Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Основы построения защищённых баз данных

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1.3 Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.

ПК-3 Способен проводить анализ уязвимостей внедряемой системы защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.3.1 Понимает модели и структуры данных, физические модели баз данных, принципы организации и методы проектирования баз данных, языки и системы программирования баз данных.

ИОПК-1.3.2 Понимает общие принципы функционирования компьютерных сетей, протоколы разных уровней модели взаимодействия открытых систем.

ИОПК-1.3.3 Оценивает состояние и эффективность системы безопасности на уровне базы данных, разворачивает и настраивает средства защиты базы данных от несанкционированного доступа.

ИПК-3.1 Проводит анализ уязвимости средств системы защиты информации.

ИПК-3.2 Устраняет выявленные уязвимости системы защиты информации.

ИПК-3.3 Разрабатывает предложения по совершенствованию системы управления защитой информации.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тесты;

– лабораторная работа.

Примеры тестовых вопросов (ИОПК-1.3.1, ИОПК-1.3.2)

Вопрос 1. Утечкой информации в системе называется ситуация, характеризуемая:

a) Потерей данных в системе
b) Изменением формы информации
c) Изменением содержания информации

Вопрос 2. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

a) Целостность
b) Доступность
c) Актуальность

Вопрос 3. Принципом политики информационной безопасности является принцип:

a) Усиления защищенности самого незащищенного звена системы
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы
d) Разделения доступа (обязанностей, привилегий) клиентам системы
e) Одноуровневой защиты системы
f) Совместимых, однотипных программно-технических средств сети, системы

g) Невозможности миновать защитные средства системы
h) Усиления основного звена сети, системы
i) Полного блокирования доступа при риск-ситуациях

Вопрос 4. Основными объектами информационной безопасности являются:

a) Компьютерные сети, базы данных
b) Информационные системы, психологическое состояние пользователей
c) Бизнес-ориентированные, коммерческие системы

Вопрос 5. Принципом информационной безопасности является принцип недопущения:

a) Неоправданных ограничений при работе в системе
b) Рисков безопасности сети, системы
c) Презумпции секретности

Вопрос 6. Основными рисками информационной безопасности являются:

a) Искажение, уменьшение объема, перекодировка информации
b) Техническое вмешательство, выведение из строя оборудования сети
c) Потеря, искажение, утечка информации

Вопрос 7. Транзакция - это

a) последовательность операций над БД, рассматриваемых СУБД как единое целое
b) последовательность выполнения команд
c) последовательность создания файлов
d) последовательность программных операций для создания единой БД
e) последовательность запоминания вложенных данных

Вопрос 8. Основные цели обеспечения логической и физической целостности базы данных?

a) защита от неправильных действий прикладного программиста
b) защита от неправильных действий администратора баз данных
c) защита от возможных ошибок ввода данных
d) защита от возможного появления несоответствия между данными после выполнения операций удаления и корректировки

Ключи: 1. a; 2. a, б; 3. d; 4. a; 5. a; 6. c; 7. a; 8. c, d.

Критерии оценивания теста:

% правильных ответов	Оценка
80 и выше	5
65 - 79	4+ - 5-
55 - 64	4
46 - 54	4-
30 - 45	3
25 - 29	3-
менее 24	2

Темы лабораторных работ (ОПК-1.3, ИПК-3.1, ИПК-3.2, ИПК-3.3):

Лабораторная работа 1. Установка, создание БД в среде MySQL.

Требуется установить сервер MySQL на локальной машине, создать базу данных, а также наполнить её данными с использованием SQL-запросов.

В ходе лабораторной работы рассматривается процесс установки MySQL-сервера, а также выполнение необходимых конфигураций. Студенты учатся создавать новую базу данных, определять её структуру (таблицы, поля), а также выполнять операции по добавлению, изменению и удалению данных с использованием SQL-запросов.

Работа считается выполненной:

успешно установлен MySQL-сервер; создана новая база данных с корректной структурой (таблицы и поля); выполнены без ошибок SQL-запросы на добавление, изменение и удаление данных без ошибок.

Работа считается не выполненной:

допущены ошибки при установке MySQL; база данных не создана или структура таблиц неверна; допущены ошибки при выполнении SQL-запросов.

Лабораторная работа 2. Средства идентификации и аутентификации.

Изучить механизмы идентификации и аутентификации пользователей в системе управления базами данных MySQL.

В рамках данной работы рассматриваются основные методы идентификации и аутентификации пользователей в MySQL (создание учетных записей пользователей, установка паролей и назначение привилегий). Выполняются практические упражнения по внедрению различных уровней доступа и проверке процесса аутентификации.

Работа считается выполненной:

созданы учетные записи пользователей с корректными привилегиями; проведены тесты на аутентификацию пользователей (успешный вход и проверка прав).

Работа считается не выполненной:

допущены ошибки в создании учетных записей; аутентификация пользователей завершалась неудачей; привилегии назначены некорректно (например, слишком много или слишком мало прав).

Лабораторная работа 3. Ссылочная целостность.

Изучить принципы и механизмы обеспечения ссылочной целостности в реляционных базах данных.

В этой лабораторной работе студенты осваивают использование внешних ключей для поддержания ссылочной целостности в базах данных MySQL. Выполняют практические задания на создание таблиц с внешними ключами, а также операции вставки и удаления данных с учётом ссылочной целостности.

Работа считается выполненной:

внешние ключи созданы и работают корректно; сохранена ссылочная целостность при выполнении операций вставки и удаления.

Работа считается не выполненной:

внешние ключи не созданы или неправильно определены; исключения или ошибки при попытке удалить или изменить записи, которые нарушают ссылочную целостность.

Лабораторная работа 4. Хранимые процедуры.

Научиться создавать и использовать хранимые процедуры в MySQL для автоматизации рутинных задач обработки данных.

В ходе выполнения данной лабораторной работы студенты знакомятся с понятием хранимых процедур, их синтаксисом и основами создания. Выполняют практические задания по написанию хранимых процедур для выполнения сложных запросов и обработки данных, а также изучению их преимуществ в управлении базами данных.

Работа считается выполненной:

хранимые процедуры созданы и протестированы на выполнение заданных операций; корректное использование параметров и возвращаемых значений.

Работа считается не выполненной:

допущены ошибки в синтаксисе при создании хранимых процедур; недостаточная функциональность (например, процедура не делает то, что задумано).

Лабораторная работа 5. Триггеры.

Исследовать механизм триггеров в MySQL, позволяющих автоматически выполнять операции на основе изменений данных в таблицах.

В рамках данной лабораторной работы студенты изучают что такое триггеры, какие типы триггеров существуют и как они работают. Практическая часть включает создание триггеров, которые срабатывают при операциях INSERT, UPDATE и DELETE, а также обсуждение сценариев использования триггеров для автоматизации процессов обработки данных.

Работа считается выполненной:

триггеры созданы и работают корректно при соответствующих операциях (INSERT, UPDATE, DELETE); логика триггеров соответствует поставленной задаче.

Работа считается не выполненной:

триггеры не работают или не срабатывают при нужных событиях; ошибки в логике триггера, приводящие к неверным результатам.

Лабораторная работа 6. Резервное копирование и восстановление БД.

Изучить методы резервного копирования и восстановления базы данных для обеспечения сохранности данных.

В ходе лабораторной работы рассматривается процесс создания резервных копий баз данных и таблиц, а также методы их восстановления. Студенты знакомятся с инструментами командной строки MySQL для осуществления резервного копирования и восстановлением данных из резервных копий, а также изучают стратегии управления резервными копиями.

Работа считается выполненной:

создание резервной копии базы данных прошло без ошибок, файл резервной копии успешно сохраняется; восстановление базы данных из резервной копии проходит без ошибок и возвращает данные в исходное состояние.

Работа считается не выполненной:

допущены ошибки при создании резервной копии или восстановлении данных; данные после восстановления не соответствуют оригинальным.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Зачет проводится по билетам. Билет содержит 2 вопроса из разных разделов дисциплины.

Вопросы к билетам (ИОПК-1.3.1, ИОПК-1.3.2, ИПК-3.1, ИПК-3.3):

Раздел «Клиент-серверная архитектура»

1. В чем заключается основная идея клиент-серверного взаимодействия?
2. Назовите основные характеристики архитектуры «клиент-сервер».
3. Опишите принцип работы двухзвенной модели архитектуры «клиент-сервер».
4. Перечислите преимущества и недостатки двухзвенной модели архитектуры «клиент-сервер».
5. Опишите принцип работы трехзвенной архитектуры «клиент-сервер».
6. Перечислите преимущества и недостатки треххзвенной модели архитектуры «клиент-сервер».
7. Дайте сравнительную характеристику двух- и трехзвенной моделей архитектур «клиент-сервер».

Раздел «Общие положения обеспечения информационной безопасности»

1. Что означает термин «информационная безопасность»?

2. Какие бывают информационные угрозы?
3. Назовите каналы, по которым может осуществляться хищение, изменение, уничтожение информации.
4. Перечислите угрозы, специфичные для систем управления базами данных.

Раздел «Условия ограничения целостности»
1. Что такое «ограничения целостности»?
2. Перечислите виды ограничений целостности.
3. В чем важность задания ограничений целостности?
4. Что такое «ограничение целостности по связи»?

Раздел «Задачи обеспечения безопасности АИС»
1. В чем суть нарушения конфиденциальности базы данных?
2. Каковы могут быть последствия нарушения целостности базы данных?
3. Какие существуют техники и технологии управления доступом?

Раздел «Модели доступа»
1. Опишите дискреционную модель, перечислите ее достоинства и недостатки.
2. Опишите мандатную модель, перечислите ее достоинства и недостатки.
3. Опишите ролевую модель, перечислите ее достоинства и недостатки.

Раздел «Процесс администрирования баз данных»

1. В чем суть централизованного администрирования управлением доступа. Приведите его достоинства и недостатки.
2. В чем суть децентрализованного администрирования управлением доступа. Приведите его достоинства и недостатки.
3. Сформулируйте понятия пароля и цели его создания. Приведите основные виды паролей, способы их защиты.

Раздел «Управление транзакциями»

1. Определите понятие транзакции. Перечислите свойства транзакций.
2. Определите варианты завершения транзакции.
3. Приведите содержимое журнала транзакций.
4. Перечислите уровни изолированности пользователей.
5. Сформулируйте понятие расписания. Приведите примеры рассогласования.
6. Управление блокированием. Перечислите основные методы синхронизационного блокирования.
7. Синхронизационные тупики, их распознавание.
8. Каково назначение и механизмы использования графа зависимостей и графа предшествования.
9. Методы разрушения тупиков.
10. Метод временных меток.

Критерии оценивания:

результаты зачета оцениваются оценками «зачтено» (студент выполнил все лабораторные работы, получил за ответы на вопросы теста оценку не ниже «3-» и дал правильные ответы на два вопроса билета) и «не зачтено» (студент не выполнил все лабораторные работы или получил за ответы на вопросы теста оценку «2» или не дал ответ на вопрос билета).

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примеры тестовых вопросов (ИОПК-1.3.1, ИОПК-1.3.2)

Вопрос 1. Утечкой информации в системе называется ситуация, характеризуемая:

a) Потерей данных в системе
b) Изменением формы информации
c) Изменением содержания информации

Вопрос 2. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

a) Целостность
b) Доступность
c) Актуальность

Вопрос 3. Принципом политики информационной безопасности является принцип:

a) Усиления защищенности самого незащищенного звена системы
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы
d) Разделения доступа (обязанностей, привилегий) клиентам системы
e) Одноуровневой защиты системы
f) Совместимых, однотипных программно-технических средств сети, системы
g) Невозможности миновать защитные средства системы
h) Усиления основного звена сети, системы
i) Полного блокирования доступа при риск-ситуациях

Вопрос 4. Основными объектами информационной безопасности являются:

a) Компьютерные сети, базы данных
b) Информационные системы, психологическое состояние пользователей
c) Бизнес-ориентированные, коммерческие системы

Вопрос 5. Принципом информационной безопасности является принцип недопущения:

a) Неоправданных ограничений при работе в системе
b) Рисков безопасности сети, системы
c) Презумпции секретности

Вопрос 6. Основными рисками информационной безопасности являются:

a) Искажение, уменьшение объема, перекодировка информации
b) Техническое вмешательство, выведение из строя оборудования сети
c) Потеря, искажение, утечка информации

Вопрос 7. Транзакция - это

a) последовательность операций над БД, рассматриваемых СУБД как единое целое
b) последовательность выполнения команд
c) последовательность создания файлов
d) последовательность программных операций для создания единой БД

e) последовательность запоминания вложенных данных

Вопрос 8. Основные цели обеспечения логической и физической целостности базы данных?

a) защита от неправильных действий прикладного программиста
b) защита от неправильных действий администратора баз данных
c) защита от возможных ошибок ввода данных
d) защита от возможного появления несоответствия между данными после выполнения операций удаления и корректировки

Ключи: 1. a; 2. a, б; 3. d; 4. a; 5. a; 6. c; 7. a; 8. c, d.

Критерии оценивания теста: тест считается выполненным, если студент правильно ответил на более 60% вопросов.

Информация о разработчиках

Головчинер Михаил Наумович, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности.

Вихорь Наталия Анатольевна, канд. физ.-мат. наук, доцент, доцент кафедры компьютерной безопасности.