МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ (ПРЕЗЕНТАЦИИ К ЛЕКЦИОННЫМ МАТЕРИАЛАМ)

Безопасность систем баз данных

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	специалист *(бакалавриат, магистратура, специалитет)*
Форма обучения	очная *(очная, очно-заочная, заочная)*
Направление(-я) подготовки	10.03.01 «Информационная безопасность автоматизированных систем» *(код и наименование)*
Институт	Кибербезопасности и цифровых технологий *(полное и краткое наименование)*
Кафедра	Информационно-аналитические системы кибербезопасности (КБ-2) *(полное и краткое наименование кафедры, реализующей дисциплину (модуль))*
Лектор	К.т.н., доцент Шукенбаев Айрат Бисенгалеевич *(сокращенно – ученая степень, ученое звание; полностью – ФИО)*

Используются в данной редакции с учебного года 2023/2024
(учебный год цифрами)

Проверено и согласовано «____» _____20___г.

_____ А.А. Бакаев
(подпись директора Института/Филиала с расшифровкой)

Москва 2024 г.

Ощущение полной безопасности наиболее опасно.
Илья Нисонович Шевелев
Везде, где есть жизнь, есть и опасность.
Ральф Уолдо Эмерсон

Безопасность систем баз данных.

Тема лекции: Анализ включающей инфраструктуры

Архитектура системы безопасности MS SQL Server. Учетные записи и пользователи. Режимы аутентификации.

Полный доступ к базе данных и всем ее объектам имеет ***администратор***, который является своего рода хозяином базы данных — ему позволено все.

Второй человек после администратора — это ***владелец объекта***. При создании любого объекта в базе данных ему назначается владелец, который может устанавливать права доступа к этому объекту, модифицировать его и удалять.

Третья категория пользователей имеет права доступа, выданные им администратором или владельцем объекта.

Учетные записи и пользователи

Система безопасности SQL Server 2012 и выше базируется на учетных записях (имена входа) и пользователях.

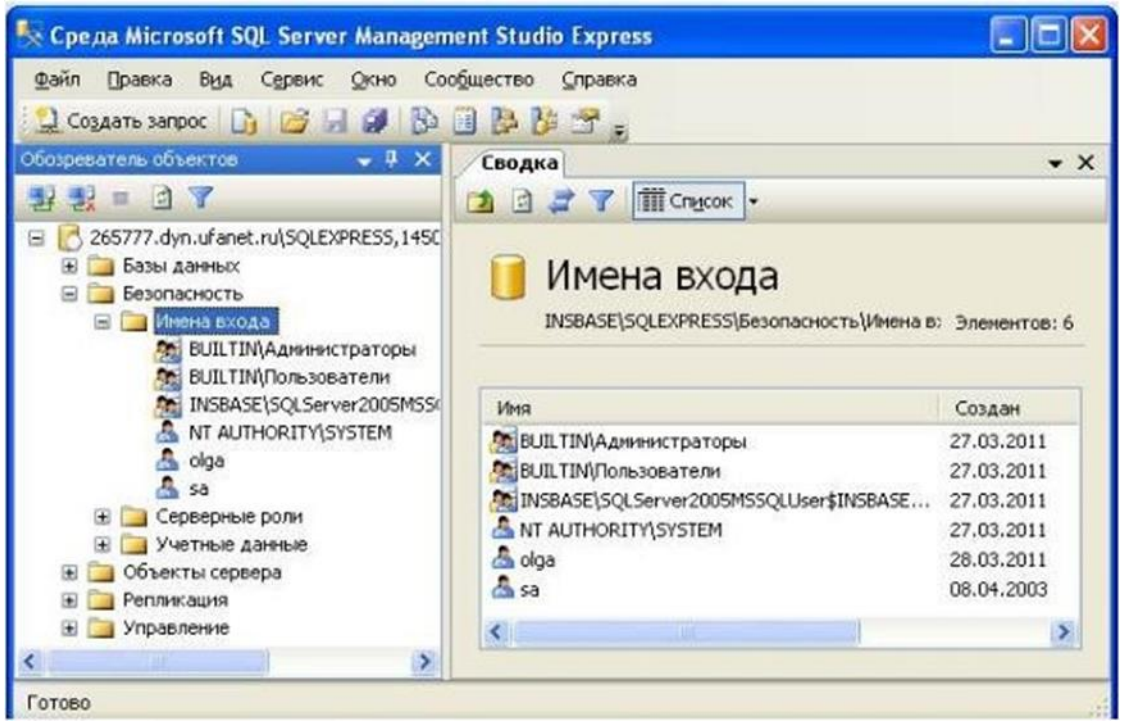


Рис. 1. Учетные записи (мена входа) определяются на уровне сервера

Пользователи проходят следующие **два этапа** проверки системой безопасности. На ***первом этапе*** пользователь идентифицируется по имени учетной записи и паролю, то есть проходит аутентификацию.

На ***втором этапе***, на основе прав, выданных пользователю как пользователю базы данных (user), его регистрационное имя (login) получает доступ к соответствующей базе данных.

на ***уровне сервера*** система безопасности оперирует следующими понятиями:

- аутентификация (authentication);
- учетная запись (login);
- встроенные роли сервера (fixed server roles).

На ***уровне базы данных*** используются следующие понятия:

- пользователь базы данных (database user);
- фиксированная роль базы данных (fixed database role); - пользовательская роль базы данных (users database role);
- роль приложения (application role).

Режимы аутентификации

SQL Server 2012 может использовать два режима аутентификации пользователей:

- режим аутентификации средствами Windows;
- смешанный режим аутентификации (Windows Authentication and SQL Server Authentication).

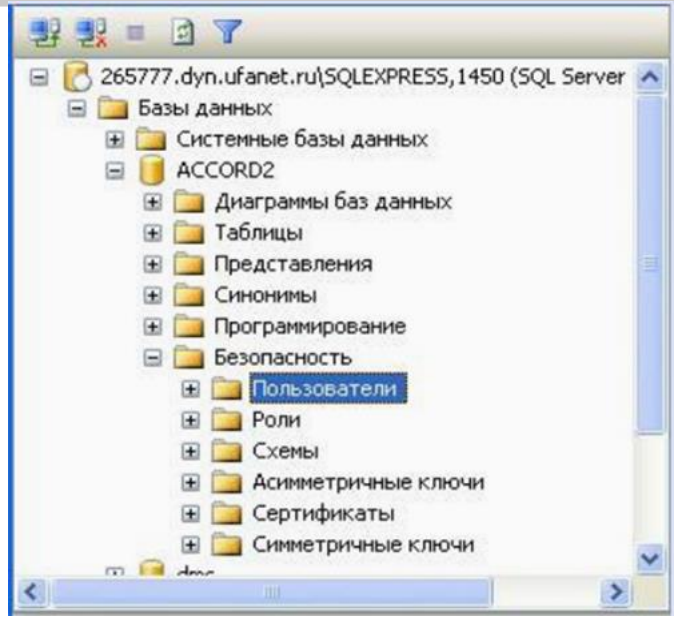


Рис. 2. Пользователи определяются для БД

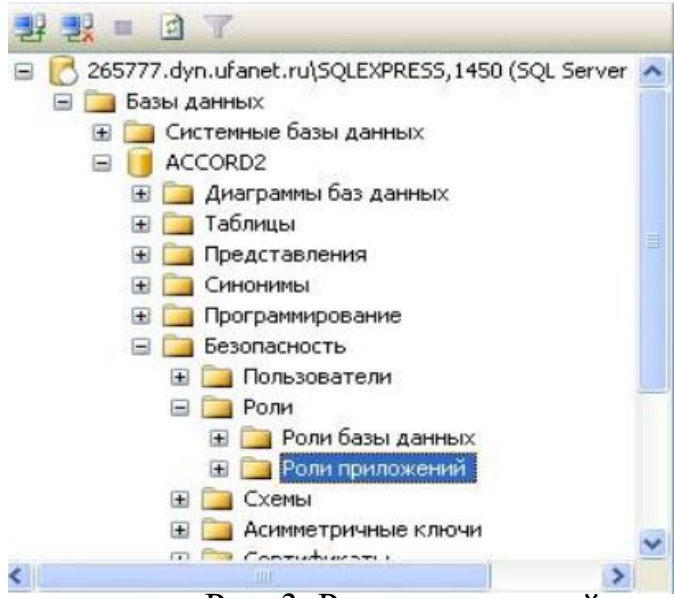


Рис. 3. Роли приложений

После аутентификации

В пользователя базы данных может отображаться:

* учетная запись Windows;
* группа Windows;
* учетная запись SQL Server.

База данных рабочей области (табличные службы SSAS)

SQL Server Data Tools (SSDT).

БД рабочей области находится в памяти на экземпляре Службы Analysis Services, запущенном в табличном режиме на том же компьютере, что и SQL Server Data Tools.

БД рабочей области создается на экземпляре служб Службы Analysis Services, указанном в свойстве "Сервер рабочей области", при создании нового проекта бизнес-аналитики с помощью одного из шаблонов проекта табличной модели в SQL Server Data Tools.

Удаленно расположенные базы данных рабочей области имеют следующие ограничения:

- потенциальные задержки при отправке запросов;
- свойство "Резервное копирование данных" не может иметь значение *Резервное копирование на диск;*
- нельзя импортировать данные из книги PowerPivot при создании нового проекта табличной модели с помощью шаблона проекта «Импорт из PowerPivot».

Свойства базы данных рабочей области

Свойства базы данных рабочей области включены в свойства модели. Чтобы просмотреть свойства модели, в SQL Server Data Tools в **обозревателе решений** щелкните файл **Model.bim**. Свойства модели могут быть настроены в окне **Свойства**.

Использование SSMS для управления базой данных рабочей области

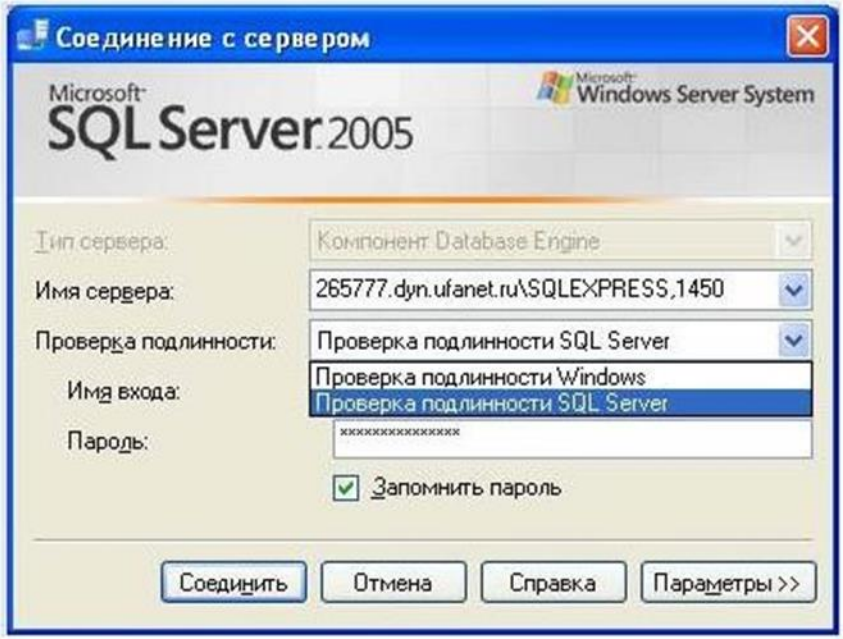


Рис. 4. Выбор режима аутентификации

Аудит систем баз данных

Причины проведения аудита

Выделяют две основные причины складывающейся ситуации:

— возрастающая роль информационных технологий в современных методах ведения бизнеса и, как следствие, более высокие требования к защищенности ИС;

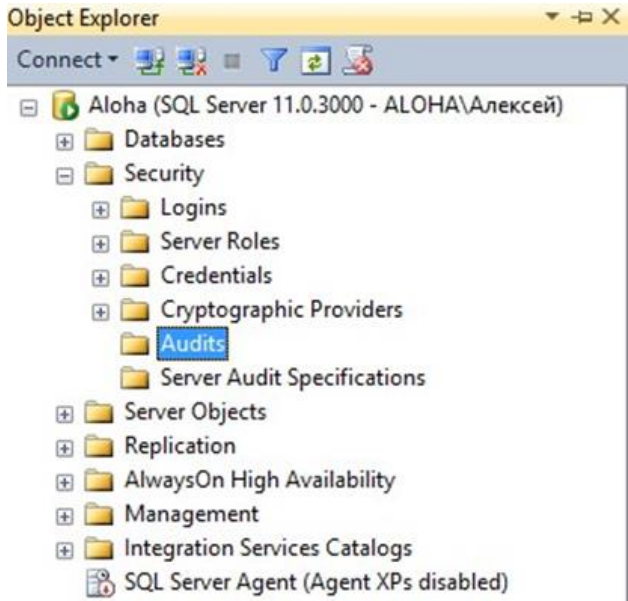
— увеличение сложности информационных систем и их подсистем обеспечения безопасности; возрастающие требования к организации деятельности и квалификации персонала, ответственного за обеспечение безопасности ИС.

Общая характеристика средств аудита СУБД

Пользователь, обладающий необходимыми полномочиями, может выполнять следующие действия со средствами аудита:

- запускать и останавливать средства аудита;
- просматривать состояние конфигурации средств аудита и настраивать средства аудита на фиксацию определенных событий;
- переписывать данные аудита во внешние файлы операционной системы для проведения независимого анализа.

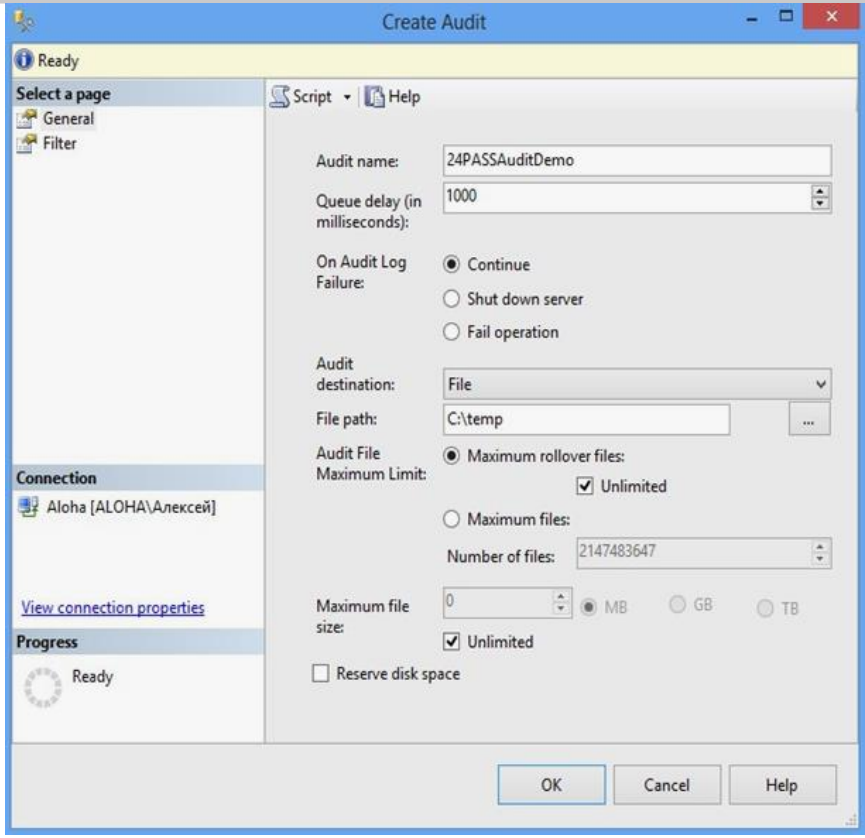
Аудит на уровне базы банных доступен только в выпусках Datacenter, Enterprise Edition, Developer Edition и Evaluation Edition.



Аудит может быть сохранѐн в один из трѐх источников:

- В файл (**File**)
- В журнал приложений Windows (**Windows Security Log**)
- В журнал безопасности Windows (**Windows Application Log**)

Для этого необходимо перейти во вкладку **Security -> Audits.**



- **Audit name** - название аудита
- **Queue delay** - Определяет задержку в миллисекундах, после которой продолжается выполнение действий аудита.
- **On Audit Log Failure** - Указывает, будет ли экземпляр, выполняющий запись в целевой объект, вызывать ошибку (**Fail operation**), продолжать работу (**Continue**) или останавливать SQL Server (**Shut down server**), если целевой объект не может выполнить запись в журнал аудита.
- **Audit destination** - Определяет расположение целевого объекта аудита.
- **File path** - Путь к журналу аудита. Имя файла формируется на основе имени аудита и его идентификатора GUID.
- **Maximum rollover files** - Указывает максимальное количество файлов, хранимых в файловой системе помимо текущего. Значением MAX_ROLLOVER_FILES должно быть целое число или UNLIMITED. Значение по умолчанию — UNLIMITED.
- **Maximum files** - Задает максимальное число файлов аудита, которые могут быть созданы. При достижении предела переключение на первый файл не производится. При достижении предела MAX_FILES любое действие, которое вызывает создание дополнительных событий аудита, завершится ошибкой.
- **Reserve disk space** - Этот параметр заранее размещает на диске файл в соответствии со значением MAXSIZE. Применяется, только если MAXSIZE не имеет значения UNLIMITED. Значение по умолчанию — OFF.

Особое внимание стоит уделить параметру **“ON_FAILURE = FAIL_OPERATION”**.

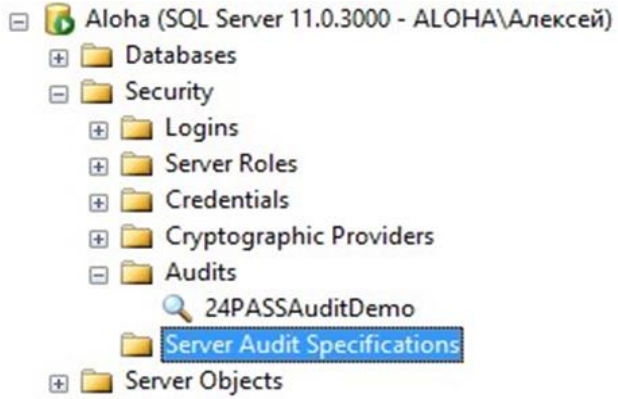
Создание Аудита с помощью запроса будет выглядеть примерно так:

```
use master; go
create server audit [24PASSAuditDemo]
to file (      filepath = N'c:\temp'
        , maxsize = 0 mb
        , max_rollover_files = 2147483647
        , reserve_disk_space = off
        )
with (      queue_delay = 1000
     , on_failure = continue
     );
go
```

После создания, аудит нужно включить:

```
use master; go
alter server audit [24PASSAuditDemo] with ( state = on );
```

Теперь можно создать **Спецификацию аудита сервера**, которая фиксирует события уровня сервера.



либо **Спецификацию аудита базы данных**, которая включает действия аудита уровня базы данных.

Список событий, на которые срабатывает аудит сервера и БД можно прочитать по ссылке: http://msdn.microsoft.com/ru-ru/library/cc280663.aspx