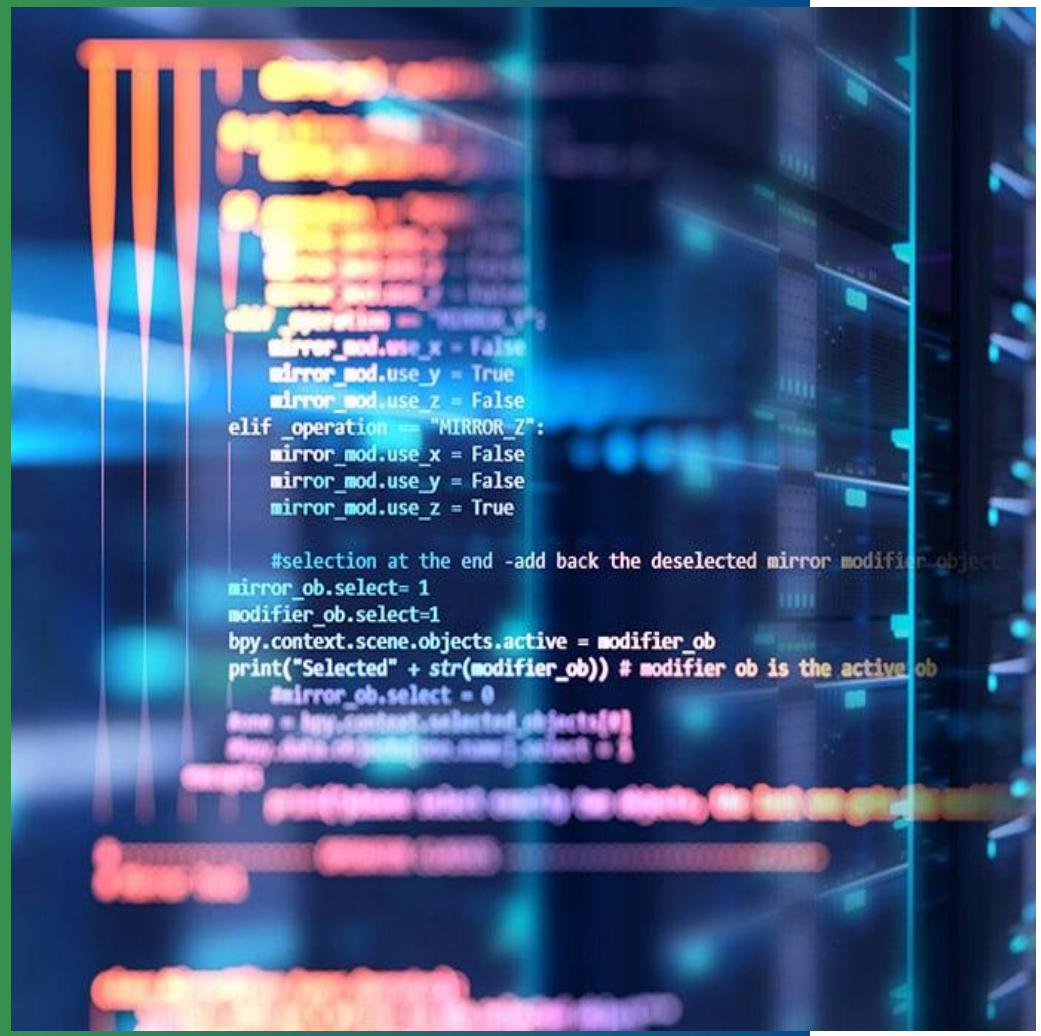


PROАГРО ЛЕКТОРИЙ

Хранимые процедуры, триггеры. Защита информации в базах данных

Быстренина Ирина Евгеньевна,
кандидат педагогических наук, доцент кафедры прикладной информатики РГАУ-МСХА имени К. А. Тимирязева

Хранимые процедуры

Хранимая процедура – это объект базы данных, который представляет собой программу, манипулирующую данными.

SQL сервере хранимые процедуры реализуют динамические запросы, выполняемые на стороне сервера.

Структура хранимой процедуры:

```
CREATE PROCEDURE <Имя процедуры>
[@<Параметр1> <Тип1>]=[<Значение1>],
[@<Параметр2> <Тип2>]=[<Значение2>],…]
[WITH ENCRYPTION]
AS <Команда SQL>,
```

где:
имя процедуры – имя создаваемой хранимой процедуры,
параметр1, параметр2,…. – параметры, передаваемые в процедуру,
значение1, значение2,…. – значения параметров по умолчанию,
тип1,тип2,…. – типы данных параметров,
WITH ENCRYPTION – шифрование данных,
команды SQL – SQL-запрос, который выполняется при запуске процедуры.

Хранимые процедуры

Локальные и глобальные переменные

- Локальные переменные и параметры в процедуре начинаются с символа @.
- Глобальные переменные начинаются с символов @@.

Объявление переменных

[DECLARE] имя_переменной, тип_переменной [(длина)]

Блок операторов заключается в команды BEGIN … END

Оператор присвоения

SELECT переменная=значение

Запуск хранимой процедуры

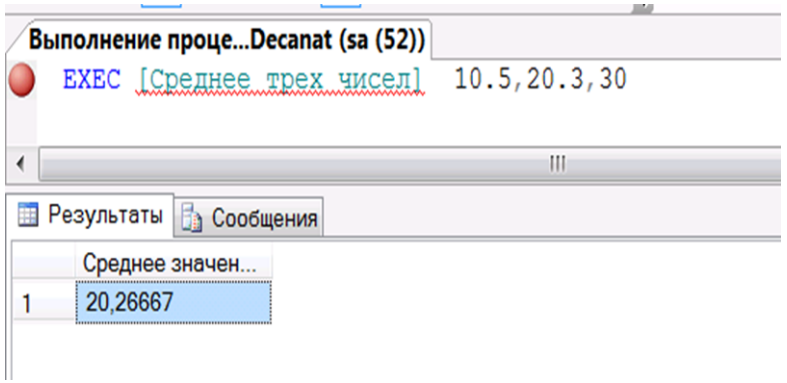
EXEC <имя процедуры> [<параметр1>,<параметр2>,…..]

Хранимые процедуры. Пример

```
CREATE PROCEDURE [Среднее трех чисел]
            @Value1  Real=0,
            @Value2  Real=0,
            @Value3 Real=0
AS
BEGIN
            SELECT ‘Среднее значение равно'=(@Value1+@Value2+@Value3)/3
END
```

Выполнение процедуры

EXEC [Среднее трех чисел] 10.5,20.3,30



Триггеры

Триггеры – это хранимые процедуры специального вида, которые автоматически выполняются при изменении таблицы с помощью операторов INSERT, UPDATE и DELETE. Триггер создается для определенной таблицы, но может использовать данные других таблиц и объекты других баз данных.

Типы триггеров: INSERT, UPDATE и DELETE. Правила работы с триггерами:

- триггеры запускаются только после выполнения вызвавшего их оператора;
- если при выполнении оператора возникает нарушение какого-либо ограничения или другая ошибка, триггер не срабатывает (даже не начинает выполняться);
- триггер и вызвавший его оператор образует транзакцию. Если нужно из триггера отменить вызвавшую его операцию, следует выполнить откат транзакции ROLLBACK;
- триггер срабатывает один раз для каждого оператора, независимо от количества изменяемых им записей.

Триггеры

Структура триггера

```
CREATE TRIGGER <имя_триггера>
        ON <имя_таблицы>
FOR INSERT | UPDATE | DELETE AS
Код_триггера
```

Пример. Триггер, выводящий сообщение о том, что запись добавлена при добавлении записи в таблицу *Disciplines*.

```
CREATE TRIGGER [Insert_Trigger_Disciplines]
   ON [Disciplines]
   AFTER INSERT
AS
BEGIN
        PRINT ('Запись в таблицу Disciplines добавлена');
END
```

Защита информации в базах данных

Безопасность информационной системы — свойство, заключающееся в способности системы обеспечить конфиденциальность и целостность информации, т.е. защиту информации от несанкционированного доступа, обращенного на ее раскрытие, изменение или разрушение.

Все угрозы информационным системам и, соответственно, базам данных можно объединить в три группы:

- **Угроза раскрытия** — возможность того, что информация станет известной тому, кому не следовало бы ее знать;
- **Угроза целостности** — умышленное несанкционированное изменение (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую;
- **Угроза отказа в обслуживании** — опасность появления блокировки доступа к некоторому ресурсу вычислительной системы.

Защита информации в базах данных

Исходя из возможных угроз безопасности можно выделить три основные задачи защиты информации:

Защита информации от хищения – предотвращение физического хищения устройств и носителей хранения информации, несанкционированного получения информации (копирования, подсмотра, перехвата и т.д.) и несанкционированного распространения программ и информации.

Защита информации от потери – поддержание целостности и корректности информации, что означает обеспечение физической, логической и семантической целостности информации. Информация в системе может быть потеряна как в случаях несанкционированного доступа в систему пользователей, программ (в том числе и компьютерных вирусов), некорректныхдействий пользователей и их программ, обслуживающего персонала, так и в случаях сбоев и отказов в сети.

Защита информации в базах данных

Защита от сбоев и отказов аппаратно-программного обеспечения сети является одним из необходимых условий нормального функционирования системы. Если вычислительная система является ненадежной, информация в ней часто искажается и иногда утрачивается. Основная нагрузка на обеспечение хорошей защиты от сбоев и отказов в системе ложится на системные аппаратно-программные компоненты: процессор, основную память, внешние запоминающиеся устройства ввода-вывода и другие устройства, а также программы операционной системы. При недостаточно надежных системных средствах защиту от сбоев следует предусматривать в прикладных программах.

Надежность информационного обеспечения – способность точно и своевременно выполнять возложенные на пего функции.

Защита информации в базах данных

Средства обеспечения информационной безопасности

- **организационные методы** – рациональное конфигурирование, организация и администрирование системы. В первую очередь это касается сетевых информационных систем, операционных систем, полномочий сетевого администратора, набора обязательных инструкций, определяющих порядок доступа и работы в сети;
- **технологические методы**, включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации;

Защита информации в базах данных

Средства обеспечения информационной безопасности

- аппаратные методы, реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т.д.;
- программные методы — это самые распространенные методы защиты информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры и т.д.). Без использования программной составляющей практически невыполнимы никакие, в том числе и первые три группы методов. При этом стоимость реализации многих программных системных решений по защите информации существенно превосходит по затратам аппаратные, технологические и тем более организационные решения.

PROАГРО
ЛЕКТОРИЙ

Спасибо за внимание!