Частное учреждение образования
«Колледж бизнеса и права»

УТВЕРЖДАЮ
Ведущий методист
колледжа
_____ Е.В. Паскал
«___»_____2022

Специальность: «Программное обеспечение информационных технологий»	Учебная дисциплина: «Базы данных и системы управления базами данных»

ЛАБОРАТОРНАЯ РАБОТА № 25

Инструкционно-технологическая карта

Тема: Создание пользователей и разграничение прав доступа к базе данных.
Цель работы: научиться создавать пользователей с различными правами доступа к базе данных.
Время выполнения: 2 часа

Содержание работы

1. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ДЛЯ ВЫПОЛНЕНИЯ РАБОТЫ

Пользователь БД (user) – это физическое или юридическое лицо, которое имеет доступ к БД и пользуется услугами информационной системы для получения информации. На каждом этапе развития базы данных (проектирование, реализация, эксплуатация, модернизация и развитие, полная реорганизация) с ней связаны разные категории пользователей.

Существуют различные категории пользователей:

1. Конечные пользователи. Это основная категория пользователей, в интересах которых создается БД. В зависимости от особенностей создаваемой БД круг конечных пользователей может различаться. Это могут быть случайные пользователи, которые обращаются за информацией к БД время от времени и регулярные пользователи. В качестве случайных пользователей могут рассматриваться, например, клиенты фирмы, просматривающие каталог продукции или услуг. Регулярными пользователями могут быть сотрудники, которые работают со специально разработанными для них программами,

которые обеспечивают автоматизацию их деятельности при выполнении служебных обязанностей.

2. Администратор базы данных (АМД) – это лицо или группа лиц, отвечающих за выработку требований к базе данных, ее проектирование, создание, эффективное использование и сопровождение. В процессе эксплуатации АБД следит за функционированием информационной системы, обеспечивает защиту от несанкционированного доступа, контролирует избыточность, непротиворечивость, сохранность и достоверность хранимой в базе данных информации. Для однопользовательских информационных систем функции АБД обычно возлагаются на лиц, непосредственно работающих с приложением БД.

В вычислительной сети АБД взаимодействует с администратором сети. В его обязанности входит контроль за функционированием аппаратно-программных средств, реконфигурация сети, восстановление программного обеспечения после сбоев и отказов оборудования, профилактические мероприятия и обеспечение разграничения доступа.

3. Разработчики и администраторы приложений. Это группа пользователей, которая функционирует во время проектирования, создания и реорганизации БД. Администраторы приложений координируют работу разработчиков при разработке конкретного приложения или группы приложений, объединенных в функциональную подсистему.

Не в каждой БД могут быть выделены все типы пользователей. При разработке информационных систем с использованием настольных СУБД администратор БД, администратор приложений и разработчик часто существовали в одном лице. Однако при построении современных сложных корпоративных баз данных, которые используются для автоматизации бизнес-процессов в крупной фирме или корпорации, могут существовать и группы администраторов приложений и отделы разработчиков. Наиболее сложные обязанности возложены на группу администратора БД.

База данных взаимодействует в соответствующей среде со множеством пользователей. Пользователи могут предъявлять противоречивые требования к базе данных. Следовательно, возникает проблема координации деятельности пользователей и управления целостностью данных и защитой БД. Необходимость решения этой проблемы вызвало необходимость администрирования в базы данных.

К основным функциям группы администратора БД относят:

1. Анализ предметной области;
2. Проектирование структуры БД;
3. Задание ограниений целостности при описании структуры БД;
4. Первоначальная загрузка и ведение БД;
5. Защита данных;
6. Обеспечерие восстановлени БД;
7. Анализ обращений пользователей: сбор статистики по характеру запросов, времени выполнения;

8. Анализ эфективности функционирования БД: анализ показателей функционирования БД, планирование реструктуризации;

9. Работа с конечными пользователями;

10. Подготовка и поддержание системных средств: анализ существующих на рынке ПС и возможность их использования и др.

11. Организационно-методическая работа по проектированию БД.

Для добавления пользователя в текущую базу данных используется инструкция CREATE USER. Синтаксис этой инструкции выглядит таким образом:

CREATE USER user_name

[FOR {LOGIN login |CERTIFICATE cert_name | ASYMMETRIC KEY key_name}]

[WITH DEFAULT_SCHEMA = schema_name]

Параметр user_name определяет имя, по которому пользователь идентифицируется в базе данных, а в параметре login указывается регистрационное имя, для которого создается данный пользователь. В параметрах cert_name и key_name указываются соответствующий сертификат и асимметричный ключ соответственно. Наконец, в параметре WITH DEFAULT_SCHEMA указывается первая схема, с которой сервер базы данных будет начинать поиск для разрешения имен объектов для данного пользователя базы данных.

Таблица предопределенных роли уровня сервера и их возможностей:

Предопределенная роль уровня сервера	**Описание**
sysadmin	Члены предопределенной роли сервера **sysadmin** могут выполнять любые действия на сервере.
serveradmin	Члены предопределенной роли сервера **serveradmin** могут изменять параметры конфигурации на уровне сервера, а также выключать сервер.
securityadmin	Члены предопределенной роли сервера **securityadmin** управляют именами входа и их свойствами. Они могут предоставлять, запрещать и отменять разрешения на уровне сервера (инструкции GRANT, DENY и REVOKE). Они также могут предоставлять, запрещать и отменять разрешения на уровне базы данных (инструкции GRANT, DENY и REVOKE) при наличии доступа к базе данных. Кроме того, они могут сбрасывать пароли для имен входа SQL Server. ○ *Примечание:* Возможность предоставления доступа к компоненте Database Engine и настройки разрешений пользователей позволяет администратору безопасности назначать большинство разрешений сервера. Роль **securityadmin** должна считаться эквивалентной роли **sysadmin**.
processadmin	Члены предопределенной роли сервера **processadmin** могут завершать процессы, выполняемые на экземпляре SQL Server.
setupadmin	Члены предопределенной роли сервера **setupadmin** могут добавлять или удалять связанные серверы с помощью инструкций Transact-SQL. (При использовании Management Studio необходи-

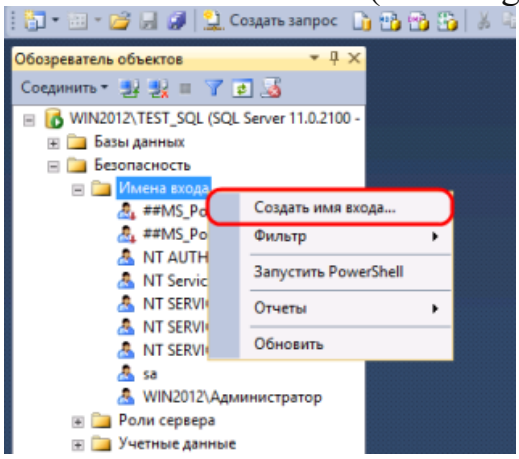
	мо членство в роли **sysadmin**.)
bulkadmin	Члены предопределенной роли сервера **bulkadmin** могут выполнять инструкцию BULK INSERT.
diskadmin	Предопределенная роль сервера **diskadmin** используется для управления файлами на диске.
dbcreator	Члены предопределенной роли сервера **dbcreator** могут создавать, изменять, удалять и восстанавливать любые базы данных.
public	Каждое имя входа SQL Server принадлежит к роли сервера **public**. Если для участника на уровне сервера не были предоставлены или запрещены конкретные разрешения на защищаемый объект, то он наследует разрешения роли **public** на этот объект. Разрешения роли **public** следует назначать только тому объекту, который будет доступен всем пользователям. Нельзя изменить членство в роли **public**. ○ *Примечание:* Роль **public** реализована не так, как другие роли. Однако разрешения для роли **public** могут быть назначены, запрещены или отозваны.

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить теоретическую часть настоящей инструкционно-технологической карты.
2. Рассмотреть работу по созданию пользователя, описанную в разделе «Примеры выполнения работы» настоящей инструкционно-технологической карты.
3. Получить у преподавателя индивидуальное задание и выполнить лабораторную работу в соответствии с вариантом задания согласно описанной в разделе «Пример выполнения работы» методике настоящей инструкционно-технологической карты.
4. Ответить на контрольные вопросы.

3. ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

1. В обозревателе объектов раскрываем вкладку «*Безопасность*» (Security), кликаем правой кнопкой мыши по вкладке «*Имена входа*» (Logins) и в контекстном меню выбираем «*Создать имя входа…*» (New Login…)



2. Откроется окно создания имени входа (Login — New). Теперь необходимо определиться с вариантом аутентификации нового пользователя. Возможны 2 варианта:

– Аутентификация с помощью пароля — Проверка подлинности SQL Server (SQL Server Authentication).

– Доступ для конкретного пользователя Windows — Проверка подлинности Windows (Windows authentication).

Проверка подлинности SQL Server

Для начала рассмотрим первый способ аутентификации. Например, создадим пользователя для работы сервера 1С:Предприятие. Укажем имя входа (Login name), выберем «Проверка подлинности SQL Server» (SQL Server Authentication) и введем пароль (Password) пользователя. Далее снимаем / отмечаем галочки у следующих параметров:

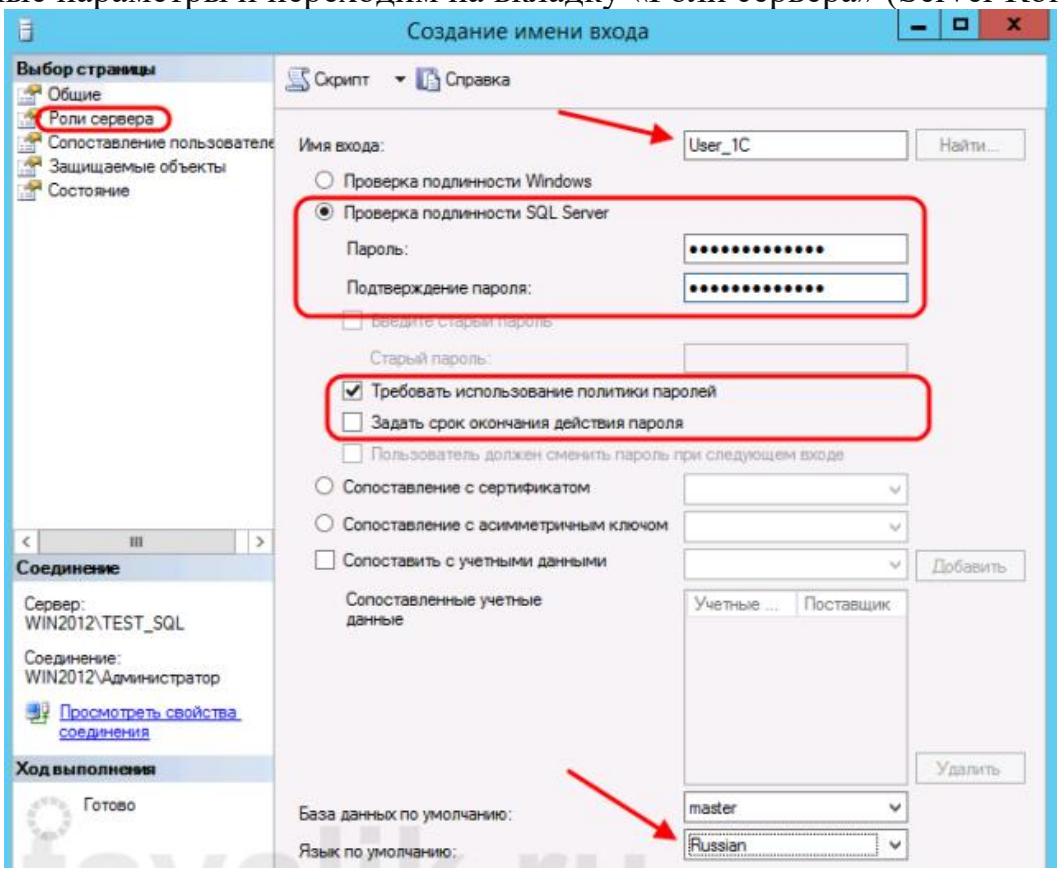
– Требовать использование политики паролей (Enforce password policy)

– Задать срок окончания действия пароля (Enforce password expiration)

– Пользователь должен сменить пароль при следующем входе (User must change password at next login)

– Для данной задачи оставляем включенным только первый параметр.

Также сразу рекомендуется выбрать язык по умолчанию. Устанавливаем необходимые параметры и переходим на вкладку «Роли сервера» (Server Roles).

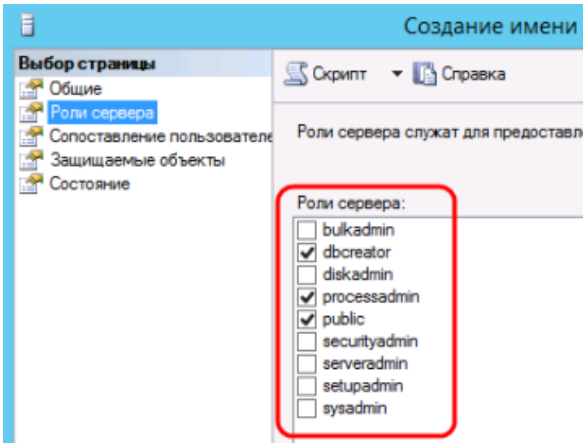


Если вы используете английскую версию SQL Server, то и служебные сообщения, которые SQL Server будет передавать приложению, подключенному под данным пользователем (в данном случае программе 1С:Предприятие, следовательно и конечному пользователю, работающему в программе) будут передаваться на английском языке. Если язык по умолчанию для пользователя выбрать,

например, русский, то и служебные сообщения будут передаваться на русском языке. Здесь выбираем набор прав добавляемого пользователя. Для этого отмечаем необходимые роли сервера.

Для текущей задачи выбираем:

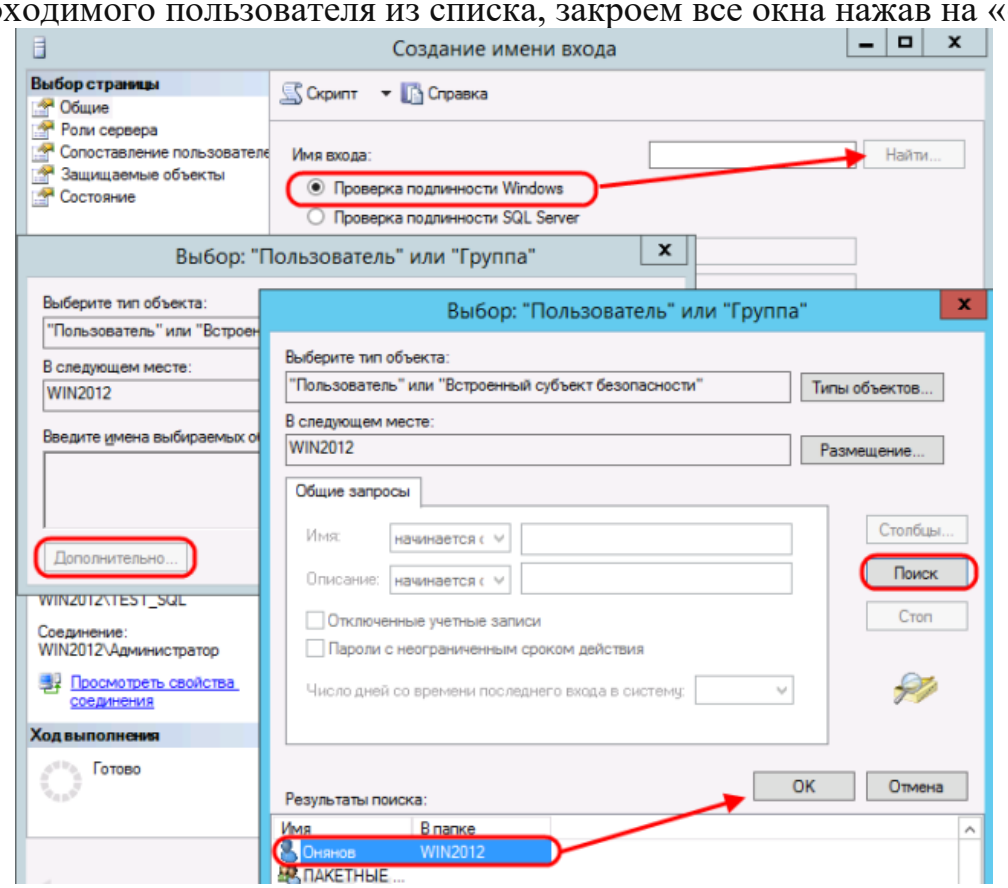
- dbcreator
- processadmin
- public



После чего нажимаем «*ОК*» для сохранения выполненных действий.

Проверка подлинности Windows

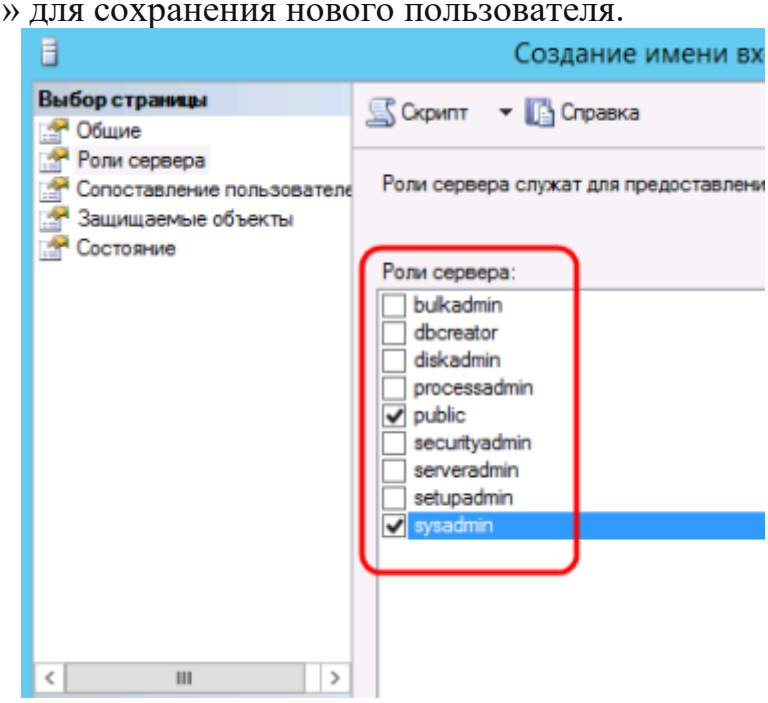
Теперь добавим администратора SQL Server, выбрав его из текущих пользователей Windows. Для этого создадим нового пользователя и способ аутентификации укажем «*Проверка подлинности Windows*» (Windows authentication). Далее, чтобы ввести имя входа, нажмем «*Найти*» (Search…), затем «*Дополнительно*» (Advanced…), в следующем окне «*Поиск*» (Find Now) и выбрав необходимого пользователя из списка, закроем все окна нажав на «*ОК*».



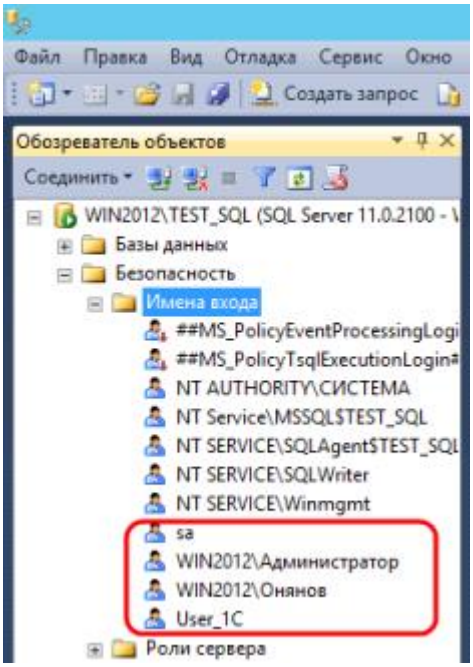
Перейдем на вкладку «*Роли сервера*» (Server Roles) и в соответствии с поставленной задачей укажем роли:

- public
- sysadmin

Нажмем «*ОК*» для сохранения нового пользователя.



Теперь в списке имен входа среди прочих мы можем увидеть только что созданных пользователей.



4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Дайте определение понятия «пользователь».
2. Какие пользователи бывают?
3. Назовите основные функциям группы администратора БД.

4. Назовите роли уровня сервера и их возможности.

5. ЛИТЕРАТУРА

1. Петкович, Д. Microsoft SQL Server 2012. Руководство для начинающих: пер. с английского / Д. Петкович. – СПб.: БХВ-Петербург, 2013. – 816 с.: ил.

2. Сеть разработчиков Microsoft [Электронный ресурс]. – Режим доступа: https://msdn.microsoft.com/ru-ru/library

Преподаватель В.Ю.Купцова

Рассмотрено на заседании цикловой
комиссии программного обеспечения
информационных технологий №10
Протокол № __ от «___»_____2022
ПредседательЦК В.Ю.Михалевич