ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники
Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.36 «Проектирование защищенных баз данных»

Специальность: 10.05.01 Компьютерная безопасность
Специализация: № 8 Информационная безопасность объектов информатизации на базе компьютерных систем в защищенном исполнении

ОПОП по специальности:
Компьютерная безопасность
Квалификация выпускника: специалист по защите информации

Форма обучения - очная
Срок обучения — 5,5 лет

Рязань, 2023 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной профессиональной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретенных обучающимися в ходе выполнения индивидуальных заданий на практических занятиях и лабораторных работах. При оценивании результатов освоения практических занятий и применяется шкала оценки «зачтено – не зачтено». Количество практических, лабораторных работ и их тематика определены рабочей программой дисциплины.

Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением экзамена и курсовой работы.

2. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1.	Введение	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
2.	Угрозы и атаки специфичные для СУБД.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
3.	Критерии защиты информации в СУБД.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
4.	Способы защиты информации в СУБД.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3,	экзамен

		ОПК-14.4, ОПК-14.5, ОПК-14.6)	
5.	Средства идентификации и аутентификации объектов баз данных. Управление доступом.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
6.	Модели безопасности, применяемые при построении защиты в СУБД.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
7.	Использование транзакции для изолирования действий пользователей.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
8.	Блокировки.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
9.	Ссылочная целостность, триггерная и событийная. Реализация правил безопасности.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
10.	Применение криптографических методов защиты информации в СУБД.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
11.	Средства поддержания высокой готовности.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
12.	Сканеры баз данных.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен
13.	Защита коммуникаций между сервером и клиентами.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен

14.	Задачи и средства администратора безопасности баз данных.	ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	экзамен

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Уровень освоения компетенций, формируемых дисциплиной:

а) описание критериев и шкалы оценивания тестирования:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100%
2 балла (продвинутый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84%
1 балл (пороговый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69%
0 баллов	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49%

б) описание критериев и шкалы оценивания теоретического вопроса:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя
2 балла (продвинутый уровень)	выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов
1 балл (пороговый уровень)	выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с

	помощью преподавателя
0 баллов	выставляется студенту, который не смог ответить на вопрос

в) описание критериев и шкалы оценивания практического задания:

Шкала оценивания	**Критерий**
3 балла (эталонный уровень)	Задача решена верно
2 балла (продвинутый уровень)	Задача решена верно, но имеются неточности в логике решения
1 балл (пороговый уровень)	Задача решена верно, с дополнительными наводящими вопросами преподавателя
0 баллов	Задача не решена

На экзамен выносится два теоретических вопроса. Максимально студент может набрать 10 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно». Шкала перевода баллов в оценки:

от 8 до 10 баллов - «отлично»;

от 6 до 7 баллов - «хорошо»;

от 3 до 5 баллов - «удовлетворительно»;

менее 3 баллов - «неудовлетворительно»

4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация (экзамен)

Коды компетенций/ и индикаторов	**Результаты освоения ОПОП Содержание компетенций/ индикаторов**
ОПК-14 (ОПК-14.1, ОПК-14.2, ОПК-14.3, ОПК-14.4, ОПК-14.5, ОПК-14.6)	**Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации.** **ОПК-14.1** ***Выбирает СУБД в соответствии с требованиями о защите информации;*** **ОПК-14.2** ***Выполняет работу с базами данных с использованием языка SQL*** **ОПК-14.3** ***Обеспечивает целостность проектируемой базы данных с использованием средств языка SQL*** **ОПК-14.4** ***Производит назначение прав пользователя в соответствии с требованиями нормативных документов по защите информации*** **ОПК-14.5** ***Осуществляет проектирование баз данных с учетом***

	различных моделей политик безопасности **ОПК-14.6** ***Осуществляет настройку СУБД в соответствии с заданной политикой безопасности***

***а) типовые тестовые вопросы*:**

1. Какие нормативные документы определяют требования по защите информации в базах данных:

– ГОСТ Р ИСО/МЭК 15408-2012 (+);
– СТР-К;
– Федеральный закон от 27 июля 2006 г. № 149-ФЗ;
– Приказ ФСТЭК России от 11 февраля 2013 г. № 17

2. Какие документы используются для сертификации СУБД по ГОСТ Р ИСО/МЭК 15408-2012:

– профиль защиты (+);
– задание по безопасности (+);
– акт проверки;
– техническое задание.

3. Что такое сертификат соответствия требованиям безопасности?

– документ, которым орган по сертификации удостоверяет соответствие выпускаемой в обращение продукции требованиям одного или нескольких технических регламентов;

– документ, которым орган по сертификации удостоверяет соответствие выпускаемой в обращение продукции требованиям безопасности (+);

– документ, удостоверяющий соответствие объекта требованиям технических регламентов, документам по стандартизации или условиям договоров;

– набор нормативных документов с требованиями по защите информации.

4. Аттестат соответствия требованиям безопасности - это:

– документ, подтверждающий, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации;

– документ, подтверждающий, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации (+);

– документ, удостоверяющий, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации;

– документ, подтверждающий наличие средств защиты информации на объекте информатизации.

5. Аттестат соответствия выдается:

– автоматизированным системам (+);
– операционным системам;
– системам управления базами данных;
– средствам криптографической защиты информации.

6. Лицензируются:
– выделенные помещения;
– виды деятельности по технической защите информации (+);
– защищаемые помещения;
– средства вычислительной техники.
7. Сертификат соответствия требованиям безопасности выдается:
– защищаемым помещениям;
– системам управления базами данных (+);
– информационным системам;
– сотрудникам отдела защиты информации.
8. Профиль защиты разрабатывается на:
– операционные системы (+);
– межсетевые экраны (+);
– маршрутизаторы;
– объекты доступа.
9. *Какие* средства защиты информации есть в СУБД?
– реализующие генерацию паролей пользователя;
– реализующие дискреционное разграничение доступа (+);
– реализующие идентификацию и аутентификацию (+);
– реализующие тестирование на проникновение;
– сканер базы данных.
10. *Виды* регистрации пользователя в СУБД:
– раздельная (+);
– смешанная (+);
– выборочная;
– удаленная.
11. Какие из перечисленных видов криптографических протоколов относятся к группе протоколов идентификации (аутентификации) участников:
– односторонней аутентификации (+);
– сложной аутентификации;
– двусторонней (взаимной) аутентификации (+);
– комбинированной аутентификации.
12. Какие средства защиты информации встроены в СУБД*:*
– дискреционное разграничение доступа (+);
– модель Белла-Ла Падула;
– модель контроля потоков;
– правила безопасности.
13. Какие языковые средства СУБД можно использовать для защиты информации?
– правила (+);
– ограничения (+);
– запросы;
– транзакции.
14. Различают:
– базовое представление (+);

– клиентское представление;
– серверное представление;
– операторное представление.

15. Многоуровневая защита в СУБД - это:
– сочетание дискреционной и мандатной моделей доступа (+);
– сочетание дискреционной и ролевой моделей доступа;
– сочетание мандатной и ролевой моделей доступа;
– сочетание дискреционной, мандатной и ролевой моделей доступа.

16. К ограничениям относятся:
– CHECK (+);
– GRANT;
– PUBLIC;
– CASCADE.

17. Что такое эффективность защиты информации?
– способность системы отражать атаки;
– степень соответствия результатов защиты информации цели защиты информации (+);
– эффективность системы защиты информации определяется ее стоимостью;
– эффективность системы защиты информации определяется ее производительностью;
– эффективность системы защиты информации определяется ее управляемостью и совместимостью.

18. Требования к эффективной реализации системы защиты информации:
– комплексность (+);
– информативность;
– адаптируемость к изменяющимся условиям (+);
– многоступенчитость .

19. Политика безопасности - это:
– совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы (+);
– требования, регламентирующие процесс обработки информации;
– правила обработки информации в СУБД;
– правила доступа объектов доступа к субъектам доступа.

20. Различают следующие модели политик безопасности:
– ролевая (+);
– полномочная (+):
– мандатная (+);
– верифицированная (+);
– избирательная (+);
– дискреционная (+)

21. Средства оценки эффективности защиты информации в СУБД:
– сканеры безопасности (+);
– средства резервного копирования;

- программы гарантированного уничтожения информации;
- средства аудита.

22. Виды контроля эффективности защиты:
    - организационный контроль (+);
    - технический контроль (+);
    - плановый контроль;
    - верифицированный контроль;
    - технологический контроль.
23. Виды резервного копирования:
    - полное (+);
    - разностное (+);
    - плановое;
    - частичное;
    - инкрементное (+).
24. В базах данных ссылочная целостность определяется:
    - первичным ключом;
    - потенциальным ключом;
    - внешним ключом (+);
    - криптографическим ключом;
    - уникальным ключом.
25. Для чего нужно ограничение CHECK?
    - задать диапазон изменения сущности;
    - задать значение сущности;
    - ввести значение сущности;
    - задать диапазон изменения атрибута (+);
    - задать значение атрибута.
26. Таблица базы данных создается командой:
    - create table….(+);
    - select * from table….;
    - insert into table….;
    - alter table…. .
27. Агрегатными функциями SQL являются:
    - grant;
    - sum (+);
    - count (+);
    - where;
    - from;
    - having.
28. Предложение ORDER BY позволяет
    - позволяет отсортировать по возрастанию выходные данные запроса;
    - позволяет отсортировать по убыванию выходные данные запроса;
    - упорядочить выходные данные запроса в соответствии со значениями одного или нескольких столбцов (+);
    - позволяет убрать повторяющиеся строки из запроса;

- позволяет выбрать данные и вывести их.

29. Объединение таблиц осуществляется оператором:
    - INNER JOIN;
    - INNER JOIN LEFT;
    - UNION (+);
    - EXISTS;
    - GROUP BY/
30. Пользователи СУБД это:
    - системные программисты;
    - прикладные программисты (+);
    - программист серверной части;
    - программист клиентской части.
31. СУБД имеют:
    - трехуровневую архитектуру (+);
    - двухуровневую архитектуру;
    - четырехуровневую архитектуру;
    - трехзвенную архитектуру.
32. Выделяю следующие модели данных:
    - Диаграмма Бахмана (+);
    - модель сущность-связь (+);
    - факторографическая модель;
    - объектно-ориентировочная.
33. Какие угрозы для баз данных знаете?
    - атака по словарю;
    - агрегирование данных (+);
    - атака «салями» (+);
    - программные «люки» и дополнительные точки входа;
    - «взлом системы».
34. Требования к средствам вычислительной техники:
    - требования к разграничению доступа (+);
    - требования к регистрации;
    - требования к документации на средства вычислительной техники;
    - требования к доступности информации.
35. Какие из перечисленных видов криптографических протоколов относятся к группе протоколов идентификации (аутентификации) участников:
    - односторонней аутентификации (+);
    - сложной аутентификации;
    - двусторонней (взаимной) аутентификации (+);
    - комбинированной аутентификации.
36. Какие средства защиты информации встроены в СУБД*:*
    - дискреционное разграничение доступа (+);
    - модель Белла-Ла Падула;
    - модель контроля потоков;
    - правила безопасности.

37. Какие языковые средства СУБД можно использовать для защиты информации?
- правила (+);
- ограничения (+);
- запросы;
- предоставления.

38. Различают:
- базовое представление (+);
- клиентское представление;
- серверное представление;
- операторное представление.

39. Многоуровневая защита в СУБД - это:
- сочетание дискреционной и мандатной моделей доступа (+);
- сочетание дискреционной и ролевой моделей доступа;
- сочетание мандатной и ролевой моделей доступа;
- сочетание дискреционной, мандатной и ролевой моделей доступа.

40. К ограничениям относятся:
- CHECK (+);
- GRANT;
- PUBLIC;
- CASCADE.

б) типовые теоретические вопросы:

1. Какие уровни доверия определены в ГОСТ ИСО/МЭК 15408-2012.
2. Для каких IT-продуктов разработаны профили защиты.
3. Какие документы определяют требования по защите информации в СУБД?
4. Перечислите уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, установленные Требованиями по безопасности информации.
5. Перечислите документы, регламентирующие получение лицензии на деятельность по технической защите конфиденциальной информации и по разработке и производству средств защиты конфиденциальной информации.
6. Каковы требования к лицензиату, планирующему осуществлять деятельность по технической защите конфиденциальной информации?
7. Надо ли защищать общедоступную информацию, хранящуюся в базе данных? Если да, то от чего?
8. Перечислите требования по защите конфиденциальной информации, хранящейся в базе данных.
9. Перечислите средства защиты информации, встроенные в СУБД
10. Как создать параметризованное представление?
11. Использование криптографических методов в СУБД.
12. Какие виды блокировок в СУБД знаете?
13. Проблемы при многопользовательской работе транзакций.
14. Виды сканеров безопасности.

15. Какие параметры оценивают сканеры безопасности?
16. Особенности использования сканеров безопасности.
17. Как настраивают политику безопасности в СУБД?
18. Использование ограничений для защиты информации в базах данных.
19. Как создать базу данных?
20. Перечислите основные понятия ER-метода.
21. Какие этапы включает проектирование реляционной базы данных с помощью ER-метода?
22. Опишите правила формирования отношений по ER-диаграмме.
23. Какие виды регистрации пользователя в СУБД знаете?
24. Как дать права пользователю для работы с базой данных?
25. Перечислите основные функции администратора СУБД.
26. Какие этапы включает в себя процесс проектирования базы данных?
15. Перечислите средства защиты информации, встроенные в СУБД
16. Как создать параметризованное представление?
17. Использование криптографических методов в СУБД.
18. Какие виды блокировок в СУБД знаете?
19. Проблемы при многопользовательской работе транзакций.
20. Какие виды блокировок знаете?
21. Теорема Хета
22. Понятие транзакции

Типовые контрольные задания или иные материалы

Типовые задания и вопросы для экзамена по дисциплине (сводный список)

1. Термины и определения.
2. Пользователи СУБД.
3. Угрозы специфичные для СУБД и БД (Получение информации путем логических выводов, ссылочная целостность, «лазейки» системы идентификации/аутентификации, компрометация всей сети, программы типа «троянский конь»).
4. Уязвимости специфичные для СУБД (уязвимости на этапе подключения к СУБД, уязвимость «маскарад», статистическая идентификация, покушение на высокую готовность, атака «салями», «скрытые» каналы, «сборка мусора», «взлом» системы, «люки», вредоносные программы, общая классификация угроз).
5. Критерии защиты информации в СУБД. Критерии по документам Гостехкомиссии России.
6. Оценка защищенности СУБД на основе Общих критериев. Общие сведения.
7. Пользователи «Общих критериев».
8. Структура «Общих критериев».
9. Основные классы требований «Общих критериев».
10. Оценка СУБД по «Общим критериям». Принципы оценки. ПЗ для СУБД.
11. ЗБ на СУБД.
12. Способы защиты информации в СУБД. Представления и защита данных.
13. Защита данных при использовании хранимых процедур и триггеров.
14. Привилегии доступа. Операторы GRANT и REVOKE.
15. Защита информации с помощью ограничений.
16. Защита информации с помощью правил.

17. Привилегии безопасности.
18. Защита информации с помощью хранимых процедур.
19. Защита информации с помощью триггеров.
20. Транзакции. Общие сведения о транзакциях и их работе.
21. Параллельное выполнение транзакций. Работа транзакций в смеси.
22. Проблемы параллельной работы транзакций. Проблема потери результатов обновления.
23. Проблема незафиксированной зависимости (чтения грязных данных, неаккуратное считывание).
24. Проблема несовместимого анализа. Конфликты доступа к данным.
25. Возможные способы решения конфликтных ситуаций. График запуска транзакций.
26. Блокировки. Понятие блокировок.
27. Преднамеренные блокировки.
28. Предикатные блокировки. Метод временных меток.
29. Механизм выделения версий данных.
30. Теорема Есварана о сериализуемости.
31. Реализация изолированности транзакции средствами SQL.
32. Какие средств поддержания высокой готовности используются для СУБД.
33. Для чего нужны сканеры баз данных.
34. Какие параметры СУБД и баз данных оценивают сканеры баз данных.
35. Как защитить передачу информации между сервером и клиентами.
36. Что дает кластерная организация серверов баз данных для защиты информации.
37. Основные функции администратора безопасности баз данных.
38. Какие типы архивирования поддерживает SQL Server 7.0?
39. Сформулировать различия между допустимыми типами архивирования.
40. Какие действия должен выполнить администратор БД при переполнении журнала транзакций?
41. От каких факторов зависит частота резервного копирования?
42. Сформулировать общие стратегии архивирования и восстановления БД.
43. База данных размером 5Гб хранится в одном файле. БД используется системой приема заказов компании, рассылающей товары почтой. Операторы принимают до 2 000 заказов в сутки. Предложите план резервного копирования для этой БД.
44. В БД объемом 700Гб хранятся фотографии, получаемые с метеоспутника. Снимки хранятся в виде графических изображений, а БД постоянно обновляется. Каждая таблица БД хранится в отдельной группе файлов. Резервное копирование всей БД требует 20 часов. Как можно ускорить ежедневное резервное копирование, обеспечив при этом надежное восстановление данных при отказе системы?
45. Почему нужны именованные устройства резервного копирования?
46. Перечислить преимущества и недостатки разностного архивирования как составной части стратегии резервного копирования.
47. Применяется только резервное копирование БД. Журнал транзакций и дополнительные файлы данных хранятся на отдельном физическом диске. Журнал накапливает сведения об изменениях. Но периодически очищается. Диск, содержащий дополнительные файлы, отказал. Как минимизировать потери данных после замены диска?
48. Есть полная резервная копия БД и несколько копий журнала транзакций. БД хранится в 4 файлах. Диск, на котором размещался третий файл, отказал. Как восстановить и реконструировать БД?
49. Есть полная резервная копия БД и несколько копий журнала транзакций. В 9:21 произошло злонамеренное изменение БД. Сейчас – 9:30. Как восстановить БД и вернуть ее в согласованное состояние?
50. Дайте определение ограничениям.
51. Перечислите виды ограничений, которые существуют.

52. Дайте определение каждому виду ограничения.

53. Расскажите, как в СУБД определяются понятия:"кластеризованный индекс" и "некластеризованный индекс"?

54. Перечислите правила при модификации первичного ключа .

55. Опишите принципы создания ограничения QNIQUE.

56. Опишите принципы создания ограничения FOREIG KEY.

57. Опишите принципы создания ограничения CHECK.

58. Что необходимо указывать, что бы использовать null-значения в какой-либо колонке?

59. Как работают отложенные ограничения при различных способах завершения транзакций?

Оценочные материалы составлены в соответствии с рабочей программой дисциплины «Проектирование защищенных баз данных» по специальности 10.05.01 Компьютерная безопасность.

Составил
старший преподаватель кафедры
«Информационная безопасность» Т.И. Калинкина