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

Паспорт
курсовой работы

по дисциплине «Безопасность систем баз данных», 6 семестр

Методика оценки.

Выполнение курсовой работы (далее – КР) является обязательным видом самостоятельной работы студента по дисциплине, предусмотренным учебным планом.

Основной целью выполнения КР является формирование компетенции ОПК-12 и индикаторов ОПК-12.1, ОПК-12.2, ОПК-12.3 по дисциплине «Безопасность систем баз данных» посредством закрепления, углубления и обобщения знаний, а также самостоятельного проектирования и проверки защищённой системы баз данных. Выполнение курсовой работы способствует подготовке к выполнению выпускной квалификационной работы.

Задачи КР: проанализировать предметную область и требования к защите данных; построить концептуальную и логическую модели БД; определить субъектов, объекты и матрицу доступа; реализовать роли и минимально необходимые разрешения в СУБД Tantor; обосновать и применить доступные средства шифрования; организовать защищённое резервное копирование и контрольное восстановление; испытать решение и оценить его соответствие заданным требованиям.

Темы КР соответствуют профилю подготовки, формируются преподавателями в начале семестра и утверждаются решением кафедры. Количество тем и индивидуальных вариантов исходных данных обеспечивает каждого обучающегося самостоятельным заданием.

Выполнение студентами КР начинается с ознакомления с примерной тематикой. Закрепление тем КР за студентами и назначение научных руководителей производится распоряжением заведующего кафедрой и/или утверждается решением кафедры.

Курсовая работа выполняется индивидуально на учебном стенде с синтетическими данными. Тема, состав объектов, роли и исходные параметры согласуются с руководителем и фиксируются в задании.

Структура курсовой работы:

Титульный лист.
Введение: актуальность, цель, задачи, предметная область и требования к защите данных.
Теоретическая часть: концептуальная модель, модель угроз и доступа, обоснование методов защиты и восстановления.
Практическая часть: реализация базы данных и ролевой модели в Tantor, настройка защиты, протоколы испытаний и контрольного восстановления.
Выводы или заключение.
Список литературы.
Приложения (при необходимости).

Заключение содержит общие выводы о выполнении требований безопасности, результатах испытаний и ограничениях разработанного решения, а также рекомендации по его применению.

Список литературы оформляется в соответствии с библиографическими требованиями в алфавитном порядке и включает источники, изученные и использованные при выполнении работы: книги, статьи, документацию СУБД и иные материалы.

Требования к оформлению:

Объем КР до 50 страниц машинописного текста формата А4. Шрифт Times New Roman, 12. Нумерация страниц сквозная, в нижней части листа по центру арабскими цифрами. КР должна быть отредактирована, не содержать орфографических, синтаксических и стилевых ошибок.

Законченная курсовая работа предоставляется для проверки в электронном виде в срок, установленный преподавателем. Преподаватель оценивает качество КР с учетом теоретического и практического содержания, достижения ее целей и задач.

Курсовая работа проверяется руководителем работы, который дает письменное заключение по работе — рецензию.

Если при выполнении КР были допущены ошибки, то работа возвращается студенту для исправления выявленных недочетов и затем вновь предоставляется руководителю для проверки. При положительном результате оценивания студент распечатывает работу, передает на кафедру и защищает до сессии в назначенное преподавателем время.

Защита КР проходит публично перед группой студентов.

По результатам защиты студенту выставляется оценка в соответствии с критериями, приведенными в п. 2 настоящего Паспорта.

Уровни сформированности компетенций и критерии оценки

В соответствии с балльно-рейтинговой системой НГТУ курсовая работа по дисциплине «Безопасность систем баз данных» в 6 семестре имеет максимальную оценку 100 баллов.

Курсовая работа выполнена на продвинутом уровне, если:

- она выполнена в полном соответствии с заданием, отличается глубиной проработки всех разделов содержательной части, текстовая часть оформлена с соблюдением установленных правил;
- руководитель характеризует деятельность студента положительно (в частности, отмечает его инициативу, самостоятельность, систематичность работы на всех этапах выполнения работы);
- в докладе исчерпывающе, последовательно, четко и логически правильно изложена суть работы и ее основные результаты;
- студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач, сформулированных в задании;
- в докладе суть работы и ее основные результаты представлены исчерпывающе, последовательно, четко и логически правильно; на все вопросы студент дал обстоятельные и аргументированные ответы, убедительно защищал свою точку зрения;
- компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которой выполняется курсовая работа, сформированы в полном объеме.

Оценка за выполнение КР составляет от 87 до 100 баллов.

Курсовая работа выполнена на базовом уровне, если:

- соответствует заданию, отличается глубиной проработки всех разделов содержательной части, текстовая часть оформлена с соблюдением установленных правил;
- руководитель характеризует деятельность студента положительно, но с незначительными замечаниями;
- в докладе правильно изложена суть работы и ее основные результаты;
- студент достаточно твердо усвоил теоретический материал и может самостоятельно его применять;
- в докладе суть работы и ее основные результаты представлены полно; на все вопросы студент дал ответы, но их полнота и аргументированность недостаточны;

компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которой выполняется курсовая работа, сформированы с небольшими пробелами и соответствуют базовому уровню.

Оценка за выполнение КР составляет от 73 до 86 баллов.

Курсовая работа выполнена на пороговом уровне, если:

выполнена в основном правильно, но без необходимой проработки некоторых разделов;

в докладе упущены некоторые принципиальные моменты содержательной части работы;

в докладе представлены суть работы и ее основные результаты; ответы на вопросы вызвали существенные затруднения;

компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которой выполняется курсовая работа, сформированы с пробелами и соответствуют пороговому уровню.

Оценка за выполнение КР составляет от 50 до 72 баллов.

Курсовая работа считается не выполненной, если студентом не проработаны важные разделы исследования, допущены принципиальные ошибки, не исправленные после замечаний руководителя КР. Студент не допущен к защите курсовой работы. Компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной, по которой выполняется курсовая работа, не сформированы.

Оценка составляет менее 50 баллов.

Шкала оценки.

Курсовая работа по дисциплине считается успешно выполненной, если сумма полученных баллов составляет от 50 до 100 баллов включительно.

Примерный перечень тем курсовой работы

1. Защищённая база данных учёта оборудования организации. Спроектировать концептуальную и логическую модели, разграничить доступ сотрудников и администраторов, реализовать защиту выбранных данных и проверить восстановление.
2. Защищённая база данных заявок технической поддержки. Определить роли заявителя, исполнителя и руководителя, ограничить доступ к записям и операциям, разработать план шифрования и резервного копирования.
3. Защищённая база данных складского учёта. Построить модель поступлений и выдачи, разделить полномочия операторов и контролёров, проверить целостность, шифрование и восстановление учебных данных.
4. Защищённая база данных библиотечного фонда. Реализовать модель экземпляров и операций выдачи, ограничить права категорий пользователей, защитить выбранные атрибуты и проверить восстановление из резервной копии.
5. Защищённая база данных учебного электронного архива. Разработать категории документов и уровни доступа, реализовать ролевую политику и защиту содержимого, проверить сохранение прав после восстановления.
6. Защищённая база данных управления проектами. Разделить доступ участников разных проектов, определить полномочия руководителей и администраторов, реализовать выбранные меры шифрования и испытать восстановление.
7. Защищённая база данных учёта программных лицензий. Спроектировать объекты и роли, ограничить операции выдачи и изменения записей, защитить служебные сведения и разработать сценарий восстановления.
8. Защищённая база данных договорного учёта. Разделить доступ к реквизитам и содержимому учебных договоров, реализовать матрицу полномочий, защитить выбранные поля и резервные копии.

9. Защищённая база данных планирования технического обслуживания. Определить роли операторов, инженеров и контролёров, обеспечить разрешённые изменения, защиту данных и восстановление после учебного сбоя.
10. Защищённая база данных учёта сетевых ресурсов. Реализовать концептуальную модель узлов и ответственных лиц, ограничить административные операции, обосновать шифрование и проверить согласованность восстановленных данных.
11. Проектирование защищённой многопользовательской БД с разделением обязанностей в Tantor. Построить концептуальную и логическую модели, разделить полномочия ввода, подтверждения и администрирования данных; реализовать ролевую политику, шифрование и защищённое резервирование. Подтвердить разделение обязанностей протоколом проверок до и после восстановления.
12. Проектирование защищённой БД с раздельным доступом к открытым и служебным данным в Tantor. Построить концептуальную и логическую модели, распределить категории данных по схемам, таблицам и столбцам; согласовать объектные права с шифрованием служебных атрибутов и защитой резервных копий. Представить таблицу проверок разрешённых и запрещённых операций до и после восстановления.
13. Защита записей разных подразделений в общей базе данных. Разработать концептуальную модель и политику доступа на уровне строк, проверить её совместно с объектными правами, шифрованием и восстановлением.
14. Безопасный доступ к данным через представления и подпрограммы. Спроектировать учебную БД, ограничить прямой доступ, реализовать минимальные полномочия и проверить контролируемые операции пользователей.
15. Перенос политики доступа между моделями SQL-разрешений. Для учебной БД сопоставить GRANT, REVOKE и DENY в поддерживающей запрет СУБД с возможностями PostgreSQL/Tantor; реализовать и проверить эквивалентную политику в Tantor.
16. Комплексная защита данных средствами шифрования и ролевого доступа в Tantor. Определить защищаемые атрибуты, выбрать доступный механизм, разделить права на данные и ключи и проверить восстановление доступа.
17. Организация защищённого резервного копирования базы данных Tantor. Спроектировать учебную БД и роли, обосновать состав и хранение копий, реализовать защиту резервов и провести контрольное восстановление.
18. Восстановление учебной БД после ошибочного изменения данных. Разработать модель и политику доступа, подготовить резервирование и сценарии сбоя, оценить полноту восстановления данных и разрешений.
19. Управление жизненным циклом ролей в базе данных Tantor. Реализовать выдачу, изменение и прекращение доступа, передачу владения объектами и проверку отсутствия остаточных полномочий, защитить резервные копии.
20. Комплексная проверка безопасности учебной автоматизированной системы на базе Tantor. Спроектировать модель данных и доступа, реализовать шифрование и резервирование, провести положительные и отрицательные испытания и обосновать устранение выявленных недостатков.

Примерный перечень вопросов к защите курсовой работы

21. Какую задачу предметной области решает работа и какие требования к безопасности приняты?
22. Какие активы, субъекты, объекты и угрозы учитывает разработанная модель безопасности?
23. Как построена концептуальная модель, какие сущности и связи в ней выделены?

24. Как концептуальная модель преобразована в схему таблиц и ограничения целостности?
25. Какие действия каждого типа пользователя отражены в матрице доступа и почему выбран такой объём полномочий?
26. Как реализовано разделение обязанностей владельца объектов, администратора и прикладных пользователей?
27. Какие особенности ролевой модели Tantor использованы в работе?
28. Как членство в ролях и переключение роли влияют на фактические полномочия пользователя?
29. Какие разрешения требуются на уровне базы данных, схемы, таблицы и столбца для выбранной операции?
30. Как проверялись выдача и отзыв прав командами GRANT и REVOKE?
31. Чем явный запрет DENY в поддерживающих его СУБД отличается от отсутствия разрешения; как реализуется нужная политика в Tantor?
32. Как исключены избыточные разрешения и неконтролируемая передача полномочий?
33. Почему выбран прямой доступ, представления, подпрограммы либо защита на уровне строк и как проверено это решение?
34. Как проверялись разрешённые и запрещённые операции от имени разных пользователей?
35. Какие угрозы устраняет выбранное шифрование и какие угрозы оно не устраняет?
36. На каком уровне защищаются данные при передаче и хранении и чем обоснован выбор механизма?
37. Как организованы хранение, доступ и смена ключей шифрования в учебной конфигурации?
38. Как обеспечивается совместное применение шифрования и ролевого разграничения доступа?
39. Как определены допустимая потеря данных и требуемое время восстановления?
40. Почему выбран соответствующий способ резервного копирования и какие объекты входят в копию?
41. Как защищены резервные копии и проверена их пригодность к восстановлению?
42. Какие действия выполнялись при контрольном восстановлении и как проверялись данные, владельцы и права?
43. Какие недостатки обнаружены при испытаниях и какими результатами подтверждено их устранение?
44. Какие ограничения имеет разработанное решение и как его можно применять и развивать в автоматизированной системе?