

**ДОРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННО-МЕТОДИЧЕСКОГО
ОБЕСПЕЧЕНИЯ КУРСА «УПРАВЛЕНИЕ ДАННЫМИ» СПЕЦИАЛЬНОСТИ 09.03.02
«ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»**

**Филина В.А, студент гр.ИТм-171, II курс
Научный руководитель: Ванеев О.Н., к.т.н. доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово**

Современное образование представляет из себя сложную систему, включающую в себя компоненты различного типа. Отдельно можно выделить комплекс методических материалов по лекционным занятиям, по лабораторным работам, включающего индивидуальные задания для студентов, контрольные вопросы и т.д. Вместе этот материал может быть представлен как информационно - методическое обеспечение курса. Данное обеспечение должно постоянно обновляться, соответствовать текущему уровню развития технологии и в то же время обеспечивать решение задач, стоящих перед учебным процессом.

Базы данных являются центральным ядром многих компаний, в которой хранится информация, без которой существование организации станет невозможным. Современная СУБД позволяет вести огромную базу данных без каких-либо ограничений, но без грамотного администрирования невозможно добиться корректной работы и использование информации, хранящейся в ней. Следовательно, необходимо выстраивать комплексную защиту элементов инфраструктуры и самих баз данных для предотвращения частичной потери или утечки коммерческой информации, что в нынешних жестких рыночных условиях может иметь обширные негативные последствия. В связи с этим, информационная безопасность является обязательным условием функционирования любого бизнеса. Таким образом администрирование представляет собой практически главнейшую область работы с СУБД.

Цель:

- Получение студентами знаний, умений навыков по администрированию СУБД.

Задачи:

- Доработка системы информационного и методического обеспечения по курсу УД:

- обеспечить знание концепции безопасности
- обеспечить умение делегирование прав и полномочий субъектов безопасности
- обеспечить владение навыками администрирования СУБД средствами языка запросов (T-SQL) и клиентского приложения SQL Server Management Studio

Согласно ФГОС по направлению подготовки 09.03.02 Информационные системы и технологии (уровень бакалавриата) 2015 г. и разработанной на его основе образовательной программе требования к результатам освоения дисциплины «Управление данными» выражаются в следующих компетенциях:

- ОПК-6 способностью выбирать и оценивать способ реализации информационных систем и устройств программно, аппаратно или программноаппаратно для решения поставленной задачи
- ПК-2 способностью проводить техническое проектирование
- ПК-3 способностью проводить рабочее проектирование

Необходимо отметить, что формулировки компетенций имеют весьма общий характер, подходящий под все стандарты, из числа указанных в приложении к ФГОС ВО. Когда гораздо важнее детализировать содержание профессиональных компетенций, отображающих знания, умения и навыки работы с конкретными процессами, технологиями и системами.

В ФГОС ВО подразумевается, что профессиональные компетенции должны формироваться на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников. Исходя из этого будет логично будет «привязать» компетенции к трудовым функциям профессиональных стандартов, что отражает прикладной характер предлагаемой системы обучения, что для такой ИТ-отрасли как является положительным фактором.

Анализ характеристик профессиональной деятельности, описанных в профессиональных стандартах показывает, что в наибольшей степени содержанию дисциплины «Управление данными» соответствуют трудовые функции профессионального стандарта «Администратор базы данных».

На рисунке 1 представлена диаграмма классов, содержащая выделенные компетенции и индикаторы достижения компетенций для дисциплины

определенные на основании обобщенных трудовых функций и трудовых функций отмеченного выше профессионального стандарта.

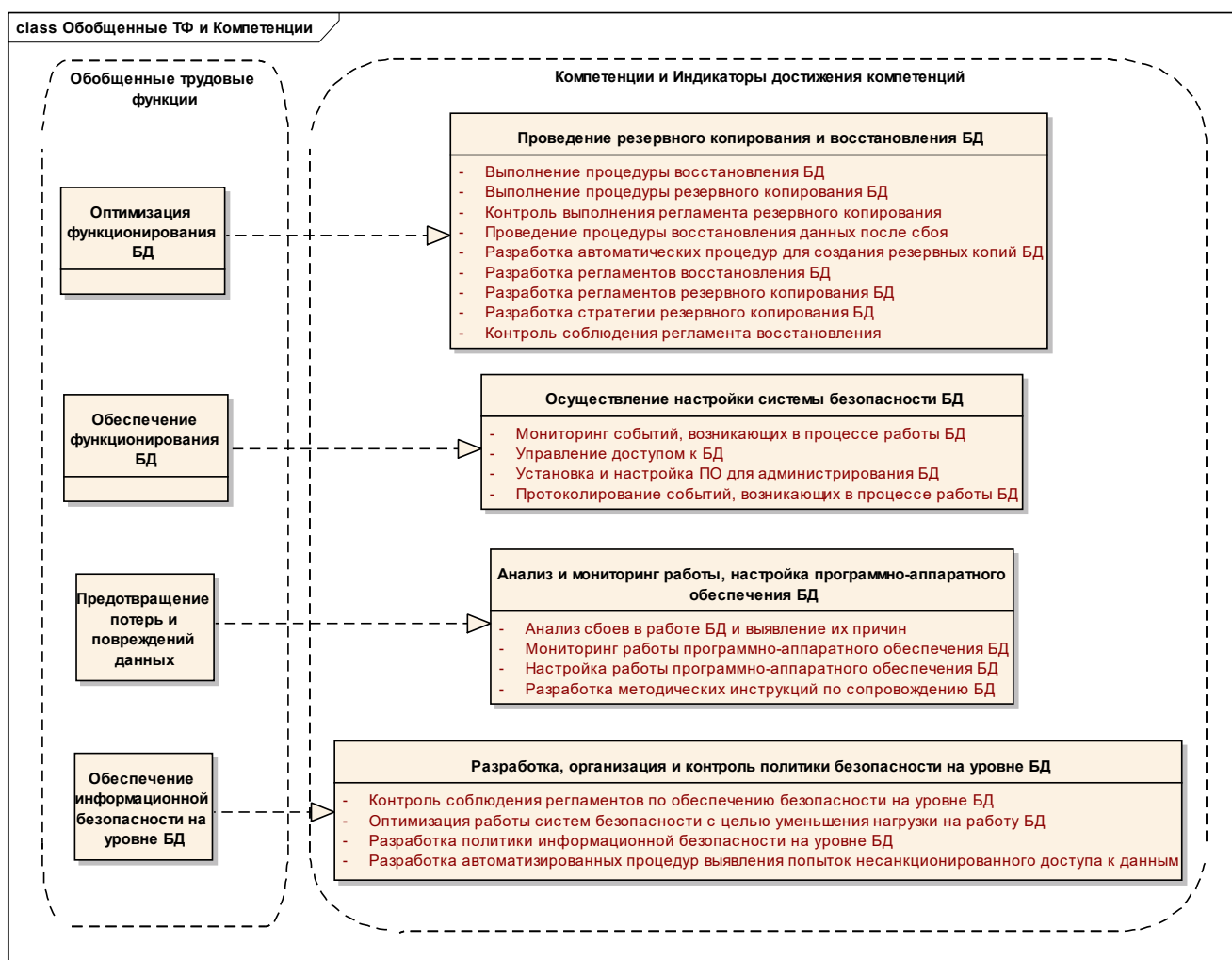


Рисунок 1. Компетенции и индикаторы достижения компетенций

Исходя из содержания диаграммы можно отметить, что компетенции, формирование и развитие которых закреплено за учебной дисциплиной «Управление данными» находят свое отражение в трудовых функциях. Таким образом, выбор указанных выше компетенций представляется обоснованным.

Процесс администрирования БД способствует интеграции аспектов безопасности в организацию. Изучение студентами вуза дисциплины «Управление данными» позволит сформировать у них компетенции по оценке и классификации угроз, и уязвимостей СУБД, разработке и введению стандартных механизмов обеспечения безопасности, и разработке комплексных методик обеспечения безопасности хранилищ данных на предприятии. Следовательно, можно предложить следующий материал дополняющий существующую программу дисциплины, для наиболее полного формирования данных компетенций. Диаграммы классов, отображающие

содержание материала и формируемые компетенции приведены на рисунках 2 и 3.

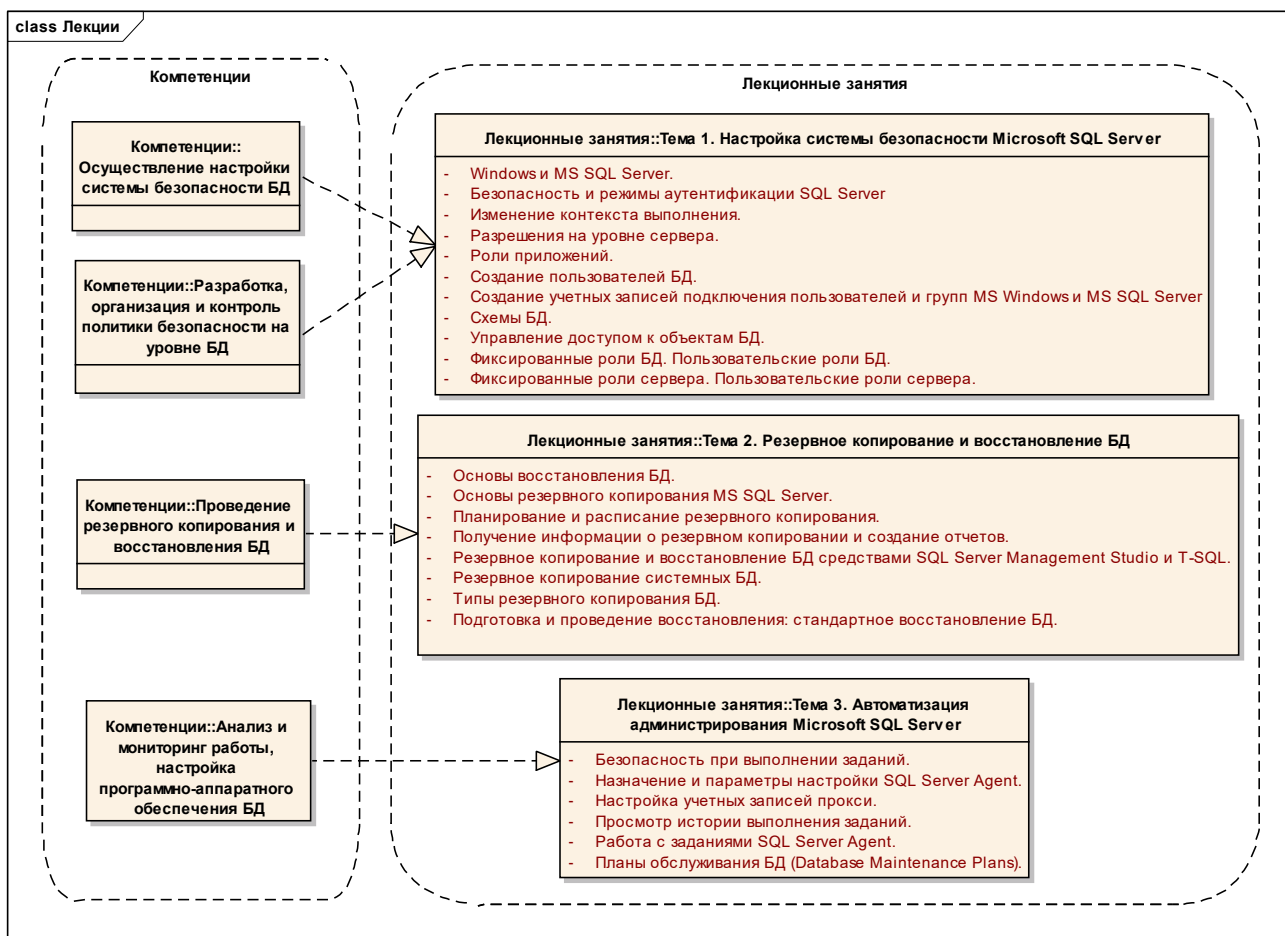


Рисунок 2. Лекционный материал

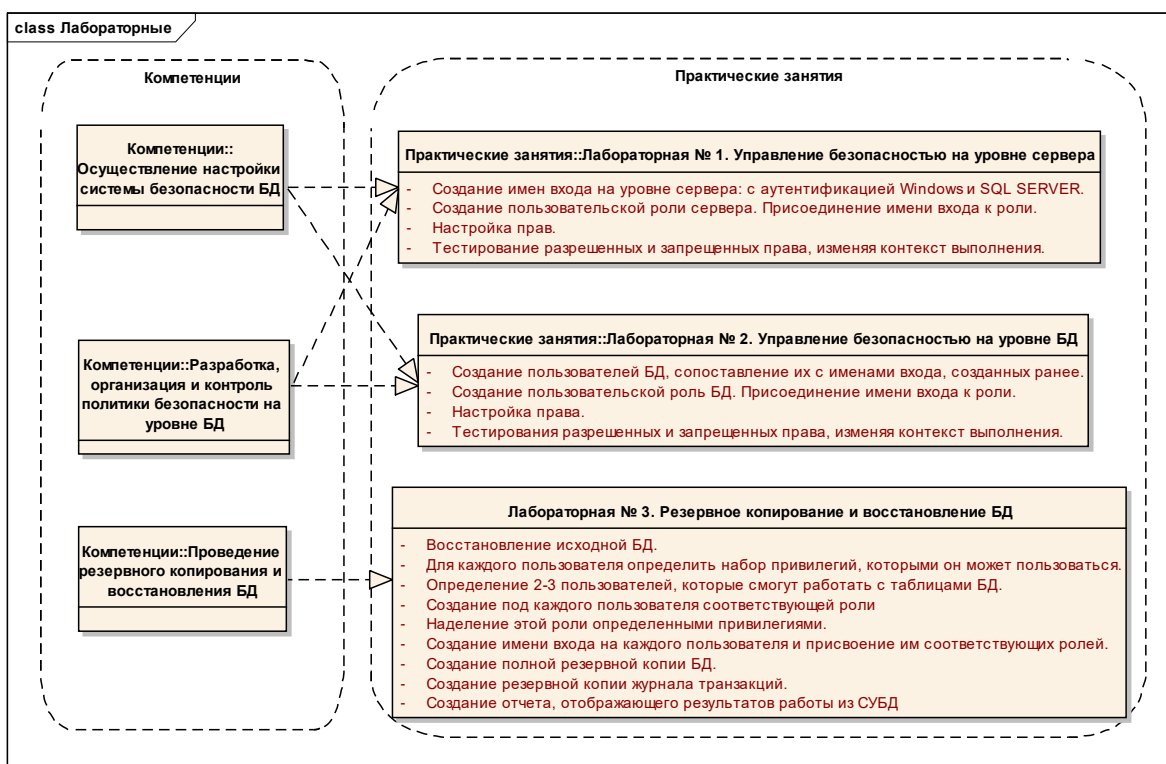


Рисунок 3. Практический материал

Приведем пример заданий для управления безопасностью на уровне сервера и БД с использованием разрешений. Для начала создадим два имени входа для сервера: director и teacher. После этого создадим пользовательскую роль сервера UsRolServ и присвоим ей разрешение CONTROL SERVER, которое дает права идентичные роли sysadmin. Затем запретим разрешение на создание или изменение других серверных ролей, имен входа и БД. Так же к данной роли присоединим ранее созданное имя входа director.

```

CREATE LOGIN director
WITH PASSWORD = 'password'
MUST_CHANGE, CHECK_EXPIRATION = ON;
GO
CREATE LOGIN teacher
WITH PASSWORD = 'EDxQk!R209*:ZJ5';
GO
USE master;
GO
CREATE SERVER ROLE UsRolServ;
GO
ALTER SERVER ROLE UsRolServ ADD MEMBER director;
GO
GRANT CONTROL SERVER TO UsRolServ;
GO
DENY ALTER ANY SERVER ROLE TO UsRolServ;
DENY ALTER ANY LOGIN TO UsRolServ;
DENY ALTER ANY DATABASE TO UsRolServ;
    
```

Рисунки 4 и 5. Создание имен входа. Настройка разрешений для роли UsRolServ

Протестируем настроенные права выполнив четыре действия: создание серверной роли, создание имени входа, создание БД и включение кода SQLCLR в экземпляре. Первые три действия не будут выполняться из-за отмены разрешений, но четвертое будет выполнено, так как данное разрешение не было запрещено, а выданное разрешение CONTROL SERVER позволяет изменять системные параметры.

```

CREATE SERVER ROLE testRole;
CREATE LOGIN testLogin WITH PASSWORD = 'AK81*9fwy/xvH';
CREATE DATABASE testDatabase;
EXEC SP_CONFIGURE 'show advanced options', '1';
GO
RECONFIGURE;
GO
EXEC SP_CONFIGURE 'clr enabled', '1'
GO
RECONFIGURE;
GO
    
```

Messages

```

Msg 15247, Level 16, State 1, Line 1
User does not have permission to perform this action.
Msg 15247, Level 16, State 1, Line 2
User does not have permission to perform this action.
Msg 262, Level 14, State 1, Line 3
CREATE DATABASE permission denied in database 'master'.
Msg 15247, Level 16, State 1, Procedure sp_configure, Line 105
User does not have permission to perform this action.
Msg 5812, Level 14, State 1, Line 6
You do not have permission to run the RECONFIGURE statement.
Msg 15247, Level 16, State 1, Procedure sp_configure, Line 112
User does not have permission to perform this action.
Msg 5812, Level 14, State 1, Line 10
You do not have permission to run the RECONFIGURE statement.
    
```

Рисунок 6. Тестирование разрешений пользователя teacher

Ввиду того, что teacher не добавлено к роли UsRolServ, оно является обычным именем входа без расширенных прав, и происходит откат транзакций, как показано на рисунке 7. Используя этот тест в качестве контрольного можно убедиться, что базовый пользователь не имеет никаких разрешений на уровне сервера. Далее повторим процесс, но с именем входа director, которое было добавлено к роли UsRolServ.

```

CREATE SERVER ROLE testRole;
CREATE LOGIN testLogin WITH PASSWORD = 'AK81*9%fwy/xvH';
CREATE DATABASE testDatabase;
EXEC SP_CONFIGURE 'show advanced options', '1';
GO
RECONFIGURE;
GO
EXEC SP_CONFIGURE 'clr enabled', '1'
GO
RECONFIGURE;
GO
    
```

100 %

Messages

Msg 15247, Level 16, State 1, Line 1
User does not have permission to perform this action.

Msg 15247, Level 16, State 1, Line 2
User does not have permission to perform this action.

Msg 262, Level 14, State 1, Line 3
CREATE DATABASE permission denied in database 'master'.

Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.

Configuration option 'clr enabled' changed from 1 to 1. Run the RECONFIGURE statement to install.

Рисунок 7. Тестирование разрешений пользователя director роли UsRolServ

Теперь, при выполнении первых трех инструкции по-прежнему происходит откат, но код SQLCLR успешно включается

Данный пример (хотя и искусственный) показывает, что можно сделать с детальными разрешениями на уровне сервера. Можно начинать с минимума разрешений необходимых пользователям для выполнения работы и по мере необходимости повышать права. Вместо того что бы действовать наоборот и изначально разрешать все, а потом отзывать отдельные

Теперь рассмотрим преимущества детальных разрешений на уровне БД. Созданное в предыдущем примере имя входа teacher сопоставим с именем входа в базе данных TeacherBD. Затем определим пользовательскую роль уровня БД teachEntry и добавим к ней пользователя teacher

```

USE teacherBD;
GO
CREATE USER teacher FOR LOGIN teacher;
GO
CREATE ROLE teachEntry AUTHORIZATION dbo;
ALTER ROLE teachEntry ADD MEMBER teacher;
GO
    
```

Рисунок 8. Создание пользователя и роли БД

Далее настроим разрешения. Дадим разрешения на выполнение инструкций INSERT и UPDATE для таблиц dbo.discipline и dbo.teacher, а также на инструкцию SELECT для таблицы dbo.discipline. Использование последней позволяет показать, как можно управлять действиями с данными на детальном уровне.

```

GRANT INSERT ON dbo.teacher TO teachEntry;
GRANT UPDATE ON dbo.teacher TO teachEntry;
GRANT INSERT ON dbo.discipline TO teachEntry;
GRANT UPDATE ON dbo.discipline TO teachEntry;
GRANT SELECT ON dbo.discipline TO teachEntry;
    
```

Рисунок 9. Настройка разрешений для роли БД

Затем дадим различным объектам разрешения разных типов, назначив разрешение EXECUTE для хранимой процедуры dbo.NumberHour, но запретив такое же разрешение для процедуры dbo.sortFioTeacher. Важно отметить, что если teacher так же состоит и в другой роли, которая имеет разрешение EXECUTE для sortFioTeacher, то он сможет выполнить процедуру. В этом отличие REVOKE от DENY.

```
GRANT EXECUTE ON dbo.NumberHour TO teachEntry;
REVOKE EXECUTE ON sortFioTeacher TO teachEntry;
```

Рисунок 10. Настройка разрешений для роли БД

Проведем тестирование используя код отображенный на рисунке 11 от имени пользователя teacher.

```
-- Блок 1
INSERT INTO dbo.teacher (id, fio, designation, grade)
VALUES (6, 'Иванов Иван Иванович', 'Профессор', 'Доктор наук');
-- Блок 2
SELECT * FROM dbo.teacher WHERE id = 6;
-- Блок 3
INSERT INTO dbo.discipline (id, name)
VALUES (7, 'Открытые информационные системы');
-- Блок 4
SELECT * FROM dbo.discipline WHERE id = 3;

-- Блок 5
INSERT INTO dbo.curriculum (id, hours)
VALUES (7, 108);
GO
-- Блок 6
DECLARE @rc INT;
EXECUTE @rc = dbo.NumberHour 100;
GO
-- Блок 7
DECLARE @rc INT;
EXECUTE @rc = dbo.sortFioTeacher 0;
GO
```

Results Messages

(1 row(s) affected)
 Msg 229, Level 14, State 5, Line 5
 The SELECT permission was denied on the object 'teacher', database 'teacherBD', schema 'dbo'.
 (1 row(s) affected)
 (1 row(s) affected)
 Msg 229, Level 14, State 5, Line 12
 The INSERT permission was denied on the object
 (4 row(s) affected)
 Msg 229, Level 14, State 5, Procedure sortFioTeacher,
 The EXECUTE permission was denied on the object 'sortFioTeacher', database 'teacherBD', schema 'dbo'.

id	name	id_t
1	3	Информатика

name	hours
1 Информатика	216
2 Информационная теория управления	108
3 Управление данными	108
4 Упрвление информационными проектами и ресурсами	108

Рисунок 11. Тестирование разрешений пользователя teacher на уровне БД

Блок 1 завершается успешно, так как teacher имеет разрешение INSERT для таблицы UnitMeasure, но блок 2 завершается неудачно из-за отсутствия разрешения SELECT. Блоки 3 и 4 завершаются успешно, так как роль имеет разрешения INSERT и SELECT для таблицы ProductCategory. Блок 5 завершается неудачей, поскольку роль вообще не имеет разрешений для таблицы HumanResources.Department. Блок 6 успешен, так как роль имеет разрешение EXECUTE для хранимой процедуры NumberHour, но блок 7 завершается неудачей, потому что разрешения для процедуры sortFioTeacher были отозваны ранее.

Анализ метаданных о доступных разрешениях позволяет получить полезную информацию для настройки прав. На рисунке 12 показано несколько

способов доступа к ним. При выполнении первой транзакции выводятся разрешения, которые имеются у роли teacherEntry в базе данных teacherBD. С помощью трех остальных транзакций выводится список всех встроенных разрешений в экземпляре сервера, всех разрешений на уровне сервера и всех на уровне БД используя функцию функцию sys.fn_builtin_permissions.

```
USE teacherBD;
GO
SELECT DB_NAME() AS 'Database', p.name, p.type_desc, dbp.state_desc,
dbp.permission_name, so.name, so.type_desc
FROM sys.database_permissions dbp
LEFT JOIN sys.objects so ON dbp.major_id = so.object_id
LEFT JOIN sys.database_principals p ON dbp.grantee_principal_id = p.principal_id
WHERE p.name = 'teacherEntry'
ORDER BY so.name, dbp.permission_name;
SELECT * FROM sys.fn_builtin_permissions(DEFAULT);
SELECT * FROM sys.fn_builtin_permissions('SERVER') ORDER BY permission_name;
SELECT * FROM sys.fn_builtin_permissions('DATABASE') ORDER BY permission_name;
```

Results

Messages

	Database	name	type_desc	state_desc	permission_name	name	type_desc
1	teacherBD	teachEntry	DATABASE_ROLE	GRANT	INSERT	discipline	USER_TABLE
2	teacherBD	teachEntry	DATABASE_ROLE	GRANT	SELECT	discipline	USER_TABLE
3	teacherBD	teachEntry	DATABASE_ROLE	GRANT	UPDATE	discipline	USER_TABLE
4	teacherBD	teachEntry	DATABASE_ROLE	GRANT	EXECUTE	NumberHour	SQL_STORED_PROCEDURE
5	teacherBD	teachEntry	DATABASE_ROLE	GRANT	INSERT	teacher	USER_TABLE
6	teacherBD	teachEntry	DATABASE_ROLE	GRANT	UPDATE	teacher	USER_TABLE

	class_desc	permission_name	type	covering_permission_name	parent_class_desc	parent_covering_permission_name
1	DATABASE	CREATE TABLE	CRTB	ALTER	SERVER	CONTROL SERVER
2	DATABASE	CREATE VIEW	CRVW	ALTER	SERVER	CONTROL SERVER
3	DATABASE	CREATE PROCEDURE	CRPR	ALTER	SERVER	CONTROL SERVER
4	DATABASE	CREATE FUNCTION	CRFN	ALTER	SERVER	CONTROL SERVER
5	DATABASE	CREATE RULE	CRRU	ALTER	SERVER	CONTROL SERVER
6	DATABASE	CREATE DEFAULT	CRDF	ALTER	SERVER	CONTROL SERVER
7	DATABASE	BACKUP DATABASE	BADB	CONTROL	SERVER	CONTROL SERVER
8	DATABASE	BACKUP LOG	BALO	CONTROL	SERVER	CONTROL SERVER

	class_desc	permission_name	type	covering_permission_name	parent_class_desc	parent_covering_permission_name
1	SERVER	ADMINISTER BULK OPERATIONS	ADBO	CONTROL SERVER		
2	SERVER	ALTER ANY AVAILABILITY GROUP	ALAG	CONTROL SERVER		
3	SERVER	ALTER ANY CONNECTION	ALCO	CONTROL SERVER		
4	SERVER	ALTER ANY CREDENTIAL	ALCD	CONTROL SERVER		
5	SERVER	ALTER ANY DATABASE	ALDB	CONTROL SERVER		

Рисунок 12. Некоторые метаданные разрешений

Заключение

Образованный специалист должен владеть навыками администрирования, для обеспечения высокого уровня защищенности сервера. Используя в СУБД разнообразие субъектов безопасности, объектов безопасности и разрешения позволяют осуществлять детальную настройку сервера. Что позволяет избежать ошибок и сбоев в работе программы, несанкционированного доступа к информации и финансового вреда производству.

Список литературы

1. Министерство образования и науки российской федерации Приказ от 19 сентября 2017 г. n 926 об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 09.03.02 информационные системы и технологии
2. Основная профессиональная образовательная программа направления подготовки: 09.03.02 Информационные системы и технологии Направленность (профиль) подготовки: Системная интеграция и автоматизация информационных процессов Присваиваемая квалификация: "Бакалавр" Формы обучения: очная Год набора: 2017
3. Рабочая программа дисциплины Управление данными Направление подготовки: «09.03.02 Информационные системы и технологии» Профиль: «01 Системная интеграция и автоматизация информационных процессов» Присваиваемая квалификация: "Бакалавр" Формы обучения: очная
4. Электронная документация по SQL Server 2014 - MSDN - Microsoft [Электронный ресурс]. – Режим доступа: [https://msdn.microsoft.com/ru-ru/library/ms130214\(v=sql.120\).aspx](https://msdn.microsoft.com/ru-ru/library/ms130214(v=sql.120).aspx), свободный. — Яз. русский. (дата обращения: 16.03.2019).
5. Windows IT Pro/RE | Издательство «Открытые системы» [Электронный ресурс]. – Режим доступа: <https://www.osp.ru/winitpro> свободный. — Яз. русский. (дата обращения: 16.03.2019).