РОССИЙСКАЯ ФЕДЕРАЦИЯ МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ФГАОУ ВО ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нестерова О. А.

БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

ТЮМЕНЬ 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Целью дисциплины «Безопасность систем баз данных» является формирование у студентов комплекса профессиональных качеств, обеспечивающих решение задач, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных (СУБД), а также связанных с обеспечением безопасности информации в автоматизированных информационных системах (АИС), в основе которых лежат базы данных (БД), навыки работы со встроенными средствами безопасности систем управления базами данных (СУБД).

Задачей курса является:

- обучение студентов принципам работы современных систем управления базами данных;
- прививание студентам навыков проектирования и реализации баз данных;
- приобретение системного подхода к проблеме защиты информации в СУБД;

Изучение курса основано на следующих дисциплинах: «Базы данных», «Информационные технологии», «Языки программирования», «Технологии и методы программирования».

В результате изучения дисциплины студенты должны знать:

- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- современные критерии и стандарты для анализа безопасности информационных систем на базе СУБД;

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- применять действующую законодательную базу в области обеспечения безопасности систем баз данных;
- применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы;

Тема 1. БЕЗОПАСНОСТЬ БД, УГРОЗЫ, ЗАЩИТА

Структурированная и систематизированная информация, размещенная в управляемых базах данных (СУБД), расположенных на выделенных серверах, легче обрабатывается и анализируется, а также используется при построении бизнес-процессов. Для киберпреступников она представляет больший интерес, чем неструктурированная информация в разрозненных файлах и кратковременной памяти. Поэтому основными задачами по обеспечению безопасности являются:

- защита информации от несанкционированного доступа инсайдеров или внешних заинтересованных сторон;
- предотвращение уничтожения данных. Механизмы современной СУБД (Database Management System) способны вычислять частично стертую и поврежденную информацию и исправлять ошибку, поэтому речь идет об обеспечении безопасности от рисков полного уничтожения содержимого базы данных;
- защита от программных и аппаратных ошибок, трудностей с доступом к серверу, которые затрудняют или делают невозможным обработку пользователями информации, содержащейся в базах данных.

Построение эффективной системы безопасности базы данных потребует оценки угроз на основе ценности информации и практики криминального посягательства на данные, сложившейся в сфере ее распространения. Так, одни инструменты используются для базы данных НИИ, а другие - для баз данных интернет-провайдеров. Среди основных:

- несанкционированное использование информации в базе данных системными администраторами, пользователями, хакерами;
- вирусные атаки с различными последствиями;
- SQL-инъекции, которые произвольно изменяют код или переформатируют базу данных;

- технические проблемы, снижение производительности, отказ в доступе, исключение возможности использования информации;
- физический ущерб, нанесенный оборудованию или каналам связи;
- ошибки, недоработки, несанкционированные функции в программах, управляющих базами данных и другим программным обеспечением, операционные системы являются наиболее уязвимыми.

Это наиболее распространенные угрозы, с которыми необходимо бороться, чтобы обеспечить информационную безопасность баз данных.

Первой задачей по обеспечению безопасности базы данных является разграничение прав доступа и определение привилегий, которые позволяют системным администраторам осуществлять контроль, а пользователям - получать доступ к данным.

Есть два типа привилегий:

- системные привилегии;
- объектные привилегии.

Системные позволяют администратору выполнять управленческие действия в отношении базы данных и содержащихся в ней информационных объектов. Так, например, указано для СУБД SQL Server, создание:

- процедуры разграничения или обработки информации;
- представления;
- резервной БД;
- таблицы;
- триггера.

Вопросы для подготовки

1. Понятие безопасности БД.
2. Угрозы безопасности БД: общие и специфичные.
3. Требования безопасности БД.

4. История развития, назначение и роль баз данных.
5. Модели данных.
6. Математические основы построения реляционных СУБД.

Лабораторная работа №1

Построить реляционную БД. Написать запросы на соединение таблиц. Создать клиентское приложение для работы с базой данных.

Тема 2. КРИТЕРИИ ЗАЩИЩЕННОСТИ БД

Защита информации — это комплекс мер, направленных на обеспечение информационной безопасности (целостность, доступность и, при необходимости, конфиденциальность информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Защищенная информация (конфиденциальная информация) - информация, которая является предметом собственности и подлежит защите в соответствии с требованиями правовых документов или требованиями, установленными владельцем информации. Очень часто наряду с термином «защищенная информация» используется также термин «конфиденциальная информация» - информация, доступ к которой ограничен в соответствии с законодательством или требованиями владельца.

Конфиденциальность — это свойство которое определяет, что информация должна быть известна только авторизованным и проверенным субъектам системы.

Защищенная информационная система - система, предназначенная для обработки защищенной информации с требуемым уровнем ее безопасности.

Система считается безопасной, если она, используя соответствующее оборудование и программное обеспечение, контролирует доступ к информации, так что только должным образом уполномоченным лицам или процессам, действующим от их имени, разрешено читать, записывать, создавать и удалять информацию. Система считается надежной (в противном случае - доверенной), если она, используя достаточное оборудование и программное обеспечение, обеспечивает одновременную обработку информации различной степени секретности группой пользователей без нарушения прав доступа.

Основными критериями оценки надежности являются политика безопасности и гарантии.

Политика безопасности — это качественное описание комплекса организационных, технологических и программно-аппаратных мер по обеспечению защиты данных, включая анализ возможных угроз и выбор соответствующих мер противодействия. Политика безопасности, являясь активным компонентом защиты, отражает совокупность законов, правил и норм поведения, которые конкретная организация использует при обработке, защите и распространении информации. Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии с сформулированной политикой безопасности.

Гарантия, являясь пассивным элементом защиты, отражает меру доверия, которую можно придать архитектуре и реализации системы (другими словами, она показывает, насколько правильно выбраны механизмы для обеспечения безопасности системы).

Формальное (математическое, алгоритмическое, схематическое) выражение и формулировка политики безопасности называется **моделью безопасности.** Большинство моделей безопасности основаны на субъектно-объектной модели компьютерных систем, включая базы данных как ядро автоматизированных информационных систем. Различаются субъекты (субъекты) базы данных (активные сущности), объекты (объекты) базы данных (пассивные сущности) и процессы, порождаемые действиями субъектов над объектами.

Таким образом, **субъект доступа** — это активный компонент системы, который может вызвать инициализацию информационного потока или изменение состояния системы. **Субъект** — это человек или процесс, действия которых регулируются правилами контроля доступа.

Объект доступа — это пассивный компонент системы, который хранит, принимает или передает информацию, доступ к которой регулируется правилами контроля доступа. Объектами доступа в базе данных являются почти все, что содержит окончательную информацию: таблицы (базовые или

виртуальные), представления, а также более мелкие элементы данных: столбцы и строки таблиц, и даже отдельные поля.

Вопросы для подготовки

1. Критерии оценки надежных компьютерных систем (TCSEC).
2. Понятие политики безопасности.
3. Совместное применение различных политик безопасности в рамках единой модели.
4. Интерпретация TCSEC для надежных СУБД (TDI).
5. Оценка надежности СУБД как компоненты вычислительной системы.

Лабораторная работа №2

Построить модель данных, разработать ограничения целостности для построенной модели. Привести к 5НФ. Рассмотреть соответствие отношений в 5НФ требованиям безопасности в выбранной предметной области.

Тема 3. МОДЕЛИ БЕЗОПАСНОСТИ В СУБД

Метод формальной разработки системы опирается на модель безопасности (модель управления доступом, модель политики безопасности). Цель этой модели - выразить сущность требований безопасности для данной системы. Он определяет потоки информации, разрешенные в системе, и правила контроля доступа к информации.

Модель позволяет анализировать свойства системы, но не накладывает ограничений на реализацию определенных механизмов защиты. Поскольку это формально, можно доказать различные свойства безопасности системы.

Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системы.

Основные концепции, используемые в моделях управления доступом, следующие.

Доступ к информации - ознакомление с информацией, ее обработка, в частности копирование, изменение или уничтожение информации.

Объект доступа — это единица информационного ресурса автоматизированной системы, доступ к которой регулируется правилами контроля доступа.

Субъект доступа — это человек или процесс, действия которых регулируются правилами контроля доступа.

Правила разграничения доступа — это набор правил, регулирующих права доступа субъектов доступа к объектам доступа.

Модель дискреционного доступа

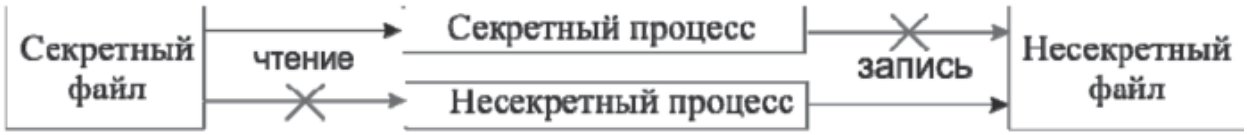
Дискреционная модель контролирует доступ субъектов (пользователей или приложений) к объектам, представляющим различные информационные ресурсы: файлы, приложения, устройства вывода и т. Д.

Для каждого объекта существует субъект-владелец, который сам определяет, кто имеет доступ к объекту, а также разрешенные операции доступа. Основными операциями доступа являются **READ** (чтение), **WRITE**

(запись) и **EXECUTE** (выполнение, имеет смысл только для программ). В модели дискреционного доступа набор разрешенных операций доступа устанавливается для каждой пары субъект-объект.

Модель безопасности Белла-ЛаПадулы

Одна из самых известных моделей безопасности — это модель Белла-ЛаПадулы (модель обязательного контроля доступа). Она определяет множество концепций, связанных с контролем доступа. Даны определения субъекта, объекта и операции доступа, а также математический аппарат для их описания. Эта модель в основном известна двумя основными правилами безопасности, одно относится к чтению, а другое - к записи данных.



Контроль доступа на основе ролей

Ролевой контроль доступа контролирует доступ пользователей к информации на основе типов их действий в системе. Под ролью понимается набор действий и обязанностей, связанных с определенным видом деятельности. Примеры ролей: администратор базы данных, менеджер, руководитель отдела.

В ролевой модели каждый объект связан с набором разрешенных операций доступа для каждой роли, а не для каждого пользователя. Каждому пользователю назначаются роли, которые он может выполнять. В некоторых системах пользователю разрешено выполнять несколько ролей одновременно, в других существует ограничение на одну или несколько неконфликтующих ролей одновременно.

Системы контроля доступа

Конкретный вариант реализации модели управления доступом можно найти в системе управления доступом (СУД). СУД — это набор

реализованных правил для разграничения доступа в компьютерных технологиях или автоматизированных системах.

Вопросы для подготовки

1. Дискреционная (избирательная) и мандатная (полномочная) модели безопасности.
2. Классификация моделей.
3. Аспекты исследования моделей безопасности.
4. Особенности применения моделей безопасности в СУБД.

Лабораторная работа №3

Рассмотреть дискреционную (избирательную) и мандатную (полномочную) модели безопасности. Исследовать применение моделей безопасности. Применить модель безопасности для разработанной БД

Тема 4. СРЕДСТВА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Правила разграничения доступа (security policy) - совокупность правил, регламентирующих права субъектов доступа к объектам доступа. Доступ к информации разделяют на санкционированный и несанкционированный:

Санкционированный доступ (authorized access to information) - доступ к информации, который не нарушает установленных правил разграничения доступа, а **несанкционированный доступ** (unauthorized access to information) - доступ к информации, который нарушает установленные правила разграничения.

Контроль доступа обязательно включает **идентификацию и аутентификацию** всех субъектов и их процессов и разграничение полномочий субъектов по отношению к объектам с последующей обязательной проверкой введенных полномочий.

Идентификация (identification) - присвоение объектам и субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификатор доступа (access identifier) - уникальный признак объекта или субъекта доступа.

Аутентификация (authentication) - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Тем самым, задача идентификации – ответить на вопрос «кто это?», а задача аутентификации – «а он ли это на самом деле». После идентификации и проверки подлинности устанавливается сфера действий субъекта. Эту процедуру называют предоставлением полномочий (авторизацией).

Авторизация (authorization) — это предоставление прав (или привилегий), позволяющих их владельцу иметь законный доступ к системе или ее объектам. Иногда в процесс авторизации включает и идентификацию, и аутентификацию субъектов, требующих получения доступа к объектам.

Привилегия доступа (уровень полномочий субъекта доступа) (subject privilege) - совокупность прав доступа субъекта доступа.

Вопросы для подготовки

1. Общие сведения. Идентификация и аутентификация.
2. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС.

Лабораторная работа №4

Аутентификация на уровне ОС и на уровне СУБД. Создать имена вход и пользователей базы данных. Изучить олицетворение.

1. **Для доступа к SQL Server создайте 4 учетные записи (логины):** «Администратор БД», «Сотрудник отдела кадров», «Сотрудник отдела продаж», «Сотрудник отдела поставок»;
2. **Учетную запись «Администратор» наделите привилегиями системного администратора (с помощью системной роли);**
3. **Напишите SQL-скрипты для получения следующей информации:**

- Секретный идентификатор, имя, хэш пароля определенной учетной записи;
- Список всех учетных записей сервера;
- Список всех учетных записей сервера, обладающих правами администратора;

4. **Напишите SQL-скрипты для выполнения следующих действий с учетной записью SQL-сервера:**

- Блокировка учетной записи (временное приостановление действия);
- Разблокировка учетной записи;
- Изменение пароля учетной записи;
- Изменение БД по умолчанию;
- Удаление учетной записи;

5. **Напишите SQL-скрипты для выполнения следующих действий с учетной записью операционной системы (ОС):**

- Регистрация учетной записи ОС в качестве учетной записи в MS SQL Server;
- Отмена регистрации учетной записи ОС в качестве учетной записи в MS SQL Server;
- Запрет подключений учетной записи ОС в качестве учетной записи в MS SQL Server;

6. Для каждой учетной записи, созданной в 1 пункте, кроме «Администратор БД» добавьте пользователя в вашу БД (AdventureWorks2008R2);

Тема 5. СРЕДСТВА УПРАВЛЕНИЯ ДОСТУПОМ

Управление доступом есть метод защиты информации путем регулирования использования ресурсов системы (элементов БД, программных и технических средств). Включает следующие функции защиты:

- идентификация пользователей и ресурсов системы;
- установление подлинности объекта или субъекта по предъявленному им идентификатору (аутентификация);
- разграничение и проверка полномочий (авторизация). Создание условий работы в пределах установленного регламента;
- регистрация обращений к защищаемым ресурсам (протоколирование и аудит);
- реагирование при попытках несанкционированного доступа.

Вопросы для подготовки

1. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления.
2. Виды привилегий: привилегии безопасности и доступа.
3. Использование ролей и привилегий пользователей.
4. Соотношение прав доступа, определяемых ОС и СУБД.
5. Использование представлений для обеспечения конфиденциальности информации в СУБД.
6. Средства реализации мандатной политики безопасности в СУБД.

Лабораторная работа №5

Изучить встроенные роли уровня сервера и базы данных. Создать пользовательские роли и привилегии пользователей. Создать представление для обеспечения конфиденциальности информации в СУБД. Использовать средства реализации политик безопасности в СУБД

Тема 6. ЦЕЛОСТНОСТЬ БД И СПОБОСЫ ЕЁ ОБЕСПЕЧЕНИЯ

Под целостностью данных понимают соответствие информационной модели предметной области, т. е. данных, хранимых в базе данных, объектам реального мира и их взаимосвязям в каждый момент времени. Любое изменение в предметной области, значимое для построенной модели, должно отражаться в базе данных, и при этом должна сохраняться однозначная интерпретация информационной модели в терминах предметной области. Целостность БД не гарантирует достоверности содержащейся в ней информации, но обеспечивает по крайней мере правдоподобность этой информации, отвергая заведомо невероятные, невозможные значения. Таким образом, не следует путать целостность БД с достоверностью данных. Достоверность (или истинность) есть соответствие фактов, хранящихся в БД, реальному миру.

Контроль целостности данных — это способность СУБД в целом обеспечить неизменность данных (данные, хранящиеся в системе, не отличаются в семантическом отношении от данных в исходных документах) в условиях случайного и (или) преднамеренного искажения (разрушения) или, иначе, под целостностью данных подразумевает отсутствие ненадлежащих изменений.

Определены девять абстрактных теоретических принципов, выполнение которых позволит обеспечить целостность данных:

- корректность транзакций;
- авторизация пользователей;
- минимизация привилегий;
- разграничение функциональных обязанностей;
- аудит произошедших событий;
- объективный контроль;
- управление передачей привилегий;
- эффективное применение механизмов защиты;

- простота использования защитных механизмов.

Вопросы для подготовки

1. Основные виды и причины возникновения угроз целостности.
2. Способы противодействия.
3. Цели использования триггеров.
4. Способы задания, моменты выполнения.
5. Декларативная и процедурная ссылочные целостности.
6. Внешний ключ.
7. Способы поддержания ссылочной целостности.

Лабораторная работа №6

Способы обеспечения целостности БД. Использование триггеров. Применение декларативной и процедурной ссылочные целостности. Способы поддержания ссылочной целостности. Резервное копирование и восстановление базы данных. "Ограничения целостности базы данных". Разработать различные виды механизмов ограничения целостности: структура базы данных, типы, связи, ключи, уникальность, общие ограничения, значения по умолчанию, триггеры.

Тема 7. КЛАССИФИКАЦИЯ УГРОЗ КОНФИДЕНЦИАЛЬНОСТИ СУБД

Конфиденциальность (confidentiality или secrecy) — это свойство информации быть известной только допущенным и прошедшим проверку субъектам системы.

К угрозам конфиденциальности информации можно отнести следующие.

1. Инъекция SQL. Во многих приложениях используется динамический SQL – формирование SQL – формирование SQL-предложений кодом программы путем конкатенации строк и значений параметров. Зная структуру базы данных, злоумышленник может либо выполнить хранимую программу в запросе, либо закомментировать «легальные» фрагменты SQL-кода, внедрив, например, конструкцию UNION, запрос которой возвращает конфиденциальные данные. В последнее время злоумышленник может использовать специальные программы, автоматизирующие процесс реализации подобных угроз.

2. Логический вывод на основе функциональных зависимостей. Пусть дана схема отношения: (, ...,). R A1 An. Пусть U = {A1, ..., An}, X, Y – подмножества из U. X функционально определяет Y, если в любом отношении r со схемой) (, ...,) R A1 An не могут содержаться два кортежа с одинаковыми значениями атрибутов из X и с различными из Y. В этом случае имеет место функциональная зависимость, обозначаемая X →Y. В реальных БД при наличии сведений о функциональных зависимостях злоумышленник может вывести конфиденциальную информацию при наличии доступа только к части отношений, составляющих декомпозированное отношение.

3. Логический вывод на основе ограничений целостности. Для кортежей отношений в реляционной модели данных можно задать ограничения целостности – логические условия, которым должны удовлетворять атрибуты кортежей. При этом ограничение целостности может быть задано в виде предиката на всем множестве атрибутов кортежа. В случае

попытки изменить данные в таблице, СУБД автоматически вычисляет значение этого предиката, и в зависимости от его истинности операция разрешается или отвергается. Многократно изменяя данные и анализируя реакцию системы, злоумышленник может получить те сведения, к которым у него нет непосредственного доступа. К этому виду угроз можно отнести также анализ значений первичных/вторичных ключей.

4. Использование оператора UPDATE для получения конфиденциальной информации. В некоторых стандартах SQL пользователь, не обладая привилегией на выполнение оператора SELECT, мог выполнить оператор UPDATE со сложным логическим условием. Так как после выполнения оператора UPDATE сообщается, сколько строк он обработал, фактически пользователь мог узнать, существуют ли данные, удовлетворяющие этому условию.

Вопросы для подготовки

1. Причины, виды, основные методы нарушения конфиденциальности.
2. Типы утечки конфиденциальной информации из СУБД, частичное разглашение.
3. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.
4. Методы противодействия.
5. Особенности применения криптографических методов

Лабораторная работа №7

Управление доступом к базе данных. Настроить разрешения для пользователей и имен входов. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия.

1. **Используя роли и привилегии каждому пользователю назначьте следующие права:**

1.1. «Сотрудник отдела продаж»:

a. разрешение на добавление, изменение, удаление данных о сотрудниках компании Adventure Works Cycles;
b. запрет на просмотр, изменение и удаление данных продукции, продаж и поставок;

1.2. «Сотрудник отдела продаж»:

a. разрешение на добавление, изменение, удаление данных о заказчиках и продажах;
b. разрешение на просмотр данных о продукции, поставщиках и поставках;
c. запрет на изменение и удаление данных о продукции, поставщиках и поставках;

1.3. «Сотрудник отдела поставок»:

a. разрешение на добавление, изменение, удаление данных о поставщиках и поставках;
b. разрешение на изменение информации о количестве продукции на складе компании;
c. для данных о продукции - разрешение на просмотр и запрет на изменение и удаление;
d. запрет на просмотр, изменение и удаление данных о сотрудниках и продажах;

2. Напишите SQL-скрипты для получения следующей информации:

- Все пользователи и все привилегии текущей БД;
- Список всех ролей и пользователей, которым присвоены эти роли;
- Список всех ролей, назначенных текущему пользователю;
- Список привилегий, ассоциированных с какой-то конкретной ролью;

- Список всех привилегий текущего пользователя;

Напишите код запроса с использованием конструкции EXECUTE AS, в ходе которого «Сотрудник отдела поставок» смог бы выполнять запросы от имени пользователя «Сотрудник отдела продаж».

Применение криптографических методов (шифрование в БД). Изучить и применить различные виды шифрования в СУБД.

Тема 8. АУДИТ И ПОДОТЧЕТНОСТЬ

Аудит (регистрация всех обращений к защищаемой информации). Для определения активности использования БД анализируются ее файлы журнала. Эти же источники могут быть использованы для выявления любых необычных действий в системе. Регулярное проведение аудиторских проверок, дополненное постоянным контролем содержимого файлов журнала с целью выявления аномальной активности в системе, очень часто позволяет своевременно обнаружить и пресечь любые попытки нарушения защиты.

Вопросы для подготовки

1. Подотчетность действий пользователя и аудит связанных с безопасностью событий.
2. Регистрация действий пользователя.
3. Управление набором регистрируемых событий.
4. Анализ регистрационной информации.

Лабораторная работа №8

Триггеры безопасности. Журналирование в СУБД. Разработать триггер входа. Изучить механизм аудита.

Тема 9. ТРАНЗАЦИИ И БЛОКИРОВКИ

Транзакции - атомарное действие над БД, переводящего ее из одного целостного состояния в другое целостное состояние. Другими словами, транзакция — это последовательность операций, которые должны быть или все выполнены или все не выполнены (все или ничего).

Методом контроля за транзакциями является ведение журнала, в котором фиксируются все изменения, совершаемые транзакцией в БД. Если во время обработки транзакции происходит сбой, транзакция откатывается - из журнала восстанавливается состояние БД на момент начала транзакции.

В СУБД различных поставщиков начало транзакции может задаваться явно (например, командой BEGIN TRANSACTION), либо предполагаться неявным (так определено в стандарте SQL), т. е. очередная транзакция открывается автоматически сразу же после удачного или неудачного завершения предыдущей. Для завершения транзакции обычно используют команды SQL:

- COMMIT - успешно завершить транзакцию
- ROLLBACK - откатить транзакцию, т. е. вернуть БД в состояние, в котором она находилась на момент начала транзакции.

Стандарт SQL определяет, что транзакция начинается с первого SQL-оператора, инициируемого пользователем или содержащегося в прикладной программе. Все последующие SQL-операторы составляют тело транзакции. Транзакция завершается одним из возможных способов:

- оператор COMMIT означает успешное завершение транзакции, все изменения, внесённые в базу данных, делаются постоянными
- оператор ROLLBACK прерывает транзакцию и отменяет все внесенные ею изменения
- успешное завершение программы, инициировавшей транзакцию, означает успешное завершение транзакции (как использование COMMIT)

- ошибочное завершение программы прерывает транзакцию (как ROLLBACK)

Пример явно заданной транзакции:

```
BEGIN TRANSACTION;              /* Начать транзакцию */
DELETE ...;                     /* Изменения */
UPDATE ...;                     /* данных    */
if (обнаружена_ошибка) ROLLBACK;
else COMMIT;                  /* Завершить транзакцию *
```

Пример неявно заданной транзакции:

```
COMMIT;          /* Окончание предыдущей транзакции */
DELETE ...;                     /* Изменения */
UPDATE ...;                     /* данных    */
if (обнаружена ошибка) ROLLBACK;
else COMMIT;               /* Завершить транзакцию */
```

Принудительное упорядочение транзакций обеспечивается с помощью механизма блокировок. Суть этого механизма в следующем: если для выполнения некоторой транзакции необходимо, чтобы некоторый объект базы данных (кортеж, набор кортежей, отношение, набор отношений,) не изменялся непредсказуемо и без ведома этой транзакции, такой объект блокируется. Основными видами блокировок являются:

- блокировка со взаимным доступом, называемая также S-блокировкой (от Shared locks) и блокировкой по чтению.
- монопольная блокировка (без взаимного доступа), называемая также X-блокировкой от (eXclusive locks) или блокировкой по записи. Этот режим используется при операциях изменения, добавления и удаления объектов.

Вопросы для подготовки

1. Транзакции как средство изолированности пользователей.
2. Сериализация транзакций.
3. Методы сериализации транзакций.
4. Режимы блокировок.
5. Правила согласования блокировок.

6. Двухфазный протокол синхронизационных блокировок.
7. Тупиковые ситуации, их распознавание и разрушение.

Лабораторная работа №9

Применить транзакций как средства изолированности пользователей. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение.

СПИСОК ЛИТЕРАТУРЫ

1. **Мартишин, С. А. Базы данных. Практическое применение СУБД SQL и NoSQL-типа для проектирования информационных систем:** учебное пособие / С.А. Мартишин, В. Л. Симонов, М. В. Храпченко. — Москва: ИД «ФОРУМ»: ИНФРА-М, 2016. — 368 с. — (Высшее образование). - ISBN 978-5-8199-0660-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/556449 (дата обращения: 15.05.2020). – Режим доступа: по подписке
2. **Дадян, Э. Г. Методы, модели, средства хранения и обработки данных:** учебник / Э.Г. Дадян, Ю. А. Зеленков. — Москва: Вузовский учебник: ИНФРА-М, 2017. — 168 с. - ISBN 978-5-9558-0490-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/543943 (дата обращения: 15.05.2020). – Режим доступа: по подписке.
3. **Баранова, Е. К. Информационная безопасность и защита информации:** учеб. пособие / Баранова Е. К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/763644 (дата обращения: 15.05.2020). – Режим доступа: по подписке.

Интернет-ресурсы

1. Вузовские электронно-библиотечные системы учебной литературы.
2. http://www.infosecurity. Report.ru (портал по информационной безопасности).
3. База научно-технической информации ВИНИТИ РАН.
4. Среды разработки на языках C#, C++, Delphi.
5. Порталы разработчиков систем управления базами данных: MS SQL Server, InterBase/FireBird, MySQL, Oracle, SQL Postgre.