Приложение 1

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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор института прикладной
математики и компьютерных наук

_____ А. В. Замятин

« 19 » мая 20 22 г.

Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине
(Оценочные средства по дисциплине)

Основы построения защищённых баз данных

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Томск – 2022

ОМ составил(и):
канд. техн. наук, доцент
доцент кафедры компьютерной безопасности М.Н. Головчинер

Рецензент:
заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент С.А. Останин

Оценочные средства одобрены на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 12 мая 2022 г. № 4

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Оценочные средства (ОС) являются элементом оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ОС разрабатываются в соответствии с рабочей программой (РП).

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и	ИОПК-9. Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности; ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных.	ОР-1.1.1 Знание базовых элементов информационной безопасности ОР-1.1.2 Знание разновидностей угроз информационной безопасности ОР-1.1.3 Знание и понимание основ проектирования защищенных БД	Отличное знание базовых элементов информационной безопасности, разновидностей угроз информационной безопасности, знание и понимание основ проектирования защищенных БД	Хорошее знание базовых элементов информационной безопасности, разновидностей угроз информационной безопасности, знание и понимание основ проектирования защищенных БД	Удовлетворительное знание базовых элементов информационной безопасности, разновидностей угроз информационной безопасности, знание и понимание основ проектирования защищенных БД	Неудовлетворительное знание базовых элементов информационной безопасности, разновидностей угроз информационной безопасности, знание и понимание основ проектирования защищенных БД

систем передачи информации						
ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации	ИОПК-14.3 Оценивает состояние и эффективность системы безопасности на уровне базы данных, разворачивает и настраивает средства защиты базы данных от несанкционированного доступа.	ОР-1.2.1 Знание угроз доступности, целостности и конфиденциальности базы данных ОР-1.2.2 Знание методов и инструментов защиты информации	Отличное знание угроз доступности, целостности и конфиденциальности базы данных, методов и инструментов защиты информации	Хорошее знание угроз доступности, целостности и конфиденциальности базы данных, методов и инструментов защиты информации	Удовлетворительное знание угроз доступности, целостности и конфиденциальности базы данных, методов и инструментов защиты информации	Неудовлетворительное знание угроз доступности, целостности и конфиденциальности базы данных, методов и инструментов защиты информации
ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик; ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты	ОР-1.3.1 Знание основных категорий уязвимостей БД ОР-1.3.2 Знание методики использования анализаторов защищенности и систем поиска уязвимостей БД ОР-1.3.3 Способность проведения анализа БД с целью поиска уязвимостей	Отличное знание основных категорий уязвимостей БД, методики использования анализаторов защищенности и систем поиска уязвимостей БД, способности проведения анализа БД с целью поиска уязвимостей	Хорошее знание основных категорий уязвимостей БД, методики использования анализаторов защищенности и систем поиска уязвимостей БД, способности проведения анализа БД с целью поиска уязвимостей	Удовлетворительное знание основных категорий уязвимостей БД, методики использования анализаторов защищенности и систем поиска уязвимостей БД, способности проведения анализа БД с целью поиска уязвимостей	Неудовлетворительное знание основных категорий уязвимостей БД, методики использования анализаторов защищенности и систем поиска уязвимостей БД, способности проведения анализа БД с целью поиска уязвимостей

	информации в компьютерных системах и сетях.					
ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей	ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием	ОР-1.4.1 Способность разработки проектов программных средств защиты информации	Отличное знание основ разработки проектов программных средств защиты информации и навыки в разработке проектов	Хорошее знание основ разработки проектов программных средств защиты информации и достаточные навыки в разработке проектов	Удовлетворительное знание основ разработки проектов программных средств защиты информации и наличие навыков в разработке проектов	Неудовлетворительное знание основ разработки проектов программных средств защиты информации и отсутствие навыков в разработке проектов

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства
1	Теоретические основы безопасности в БД	ОР-1.1.1, ОР-1.1.2	Тест
2	Управление доступом к данным	ОР-1.1.3, ОР-1.4.6	Тест
3	Обеспечение целостности данных	ОР-1.2.1, ОР-1.2.2 ОР-1.3.1, ОР-1.3.2	Тест
4	Защита данных в распределенных системах	ОР-1.2.3, ОР-1.3.1, ОР-1.3.2, ОР-1.3.3	Тест
5	Нереляционные базы данных	ОР-1.4.3	Тест

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Вариант теста:

Вопрос 1. Информационная безопасность зависит от:

- компьютеров, поддерживающей инфраструктуры
- пользователей
- информации

Вопрос 2. Кто является основным ответственным за определение уровня классификации информации:

- руководитель среднего звена
- владелец
- высшее руководство

Вопрос 3. Утечкой информации в системе называется ситуация, характеризуемая:

- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

Вопрос 4. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- Целостность
- Доступность
- Актуальность

Вопрос 5. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:

- хакеры
- контрагенты

- сотрудники

Вопрос 6. Принципом политики информационной безопасности является принцип:

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

Вопрос 7. Основными источниками угроз информационной безопасности является:

- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

Вопрос 8. Основными объектами информационной безопасности являются:

- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

Вопрос 9. К основным принципам обеспечения информационной безопасности относятся:

- Экономическая эффективность системы безопасности
- Многоплатформенная реализации системы
- Усиление защищенности всех звеньев системы

Вопрос 10. К наиболее распространенным угрозам информационной безопасности корпоративной системы относится:

- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательное внедрение сетевых вирусов

Вопрос 11. Диспетчер доступа...

- использует базу данных защиты, в которой хранятся правила разграничения доступа
- использует атрибутные схемы для представления матрицы доступа
- выступает посредником при всех обращениях субъектов к объектам
- фиксирует информацию о попытках доступа в системном журнале

Вопрос 12. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?

- целостность
- апеллируемость
- доступность
- конфиденциальность
- аутентичность

Вопрос 13. В число основных понятий ролевого управления доступом входит:

- роль

- исполнитель роли
- пользователь роли

Вопрос 14. В число основных понятий ролевого управления доступом входит:

- объект
- субъект
- метод

Вопрос 15. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:

- когда риски не могут быть приняты во внимание по политическим соображениям
- для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- когда стоимость контрмер превышает ценность актива и потенциальные потери

Вопрос 16. К основным функциям системы безопасности относятся:

- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

Вопрос 17. Принципом информационной безопасности является принцип недопущения:

- Неоправданных ограничений при работе в системе
- Рисков безопасности сети, системы
- Презумпции секретности

Вопрос 18. Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

Вопрос 19. Основные функции СУБД

- управление транзакциями
- журнализация
- сбор информации
- заполнение БД
- запоминание с помощью программ всех данных находящихся во внешней памяти

Вопрос 20. Журнал - это

- особая часть БД, недоступная пользователям СУБД
- особая часть БД, поддерживаемая с особой тщательностью, в которую поступают записи обо всех изменениях основной части БД
- особая часть БД для поддержания логической целостности БД
- особая часть БД для доступа к данным во внешней памяти
- особая часть БД для считывания информации из буфера внутренней памяти

Вопрос 21. Транзакция - это

- последовательность операций над БД, рассматриваемых СУБД как единое целое
- последовательность выполнения команд
- последовательность создания файлов
- последовательность программных операций для создания единой БД
- последовательность запоминания вложенных данных

Вопрос 22. Операции, обеспечивающие безопасность

- шифрование прикладных программ; шифрование данных
- защита паролем; ограничение уровня доступа
- правильное проектирование; шифрование данных
- правильное построение БД, ограничение доступа
- правильное оформление документов к БД; защита паролем

Вопрос 23. Основные цели обеспечения логической и физической целостности базы данных?

- защита от неправильных действий прикладного программиста
- защита от неправильных действий администратора баз данных
- защита от возможных ошибок ввода данных
- защита от возможного появления несоответствия между данными после выполнения операций удаления и корректировки

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Вопросы к билетам:

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 трехзвенной 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.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Оценки по тесту:

% 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

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Учет ответов на вопросы билета (2 вопроса) и оценки тестирования:

Ответ на билет	Оценка теста	Окончательная оценка
5	4 - 5	5
5	3 - 4-	4
5	3-	3
4	4+ - 5	4
4	3 - 4	4
4	3-	3
3	4+ - 5	4
3	3- - 4	3