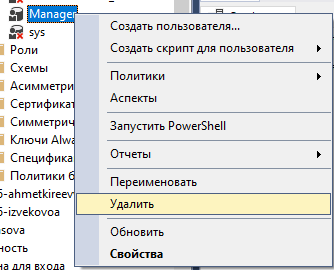
Все Пользователи находятся по пути: «Название нашей БД» 🡪 Безопасность 🡪 Пользователи

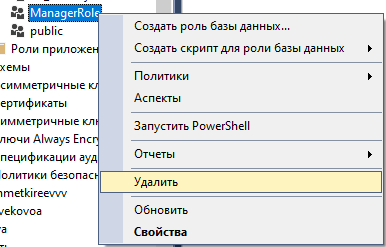
Все Роли находятся по пути: «Название нашей БД» 🡪 Безопасность 🡪 Роли 🡪 Роли базы данных

Не забудем и о том, что помимо нашей БД, они хранятся и в общем месте:

Для удаления Пользователей переходим по пути: База данных 🡪 Безопасность 🡪 Имена для входа

Для удаления Ролей: База данных 🡪 Безопасность 🡪 Роли сервера

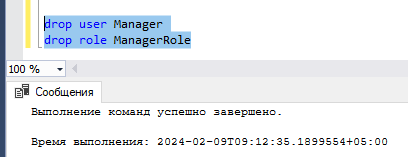




**3 Вариант:**

Почистить всё через скрипт





**Вопрос: Почему проведение данной чистки является одним из необходимых этапов, к чему может привести отсутствие чистки?**

Проведение чистки в базе данных является одним из необходимых этапов, так как отсутствие чистки может привести к следующим проблемам:

1. Нарушение целостности данных:

Если в базе данных остаются манипуляции SQL или подозрительные данные, это может привести к нарушению целостности данных. Это может привести к ошибкам в работе приложений, некорректным результатам запросов или даже потере данных.

1. Угроза безопасности:

Оставленные манипуляции SQL могут быть использованы злоумышленниками для получения несанкционированного доступа к данным или выполнения вредоносных операций в базе данных. Это может привести к утечке конфиденциальной информации или повреждению данных.

1. Падение производительности:

Наличие манипуляций SQL или подозрительных данных в базе данных может снизить производительность системы из-за неэффективных запросов или нагрузки на сервер базы данных.

1. Негативное влияние на репутацию компании:

Если данные в базе данных подвергаются манипуляциям или атакам, это может негативно отразиться на репутации компании перед клиентами, партнерами и общественностью.

Поэтому проведение чистки в базе данных является важным шагом для обеспечения безопасности, целостности и производительности системы.