Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт экзамена

по дисциплине «Безопасность систем баз данных», 6 семестр

Методика оценки

Экзамен проводится в устной форме по билетам. Билет состоит из 2 вопросов и формируется по следующему правилу:
первый вопрос выбирается из диапазона вопросов 1–16;
второй вопрос выбирается из диапазона вопросов 17–32.

Таким образом, проверяются результаты обучения по дисциплине, соотнесённые с установленными в программе индикаторами достижения компетенций ОПК-12.1, ОПК-12.2 и ОПК-12.3.

На экзамене преподаватель вправе задавать студенту уточняющие и дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Безопасность систем баз данных»

---

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент проводит сравнительный комплексный анализ материала, выявляет проблемы, предлагает механизмы их решения, представляет количественные характеристики определенных процессов, приводит конкретные примеры, не допускает ошибок. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 35 до 40 баллов.*

Ответ на экзаменационный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, дает характеристику процессов, явлений, проводит анализ причин, условий, способен представить количественные и качественные характеристики процессов, не допускает существенных ошибок. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 27 до 34 баллов.*

Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, допускает непринципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 20 до 26 баллов.*

Ответ на экзаменационный билет считается **неудовлетворительным** (ниже порогового уровня), если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее* 20 *баллов.*

Шкала оценки

Экзамен считается сданным, если сумма баллов по всем заданиям билета составляет от 20 до 40 баллов включительно. Сумма менее 20 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

Вопросы к экзамену **по дисциплине «**Безопасность систем баз данных**»**

1. Безопасность систем баз данных: защищаемые активы, субъекты, объекты и отношения доступа.
2. Угрозы конфиденциальности, целостности и доступности данных. Границы ответственности СУБД, ОС и приложения.
3. Концептуальная модель базы данных: сущности, атрибуты, связи и ограничения предметной области.
4. Выделение защищаемых данных и ролей пользователей при построении концептуальной модели.
5. Переход от концептуальной модели к схеме базы данных с учётом требований безопасности.
6. Доступ к концептуальной модели БД. Отображение пользовательских функций на объекты и операции.
7. Матрица доступа в системе баз данных. Обоснование минимально необходимых полномочий для ролей.
8. Разграничение доступа на уровне базы данных, схемы, таблицы, столбца и строки.
9. Владение объектами и административные полномочия. Разделение обязанностей и контроль избыточных прав.
10. Разрешения прямого доступа и доступ через представления и подпрограммы. Выбор способа ограничения данных.

11. Команда GRANT языка SQL. Выдача привилегий и права передачи полномочий.
12. Команда REVOKE языка SQL. Отзыв привилегий и влияние зависимых разрешений на итоговый доступ.
13. Команда DENY в поддерживающих её СУБД. Отличие явного запрета от отсутствия разрешения и от REVOKE; особенности переноса политики в PostgreSQL/Tantor.
14. Проверка эффективных прав при наличии нескольких ролей, членства и разрешений на разных уровнях.
15. Пользователи и роли в БД. Атрибуты, членство, наследование полномочий и переключение роли.
16. Жизненный цикл учётной записи БД: создание, предоставление минимальных прав, блокирование и прекращение доступа.
17. СУБД Tantor: назначение, организация учебного экземпляра и основные объекты администрирования.
18. Ролевая модель доступа в СУБД Tantor. Групповые роли, роли подключения и проверка полномочий.
19. Управление доступом в СУБД Tantor. Выдача и отзыв разрешений на схемы и объекты базы данных.
20. Проверка ролевой модели в Tantor: разрешённые и запрещённые операции, фиксация результатов и устранение избыточных прав.
21. Шифрование данных в системе БД. Цели защиты, область применения и ограничения по отношению к разграничению доступа.
22. Защита данных при передаче и хранении. Различие уровней шифрования и выбор механизма для конкретной угрозы.
23. Управление ключами шифрования: создание, хранение, разграничение доступа, смена и восстановление доступности ключей.
24. Применение шифрования в СУБД Tantor. Выбор доступного в учебной конфигурации механизма и проверка возможности восстановления данных.
25. Совместное применение ролевого доступа и шифрования. Разделение прав на зашифрованные данные и на операции с ключами.
26. Резервное копирование и восстановление БД. Цели, типы отказов и определение требований к потере данных и времени восстановления.
27. Логическое и физическое резервное копирование. Состав копии, условия восстановления и ограничения применимости.
28. Журнал транзакций и восстановление согласованного состояния. Назначение архивирования журнала и восстановления на момент времени.
29. Защита резервных копий: разрешения доступа, шифрование, хранение и проверка целостности.
30. Восстановление базы данных на учебном стенде. Последовательность действий и проверка данных, владельцев и разрешений.
31. План испытаний защиты БД: проверка модели доступа, шифрования и восстановления, критерии успешности и протоколирование.
32. Обоснование решений по безопасности при разработке автоматизированной системы на базе Tantor: модель данных, роли, защита информации и восстановление.