ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО РЫБОЛОВСТВУ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
(ФГБОУ ВО «КГТУ»)
БГАРФ

УТВЕРЖДАЮ
И.о. декана РТФ
/В.А. Баженов/
27.06 2018 г.

Рабочая программа дисциплины
Безопасность систем баз данных
(наименование дисциплины)
базовой части образовательной программы
по специальности
10.05.03 «Информационная безопасность автоматизированных систем»
(код и наименование специальности)
Специализация программы
«Обеспечение информационной безопасности распределенных систем»
(наименование специализации программы)

Радиотехнический факультет
(наименование)

Кафедра – Информационная безопасность
(наименование)

Калининград 2018

Визирование РПД для исполнения в очередном учебном году

Утверждаю: и.о. декана РТФ_____ В.А. Баженов
«24» 06 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2018-2019 учебном году на заседании кафедры
Информационной безопасности
Протокол от «14» 06 2018 г. № 9
Зав. кафедрой ИБ_____Великите Н.Я.

Визирование РПД для исполнения в очередном учебном году

Утверждаю: и.о. декана РТФ_____ В.А. Баженов
«____» _____ 2019 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры
Информационной безопасности
Протокол от «____» __ 2019 г. №_____
Зав. кафедрой ИБ_____Великите Н.Я.

Визирование РПД для исполнения в очередном учебном году

Утверждаю:и.о. декана РТФ_____ В.А. Баженов
«____» _____ 2020 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры
Информационной безопасности
Протокол от «____» __ 2020г. №_____
Зав. кафедрой ИБ_____Великите Н.Я.

Визирование РПД для исполнения в очередном учебном году

Утверждаю: и.о. декана РТФ_____ В.А. Баженов
«____» _____ 2021 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры
Информационной безопасности
Протокол от «____» __ 2021 г. №_____
Зав. кафедрой ИБ_____Великите Н.Я.

1. Цель освоения дисциплины

Целью освоения дисциплины является формирование у обучаемых компетенций, необходимых для профессиональной деятельности в области обеспечения информационной безопасности систем баз данных, их теоретическая и практическая подготовка по вопросам безопасности систем баз данных, освоение основных положений теории баз данных, методов решения задач, связанных с проблемами обеспечения их информационной безопасности на этапах проектирования и эксплуатации.

2. Результаты освоения дисциплины

Обучающийся должен овладеть следующими компетенциями, формируемыми в результате освоения дисциплины:

ОПК-3 - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	
Знать:	
Уровень 1	иметь представление об основных математических моделях данных и способах их интерпретации средствами вычислительной техники
Уровень 2	способы построения математических моделей данных и способы их интерпретации средствами вычислительной техники
Уровень 3	программные средства для построения математических моделей данных и особенности их реализации средствами вычислительной техники
Уметь:	
Уровень 1	реализовывать простые модели данных средствами СУБД с графическим интерфейсом
Уровень 2	создавать простые модели данных языковыми средствами СУБД с SQL интерфейсом
Уровень 3	создавать модели данных, запросы и формы различной сложности языковыми средствами СУБД с различными интерфейсами
Владеть:	
Уровень 1	навыками использования средств программирования локальных баз данных с преимущественно графическим интерфейсом
Уровень 2	навыками использования средств программирования баз данных, в том числе с SQL интерфейсом
Уровень 3	навыками использования средств программирования как локальных, так и удаленных баз данных, в том числе с SQL интерфейсом

ОПК-8 – способностью к освоению новых образцов программных, технических средств и информационных технологий	
Знать:	
Уровень 1	разновидности программных, технических средств и информационных технологий
Уровень 2	разновидности программных, технических средств и информационных технологий; функциональные возможности и назначение различных видов программных, технических средств и информационных технологий;
Уровень 3	разновидности программных, технических средств и информационных технологий; функциональные возможности и назначение различных видов программных, технических средств и информационных технологий; общие методологические приемы их освоения;
Уметь:	
Уровень 1	осваивать различные виды программных, технических средств и информационных технологий
Уровень 2	осваивать различные виды программных, технических средств и информационных технологий; использовать общие методологические приемы по их освоению
Уровень 3	осваивать разновидности программных, технических средств и информационных технологий; использовать общие методологические приемы их освоения; осваивать функциональные возможности различных видов программных, технических средств и информационных технологий
Владеть:	
Уровень 1	навыками освоения программных и технических средств, а также информационных технологий по проектированию и эксплуатации баз данных
Уровень 2	навыками освоения программных и технических средств, а также информационных технологий по проектированию и эксплуатации баз данных; навыками использования общих методологических приемов по их освоению
Уровень 3	навыками освоения программных и технических средств, а также информационных технологий по проектированию и эксплуатации баз данных; навыками использования общих методологических приемов по их освоению; навыками работы с СУБД на различных платформах

ПК-3: - способностью проводить анализ защищенности автоматизированных систем	
Знать:	
Уровень 1	требования и признаки защищенных систем, критерии защищенности БД
Уровень 2	требования и признаки защищенных систем, критерии защищенности БД, угрозы информационной безопасности баз данных

Уровень 3	требования и признаки защищенных систем, критерии защищенности БД, угрозы информационной безопасности баз данных, критерии оценки надежных компьютерных систем, средства аудита информационной безопасности
Уметь:	
Уровень 1	выявлять объективно существующие угрозы информационной безопасности баз данных
Уровень 2	выявлять объективно существующие угрозы информационной безопасности баз данных, выявлять источники этих угроз с учетом среды эксплуатации БД, определять субъекты информационных отношений на уровне предметной области и их интересы
Уровень 3	выявлять объективно существующие угрозы информационной безопасности баз данных, выявлять источники этих угроз с учетом среды эксплуатации БД, определять субъекты информационных отношений на уровне предметной области и их интересы, оценивать методы противодействия нарушениям конфиденциальности, методы управления доступом, соотношение доступности и защищенности данных
Владеть:	
Уровень 1	навыками анализа уровня информационной безопасности баз данных
Уровень 2	навыками анализа уровня информационной безопасности баз данных, навыками анализа методов и средств противодействия нарушениям конфиденциальности, управления доступом
Уровень 3	навыками анализа методов и средств противодействия нарушениям конфиденциальности, управления доступом, целостности БД, аудита защищенности СУБД

ПК-22 – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
Знать:	
Уровень 1	сущность политики безопасности и цель формализации политики информационной безопасности
Уровень 2	сущность политики безопасности и цель формализации политики информационной безопасности; принципы построения защищенных систем баз данных
Уровень 3	сущность политики безопасности и цель формализации политики информационной безопасности; принципы построения защищенных систем баз данных; стратегию применения средств обеспечения информационной безопасности
Уметь:	
Уровень 1	формулировать в терминах естественного языка правила и нормы политики информационной безопасности; общие принципы и конкретные правила работы с информационными ресурсами, в том числе, баз данных для различных категорий пользователей

Уровень 2	формулировать в терминах естественного языка правила и нормы политики информационной безопасности; общие принципы и конкретные правила работы с информационными ресурсами, в том числе, баз данных для различных категорий пользователей; оформлять документально политику безопасности для разных уровней управления
Уровень 3	формулировать в терминах естественного языка правила и нормы политики информационной безопасности; общие принципы и конкретные правила работы с информационными ресурсами, в том числе, баз данных для различных категорий пользователей; оформлять документально политику безопасности для разных уровней управления; выбирать стратегию применения средств обеспечения информационной безопасности
Владеть:	
Уровень 1	навыками формулирования правил и норм политики информационной безопасности, общих принципов и конкретных правил работы с информационными ресурсами, в том числе, баз данных для различных категорий пользователей
Уровень 2	навыками формулирования правил и норм политики информационной безопасности, общих принципов и конкретных правил работы с информационными ресурсами, в том числе, баз данных для различных категорий пользователей; навыками разработки и документального оформления политики безопасности для разных уровней управления
Уровень 3	навыками формулирования правил и норм политики информационной безопасности, общих принципов и конкретных правил работы с информационными ресурсами, в том числе, баз данных для различных категорий пользователей; навыками разработки и документального оформления политики безопасности для разных уровней управления; методологией выбора стратегии применения средств обеспечения информационной безопасности

ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Знать:	
Уровень 1	меры по обеспечению защиты информации ограниченного доступа: меры по предотвращению несанкционированного доступа с использованием паролей; методы разграничения прав доступа (методы дискреционного доступа, разграничения; метод разграничения доступа на основе ролей; мандатная модель доступа в СУБД); идентификации и аутентификации пользователей
Уровень 2	меры по обеспечению защиты информации ограниченного доступа: меры по предотвращению несанкционированного доступа с использованием паролей; разграничение прав доступа (методы дискреционного разграничения доступа; метод разграничения доступа на основе ролей; мандатная модель доступа в СУБД); процедуры идентификация и аутентификация пользователей;

Уровень 3	меры по обеспечению защиты информации ограниченного доступа: меры по предотвращению несанкционированного доступа с использованием паролей; разграничение прав доступа (методы дискреционного разграничения доступа; метод разграничения доступа на основе ролей; мандатная модель доступа в СУБД); процедуры идентификация и аутентификация пользователей; виды нормативных актов и инструкций по обеспечению защиты информации ограниченного доступа
Уметь:	
Уровень 1	разрабатывать меры по предотвращению несанкционированного доступа с использованием паролей; выполнять разграничение прав доступа различными методами;
Уровень 2	разрабатывать меры по предотвращению несанкционированного доступа с использованием паролей; выполнять разграничение прав доступа различными методами; использовать процедуры аутентификации пользователей
Уровень 3	разрабатывать меры по предотвращению несанкционированного доступа с использованием паролей; выполнять разграничение прав доступа различными методами; использовать процедуры аутентификации пользователей; разрабатывать акты и инструкции по обеспечению защиты информации ограниченного доступа
Владеть:	
Уровень 1	методами предотвращения несанкционированного доступа с использованием паролей; методами разграничения прав доступа
Уровень 2	методами предотвращения несанкционированного доступа с использованием паролей; методами разграничения прав доступа; методами аутентификации пользователей
Уровень 3	методами предотвращения несанкционированного доступа с использованием паролей; методами разграничения прав доступа; методами аутентификации пользователей; методикой разработки актов и инструкций по обеспечению защиты информации ограниченного доступа

ПК-24 – способностью обеспечивать эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать:	
Уровень 1	угрозы целостности СУБД, основные виды и причины возникновения угроз целостности, доступности, конфиденциальности
Уровень 2	угрозы целостности СУБД, основные виды и причины возникновения угроз целостности, доступности, конфиденциальности, способы противодействия угрозам
Уровень 3	угрозы целостности СУБД, основные виды и причины возникновения угроз целостности, доступности, конфиденциальности, способы противодействия угрозам, аудита информационной безопасности
Уметь:	
Уровень 1	разрабатывать проектные и эксплуатационные решения и режимы с учетом требований обеспечения целостности, доступности, конфиденциальности

Уровень 2	разрабатывать проектные и эксплуатационные решения и режимы с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам
Уровень 3	разрабатывать проектные и эксплуатационные решения и режимы с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам, проводить аудит информационной безопасности
Владеть:	
Уровень 1	методами проектирования и эксплуатации СУБД с учетом требований обеспечения целостности, доступности, конфиденциальности
Уровень 2	методами проектирования и эксплуатации СУБД с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам
Уровень 3	методами проектирования и эксплуатации СУБД с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам, проводить аудит информационной безопасности

ПК-25 – способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать:	
Уровень 1	требования и признаки защищенных систем
Уровень 2	требования и признаки защищенных систем, критерии защищенности БД
Уровень 3	требования и признаки защищенных систем, критерии защищенности БД, средства защиты баз данных и восстановления БД
Уметь:	
Уровень 1	использовать методы противодействия нарушениям конфиденциальности
Уровень 2	использовать методы противодействия нарушениям конфиденциальности, управлять доступом
Уровень 3	использовать методы противодействия нарушениям конфиденциальности, управлять доступом, выбирать разумное соотношение доступности и защищенности данных
Владеть:	
Уровень 1	средствами противодействия нарушениям конфиденциальности
Уровень 2	средствами противодействия нарушениям конфиденциальности, управления доступом
Уровень 3	средствами противодействия нарушениям конфиденциальности, управления доступом, аудита защищенности СУБД

ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	
Знать:	
Уровень 1	причины проведения мониторинга и аудита систем баз данных

Уровень 2	причины проведения мониторинга и аудита систем баз данных; общую характеристику средств аудита СУБД
Уровень 3	причины проведения мониторинга и аудита систем баз данных; общую характеристику средств аудита СУБД; работы по реализации частных политик аудита баз данных
Уметь:	
Уровень 1	обосновывать причины проведения мониторинга и аудита систем баз данных
Уровень 2	обосновывать причины проведения мониторинга и аудита систем баз данных; использовать средства аудита СУБД
Уровень 3	обосновывать причины проведения мониторинга и аудита систем баз данных; использовать средств аудита СУБД; выполнять работы по реализации частных политик аудита баз данных в составе автоматизированных систем
Владеть:	
Уровень 1	методикой проведения мониторинга и аудита систем баз данных
Уровень 2	методикой проведения мониторинга и аудита систем баз данных; методикой использования средств аудита СУБД
Уровень 3	методикой проведения мониторинга и аудита систем баз данных; методикой использования средств аудита СУБД; методикой выполнения работ по реализации частных политик аудита баз данных в составе автоматизированных систем

ПК-28 – способностью управлять информационной безопасностью автоматизированной системы	
Знать:	
Уровень 1	угрозы целостности СУБД, основные виды и причины возникновения угроз целостности, доступности, конфиденциальности
Уровень 2	угрозы целостности СУБД, основные виды и причины возникновения угроз целостности, доступности, конфиденциальности, способы противодействия угрозам
Уровень 3	угрозы целостности СУБД, основные виды и причины возникновения угроз целостности, доступности, конфиденциальности, способы противодействия угрозам, аудита информационной безопасности
Уметь:	
Уровень 1	разрабатывать проектные и эксплуатационные решения и режимы с учетом требований обеспечения целостности, доступности, конфиденциальности
Уровень 2	разрабатывать проектные и эксплуатационные решения и режимы с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам

Уровень 3	разрабатывать проектные и эксплуатационные решения и режимы с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам, проводить аудит информационной безопасности
Владеть:	
Уровень 1	методами проектирования и эксплуатации СУБД с учетом требований обеспечения целостности, доступности, конфиденциальности
Уровень 2	методами проектирования и эксплуатации СУБД с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам
Уровень 3	методами проектирования и эксплуатации СУБД с учетом требований обеспечения целостности, доступности, конфиденциальности, способов противодействия угрозам, проводить аудит информационной безопасности

ПСК-7.4 – способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	
Знать:	
Уровень 1	задачи и средства администратора БД
Уровень 2	задачи и средства администратора БД, понятие политики безопасности для распределенных информационных систем
Уровень 3	задачи и средства администратора БД, понятие политики безопасности для распределенных информационных систем, средства и режимы администрирования баз данных для распределенных информационных систем
Уметь:	
Уровень 1	применять различные политики безопасности в рамках единой модели
Уровень 2	применять различные политики безопасности в рамках единой модели, разрабатывать меры противодействия угрозам доступности, целостности и конфиденциальности систем баз данных
Уровень 3	применять различные политики безопасности в рамках единой модели, разрабатывать меры противодействия угрозам доступности, целостности и конфиденциальности, безопасности распределенных СУБД
Владеть:	
Уровень 1	навыками удаленного администрирования СУБД для распределенных систем
Уровень 2	навыками удаленного администрирования СУБД для распределенных систем, методами управления доступом – субъекты и объекты, группы пользователей, привилегии, роли и представления
Уровень 3	навыками оперативного администрирования СУБД для распределенных систем, методами управления доступом – субъекты и объекты, группы пользователей, привилегии, роли и представления, навыками аудита информационной безопасности.

В результате освоения дисциплины обучающийся должен:

Знать:

- методы абстрагирования данных;

- характеристики и типы систем БД;
- области применения СУБД;
- этапы проектирования БД;
- средства поддержания целостности;
- критерии защищенности БД;
- угрозы безопасности БД;
- критерии и методы оценивания механизмов защиты;
- особенности организации средств защиты в распределенных СУБД.

Уметь:

- выделять сущности и связи в предметной области;
- отображать предметную область в конкретную модель данных;
- пользоваться средствами защиты СУБД;
- создавать дополнительные средства защиты;
- проводить анализ и оценивание механизмов защиты.

Владеть:

- навыками работы со средствами поддержания интерфейса с различными категориями пользователей;
- навыками работы с СУБД на различных платформах;
- навыками разработчика и администратора БД;
- работы со средствами обеспечения целостности и конфиденциальности в БД;
- работы администратора по защите БД.

3. Место дисциплины в структуре образовательной программы

Дисциплина (модуль) Б1.Б.23 «Безопасность систем баз данных» относится к дисциплинам (модулям) базовой части блока 1 ОП ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных систем».

Дисциплина изучается на 4 курсе в 7 семестре.

Дисциплина логически взаимосвязана с дисциплинами профессионального цикла, изучающими основы информационной безопасности, организационное и правовое обеспечение информационной безопасности, вопросы безопасности операционных систем. В связи с этим для успешного освоения дисциплины студент должен иметь базовую подготовку по дисциплинам «Информатика», «Языки программирования», «Безопасность операционных систем», «Основы информационной безопасности», «Теория информации», «Безопасность сетей электронных вычислительных машин», «Правовое обеспечение информационной безопасности».

Дисциплина «Безопасность систем баз данных» предусматривает систематизированное изучение основных концептуальных подходов к проектированию баз данных и их эксплуатации, обеспечению их информационной безопасности, развитие у студентов умения применять на практике полученные знания для решения задач их будущей профессиональной деятельности.

Изучение дисциплины необходимо для успешного освоения дисциплин профессионального цикла и практик, формирующих компетенции ОПК-3, ОПК-8, ПК-3, ПК-22, ПК-23, ПК-24, ПК-25, ПК-27, ПК-28, ПСК-7.4. Она является предшествующей для изучения таких дисциплин, как «Методы проектирования защищенных распределенных информационных систем», «Информационная безопасность распределенных информационных систем», «Технология построения защищенных распределенных информационных систем».

Знания и практические навыки, полученные в ходе изучения данной дисциплины, используются студентами при выполнении курсовых и дипломных работ.

4. Содержание дисциплины (по разделам и темам)

Раздел 1. Введение. Основы построения и эксплуатации баз данных

Тема 1.1. Введение в дисциплину. Назначение и роль баз данных. История развития вопроса безопасности баз данных

Предмет и задачи дисциплины. Общие требования к хранению информации. Назначение и роль баз данных в составе автоматизированных информационных систем. Классификация задач, решаемых с использованием технологии баз данных.

Тема 1.2. Модели данных

Отображение предметной области. Сущности и связи. Методы абстрагирования данных. Иерархическая, сетевая, реляционная, объектная модели данных. Области применения моделей данных.

Тема 1.3. Математические основы построения реляционных СУБД

Реляционные исчисления, построенные на доменах и кортежах. Реляционная алгебра и безопасные выражения. Алгебра отношений, моделирование теоретико-множественных операций.

Раздел 2. СУБД – средства управления данными в БД

Тема 2.1. Общие принципы построения СУБД

Понятие СУБД. Концептуальные основы реляционных БД. Основные понятия СУБД, компоненты, языки.

Состав и архитектура СУБД.

Информационное, лингвистическое, математическое, аппаратное, организационное, правовое обеспечения СУБД.

Тема 2.2. Эксплуатация баз данных. Состав и проведение регламентных работ

Состав, порядок планирования и проведения регламентных работ. Сервисные средства СУБД. Задачи администратора базы данных. Организация труда обслуживающего персонала.

Раздел 3. Организация вычислений в среде клиент / сервер

Тема 3.1. Технология и модели архитектуры клиент/сервер /

Архитектура систем управления базами данных. Понятие сервера и клиента. Архитектура «клиент – сервер», назначение, преимущества и недостатки.

Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование СУБД. Механизмы блокирования и управления доступом в многопользовательской среде.

Тема 3.2. Серверы баз данных

Использование средств прямого ввода-вывода, управления памятью, поддержания целостности, защиты от сбоев. Настройка механизмов поддержания целостности на примере сервера СУБД MS Access. Возможности по обработке неструктурированных данных большого объема. Поддержка работы в сети Internet. Оценка эффективности и адаптации функционирования сервера баз данных (тесты производительности). Методы оптимизации доступа к базе данных.

Тема 3.3. Клиентская часть архитектуры клиент/сервер

Средства поддержания интерфейса с различными категориями пользователей. Языки запросов. Языки описания данных. Языки манипулирования данными. Стандарты SQL. Языки четвертого поколения (4GL, PL/SQL). Использование курсоров в языке PL/SQL Oracle.

Интерфейс языков СУБД с языками программирования высокого уровня (C++, .NET, Java и др.). Средства реализации диалогового интерфейса и подготовки отчетов в языках СУБД. Клиентское приложение Oracle SQL*Plus. Стандарты на графический пользовательский интерфейс (GUI). Тонкие клиенты БД и пограничные интерфейсы пользователей.

Тема 3.4. Интерфейс между клиентом и сервером

Протоколы согласованной работы. Распределенные базы данных в сетях ЭВМ. Средства интеграции и взаимодействия разнородных распределенных баз данных. Поддержка Internet. Интерфейсы доступа к БД (ODBC, JDBC).

Раздел 4. Проектирование баз данных

Тема 4.1. Задачи и этапы проектирования БД

Использование нормальных форм при проектировании приложений в реляционных СУБД. Аномалии при эксплуатации баз данных. Нормализация отношений.

Методологии проектирования. Этапы нормализации отношений.

Тема 4.2. Автоматизированное проектирование

Основы CASE-технологии. Классификация CASE-средств. Современные CASE-пакеты.

Раздел 5. Концепции безопасности БД

Тема 5.1. Понятие безопасности БД

Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Критерии качества баз данных. Понятие безопасности баз данных. Классификация угроз информационной безопасности баз данных.

Тема 5.2. Многоуровневая защита

Понятие многоуровневой защиты баз данных. Защита от любых несанкционированных действий или атак. Кэширование. Аудит и маскирование.

Раздел 6. Теоретические основы безопасности в СУБД

Тема 6.1. Критерии защищенности БД

Обеспечение конфиденциальности информации. Обеспечение целостности. Обеспечение доступности.

Тема 6.2. Модели безопасности СУБД

Модель дискреционного управления доступом.
Базовая ролевая модель разграничения доступа.
Мандатная модель доступа.

Раздел 7. Механизмы обеспечения целостности СУБД

Тема 7.1. Угрозы целостности СУБД /Лек/

Угрозы целостности информации, специфические для систем управления базами данных. Возможность модификации данных в реляционных СУБД с помощью SQL-операторов.

Тема 7.3. Понятие транзакции

Понятие транзакции. Примеры транзакций. Свойства транзакций. Уровни изолированности транзакций. Журнал транзакций и сегмент отката.

Тема 7.4. Блокировки

Понятие блокировки. Три уровня блокировок: блокировка базы даны;. блокировка таблицы. Блокировка страницы.

Тема 7.5. Ссылочная целостность

Понятие ссылочной целостности в базах данных. Поддержание ссылочной целостности в БД. Причины нарушений. Пустые внешние ключи. Ссылочная целостность на триггерах. Ссылочная целостность на внешних ключах.

Тема 7.6. Правила. Триггеры. События

Понятие события, правила и процедуры (триггера) в базах данных. Суть идеи механизма событий, правил и процедур Их взаимосвязь.

Раздел 8. Механизмы обеспечения конфиденциальности в СУБД

Тема 8.1. Классификация угроз конфиденциальности СУБД

Понятие конфиденциальности. Источники угроз конфиденциальности. Классификация угроз конфиденциальности в СУБД: инъекция SQL; логический вывод на основе функциональных зависимостей; логический вывод на основе ограничений целостности; использование оператора Update для получения конфиденциальной информации. Аудит событий, связанных с доступом к объекту.

Тема 8.2. Средства идентификации и аутентификации

Понятие авторизации, идентификации и аутентификации и их связь.

Аутентификация на основе паролей. Аутентификация на основе наличия у пользователя некоторого конфиденциального предмета. Аутентификация на основе на основе проверки некоторых уникальных характеристик пользователя (на основе биометрических характеристик).

Тема 8.3. Средства управления доступом /

Привилегия как базовое понятие системы разграничения доступа. Системная привилегия. Привилегия доступа к объекту.

Роли и разграничение доступа на основе ролей. Административные привелегии. Привилегии безопасности.

Тема 8.4. Аудит и подотчетность

Причины проведения аудита. Общая характеристика средств аудита СУБД. Журнал аудита. Аудит событий, связанных с доступом к объекту.

Раздел 9. Механизмы, поддерживающие высокую готовность

Тема 9.1. Средства, поддерживающие высокую готовность /

Средства, поддерживающие высокую готовность. Функциональная насыщенность СУБД. Системы, обладающие свойством высокой надежности.

Тема 9.2.Оперативное администрирование

Понятие оперативного администрирования баз данных, функции и роли администраторов. Управление целостностью данных в системах управления базами данных, буферизация, транзакция, журнализация. Управление безопасностью в системах, источники нарушения целостности данных.

Тема 9.3.Функциональная насыщенность СУБД

Понятие функциональной насыщенности СУБД. Аппаратная избыточность. Зеркалирование дисков. Тиражирование.

Раздел 10. Защита данных в распределенных системах

Тема 10.1. Распределенные вычислительные среды

Распределенная обработка информации в среде клиент - сервер. Концепция распределенной вычислительной среды DCE. Распределенные базы данных в сетях ЭВМ.

Технологии удаленного доступа к системам баз данных. Тиражирование и синхронизация в распределенных системах баз данных.

Тема 10.2 Угрозы безопасности распределенных СУБД

Угрозы доступности, целостности и конфиденциальности данных. Механизмы противодействия. Средства безопасности СУБД.

Тема 10.3. Распределенная обработка данных

Понятие распределенной транзакции. Модель обработки транзакции. Корпоративная среда обработки транзакций. Защищенные протоколы фиксации. Обработка распределенных транзакций в базах данных с многоуровневой секретностью.

Тема 10.4. Протоколы фиксации

Понятие протокола фиксации транзакций. Механизм действия.

Тема 10.5. Тиражирование данных

Понятие тиражирования данных. Назначение. Технология тиражирования данных в распределенных системах.

Тема 10.6. Интеграция БД в интернет

Современные тенденции. Обзор современных технологий (WEBDBC и другие). Вопросы безопасности: угрозы и методы противодействия. Перспективы развития.

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации по ней

5.1 Объем (трудоемкость освоения) и структура дисциплины, формы аттестации по ней для очной формы обучения.

Номер и наименование раздела, темы	Объем учебной работы (час.)					
	Лекции	ЛЗ	ПЗ	СРС	КСР	Всего
Семестр - седьмой (6 ЗЕТ, 216 час., из них 45 часов КСР)						
Раздел 1. Введение. Основы построения и эксплуатации баз данных						
Тема 1.1. Введение в дисциплину. Назначение и роль баз данных. История развития вопроса безопасности баз данных	1	-				1
Тема 1.2. Модели данных	1	4			1	6
Тема 1.3. Математические основы построения реляционных СУБД	1					1
Тема 1.4. Математические модели СУБД				1	1	2
Раздел 2 СУБД – средства управления данными в БД						
Тема 2.1. Общие принципы построения СУБД	1	4				5
Тема 2.2. Эксплуатация баз данных. Состав и проведение регламентных работ	1					1
Тема 2.3 Средства управления данными в БД				1	1	2
Раздел 3. Организация вычислений в среде клиент / сервер						
Тема 3.1 Технология и модели архитектуры клиент/сервер	1	4			1	6
Тема 3.2 Серверы баз данных	1	4				5

Тема 3.3 Клиентская часть архитектуры клиент/сервер	1					1
Тема 3.4 Интерфейс между клиентом и сервером	1					1
Тема 3.5 Организация вычислений в среде «клиент-сервер»				1	1	2
Раздел 4. Проектирование баз данных						
Тема 4.1 Задачи и этапы проектирования БД /Лек/	1	4			1	6
Тема 4.2 Автоматизированное проектирование /Лек/	1	4			1	6
Тема 4.3 Основы проектирования БД				1	1	2
Раздел 5. Концепции безопасности БД						
Тема 5.1 Понятие безопасности БД	1					1
Тема 5.2 Многоуровневая защита	1					1
Тема 5.3 Концепции безопасности БД				1	1	2
Раздел 6. Теоретические основы безопасности в СУБД						
Тема 6.1 Критерии защищенности БД	1					1
Тема 6.2 Модели безопасности СУБД	1					1
Тема 6.3 Основы безопасности БД. Руководящие материалы				1	1	2
Раздел 7. Механизмы обеспечения целостности СУБД						
Тема 7.1 Угрозы целостности СУБД	1					1
Тема 7.2 Метаданные и словарь данных	1					1
Тема 7.3 Понятие транзакции	1	4			1	6
Тема 7.4Блокировки	1					1
Тема 7.5 Ссылочная целостность	1	4			1	6
Тема 7.6 Правила. Триггеры. События	1					1
Тема 7.7 Обеспечение целостности в БД				1	1	2
Раздел 8. Механизмы обеспечения конфиденциальности в СУБД						
Тема 8.1 Классификация угроз конфиденциальности СУБД	1					1
Тема 8.2 Средства идентификации и аутентификации	1	4			1	6
Тема 8.3 Средства управления доступом	1	4			1	6
Тема 8.4 Аудит и подотчетность	1					1
Тема 8.5 Обеспечение конфиденциальности в БД				1	1	2
Раздел 9. Механизмы, поддерживающие высокую готовность						
Тема 9.1 Средства, поддерживающие высокую готовность	1					1
Тема 9.2 Оперативное администрирование	1					1
Тема 9.3 Функциональная насыщенность СУБД	1					1
Тема 9.4 Средства обеспечения высокой готовности				1	1	2
Раздел 10. Защита данных в распределенных системах						
Тема 10.1 Распределенные вычислительные среды	1					1
Тема 10.2 Угрозы безопасности распределенных СУБД	1					1
Тема10.3 Распределенная обработка данных	1					1

Тема 10.4 Протоколы фиксации	1					1
Тема 10.5 Тиражирование данных	1					1
Тема 10.6 Интеграция БД в интернет	1					1
Тема10.7 Средства защиты данных в распределенных системах				2	2	4
Подготовка к лабораторным занятиям, оформлени отчетов				10	10	20
Подготовка сообщений, докладов, рефератов, презентаций по вопросам, вынесенным на самостоятельную проработку (по заданию преподавателя)				2	2	4
Работа с учебниками, иной учебной и учебно-методической литературой, Интернет-источниками				8	8	16
Проверка выполнения практических заданий на компьютере					2	2
Выполнение КР (КП)				20	4	24
Подготовка к сдаче и сдача экзамена				18		18
Всего в семестре	**34**	**68**		**69**	**45**	**216**
	102					
Итого по дисциплине	**34**	**68**		**69**	**45**	**216**
	102					

Учебным планом предусмотрено изучение материала также и в интерактивных формах в объёме 25 часов

5.2 Объем (трудоемкость освоения) и структура дисциплины, формы аттестации по ней для заочной формы обучения – не предусмотрено.
5.3 Объем (трудоемкость освоения) и структура дисциплины, формы аттестации по ней для заочной ускоренной формы обучения – не предусмотрено.

6. Лабораторные занятия

6.1 Лабораторные работы по очной форме обучения:

Номер Л/Р	**Номер раздела дисциплины**	**Наименование лабораторной работы**	**Кол-во часов Л/З**
Семестр - седьмой			
1.	2	Основные понятия реляционной СУБД	4
2.	2, 7	Создание базы данных	4
3.	3	Сверка данных	4
4.	3	Импорт данных	4
5.	4	Выполнение запросов данных	4
6.	4	Выполнение фильтрации данных	4
10	10	Средства обеспечения целостности на этапе разработки БД	4
7.	7	Особенности выполнение транзакций в БД	4

8.	7	Использование форм	4
9.	4	Практическое знакомство со средствами языка SQL	4
11.	8	Создание и сопровождение БД средствами языка SQL	4
12.	8	Начало работы с СУБД My SQL	4
13.	9	Средства обеспечения высокой готовности в распределенных БД	4
14.	9	Исследование проблем при работе с базой данных на примере БД электронного магазина	4
15.	10	Использование языка PHP для управления обменом данными в БД. Уязвимости.	4
16.	10	Использование языка PHP для управления обменом данными. Способы противодействия угрозам	4
17.	10	Создание простейшей базы данных	4
Всего			**68**

6.2 Лабораторные работы по заочной форме обучения – не предусмотрены.

6.3 Лабораторные работы для заочной ускоренной формы обучения – не предусмотрены.

7. Практические занятия

7.1 Практические занятия по очной форме обучения не предусмотрены.

7.2 Практические занятия по заочной форме обучения не предусмотрены.

7.3 Практические занятия по заочной ускоренной форме обучения не предусмотрены.

8. Самостоятельная работа студента

8.1 Самостоятельная работа студента очной формы обучения:

№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации
1.	Изучение теоретического материала по теме «Математические модели СУБД»	1	Проверка конспекта, устный опрос, оценка результатов
2.	Изучение теоретического материала по теме «Средства управления данными в БД»	1	Проверка конспекта, устный опрос, оценка результатов
3.	Изучение теоретического материала по теме «Организация вычислений в среде клиент-сервер»	1	Проверка конспекта, устный опрос, оценка результатов
4.	Изучение теоретического материала по теме «Основы проектирования баз данных»	1	Проверка конспекта, устный опрос, оценка результатов
5.	Изучение теоретического материала по теме «Концепция безопасности БД»	1	Проверка конспекта, устный опрос, оценка результатов
6.	Изучение теоретического материала по теме «Основы безопасности БД. Руководящие материалы»	1	Проверка конспекта, устный опрос, оценка результатов

7.	Изучение теоретического материала по теме «Обеспечение целостности в БД»	1	Проверка конспекта, устный опрос, оценка результатов
8.	Изучение теоретического материала по теме «Обеспечение конфиденциальности в БД»	1	Проверка конспекта, устный опрос, оценка результатов
9.	Изучение теоретического материала по теме «средства обеспечения высокой готовности»	1	Проверка конспекта, устный опрос, оценка результатов
10.	Изучение теоретического материала по теме «Средства защиты данных в распределенных системах»	2	Проверка конспекта, устный опрос, оценка результатов
11.	Подготовка к лабораторным занятиям, оформление отчетов	10	Проверка конспекта, устный опрос, оценка результатов
12.	Подготовка сообщений, докладов, рефератов, презентаций по вопросам, вынесенным на самостоятельную проработку (по заданию преподавателя)	2	Заслушивание сообщений, докладов, рефератов и презентаций в группе, их оценка
13.	Работа с учебниками, иной учебной и учебно-методической литературой, Интернет-источниками	8	Проверка конспекта лекций, письменных ответов на вопросы курса
14.	Выполнение курсовой работы по индивидуальным заданиям согласно тематике, представленной в п. 8.2	20	Защита курсовой работы, зачет с оценкой
15.	Подготовка к итоговой аттестации по дисциплине	18	Устный опрос по экзаменационным вопросам, экзамен
Итого		**69**	

8.2 Перечень примерных тем курсовых работ по дисциплине «Безопасность систем баз данных»:

1) Проектирование защищенной базы данных библиотеки.
2) Проектирование защищенной базы данных отдела кадров.
3) Проектирование защищенной базы данных электронного магазина.
4) Проектирование защищенной базы данных поликлиники.
5) Проектирование защищенной базы данных системы электронного документооборота.
6) Проектирование защищенной базы данных отдела кадров коммерческой организации.
7) Проектирование защищенной базы данных отдела кадров учебной организации.
8) Проектирование защищенной базы данных склада стройматериалов.
9) Проектирование защищенной базы данных оптово-розничного магазина.
10) Проектирование защищенной базы данных музейного каталога.
11) Проектирование защищенной базы данных билетной кассы.
12) Проектирование защищенной базы данных склада рыбной продукции.
13) Проектирование защищенной базы данных отдела кадров детского учреждения.
14) Проектирование защищенной базы данных учета успеваемости студентов вуза.
15) Проектирование защищенной базы данных магазина автозапчастей.

16) Проектирование защищенной базы данных клиентов охранной организации.
17) Проектирование защищенной базы данных сервисного центра по обслуживанию и ремонту компьютерного оборудования.
18) Проектирование защищенной базы данных складского учета.
19) Проектирование защищенной базы данных учета торгового предприятия.
20) Проектирование защищенной базы данных клиентов энергосети.
21) Проектирование защищенной базы данных клиентов банка.
22) Проектирование защищенной базы данных по продаже железнодорожных билетов.
23) Проектирование защищенной базы данных клиентов системы мобильной связи.
24) Проектирование защищенной базы данных архива.
25) Проектирование защищенной базы данных клиентов жилищно-эксплуатационной организации.

8.3 Самостоятельная работа студента по заочной полной форме обучения – не предусмотрена.
8.4 Самостоятельная работа студента по заочной ускоренной (сокращенной) форме обучения – не предусмотрена.

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

9.1 Основная литература:

1. Астахова И.Ф., Мельников В.М., Толстобров А.П., Фертиков В.В. СУБД. Язык SQL в примерах и задачах: учебное пособие. – М.: Академия, 2007. 168 с. (библиотека БГАРФ – 15 экз.)
2. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с. (библиотека БГАРФ – 30 экз.)

9.2 Дополнительная литература:

1. Агальцов В. П. Базы данных. В 2-х кн. [Текст]: учебник / В. П. Агальцов. - М.: ИД "Форум"; М.: ИНФРА-М.Кн.1: Локальные базы данных. - 2013. - 352 с. (библиотека БГАРФ – 1 экз.)
2. Агальцов В. П. Базы данных. В 2-х кн. [Текст]: учебник / В. П. Агальцов. - М.: ИД "Форум"; М.: ИНФРА-М. Кн.2 : Распределенные и удаленные базы данных. - 2013. - 272 с. (библиотека БГАРФ – 1 экз.)
3. Администрирование Microsoft SQL Server 2000: учебный курс MCSA/ MCSE, MCDBA: экзамен 70-228: официальное пособие для самоподготовки: пер. с англ. / пер. А. П. Харламов. - 2-е изд., испр. - М. : Русская редакция ; СПб. : Питер, 2006. - 610 с. : ил. - (Учебный курс Microsoft). - Предм. указ.: с. 588. (библиотека БГАРФ –1 экз.)
4. Гагарина Л. Г., Кисилев Д.В., Е. Л. Федотова Е.Л.. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие. - М.: ИД "Форум", 2009. - 384 с. (библиотека БГАРФ, 15 экз.)
5. Гольцман В. MySQL 5.0: Практическое пособие. - СПб.: Питер, 2009. - 256 с. (библиотека БГАРФ, 1 экземпляр)
6. Дейт К. Дж. Введение в системы баз данных. М.: ИД Вильямс, 2002. 1072 с. (библиотека БГАРФ, 29 экз.)
7. Информатика. Базовый курс: учебное пособие / ред. С. В. Симонович. - 3-е изд. Стандарт третьего поколения. - СПб. : Питер, 2013. - 640 с. (библиотека БГАРФ – 21 экз.)

8. Мартишин С.А. Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench. Методы и средства проектирования информационных систем и технологий. Инструментальные средства информационных систем: учебное пособие / С. А. Мартишин, В. Л. Симонов, М. В. Храпченко. - М. : ИД "Форум" ; М. : ИНФРА-М, 2012. - 160 с. (библиотека БГАРФ - 3 экз.)
9. Проектирование и реализация баз данных Microsoft SQL Server 2000 : учебный курс MCAD/MCSE, MCDBA: экзамен 70-229: официальное пособие для самоподготовки: пер. с англ. / пер. В. Г. Вшивцев. - 3-е изд. - М. : Русская редакция ; СПб. : Питер, 2005. - 482 с. : ил. - (Учебный курс Microsoft). - Предм. указ.: с. 468. (библиотека БГАРФ – 1 экз.)
10. Суркова Н.Е. Методология структурного проектирования информационных систем [Электронный ресурс]: монография / Н. Е. Суркова, А. В. Остроух. - Красноярск: Научно-инновационный центр, 2014. - 190 с.
11. Фуфаев, Э. В.Базы данных: учебное пособие / Э. В. Фуфаев, Д. Э. Фуфаев. - 4-е изд., - М. : Academia, 2008. - 320 с. (библиотека БГАРФ, 5 экз.)
12. Хомоненко, А.Д. Базы данных: учебник / А. Д. Хомоненко, В. М. Цыганков, М. Г. Мальцев. - 6-е изд., доп. - СПб. : КОРОНА-Век, 2009. - 736 с. (библиотека БГАРФ – 5 экз.)

9.3 Учебно-методические пособия по дисциплине:

1. Капустин В.В. Обеспечение информационной безопасности при проектировании базы данных: Методические указания по выполнению курсовой работы - Калининград: Изд-во БГАРФ, 2010. - 36 с. (библиотека БГАРФ, 42 экземпляра)

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины

При осуществлении образовательного процесса по дисциплине «Безопасность систем баз данных» используются технологии мультимедиа.

Для обеспечения образовательного процесса по дисциплине необходимо следующее программное обеспечение:

- программное обеспечение Microsoft Desktop Education (операционная система Windows Desktop operating system, офисные приложения: Microsoft Office, включая СУБД MS Access) по соглашению V9002148 Open Value Subscription;
- СУБД MS SQL 5.0 , лицензия: свободная GNU General Public Licence / проприетарная EULA;
- средство визуального проектирования баз данных My SQL WorkBench 8.0 12 лицензия: свободная GNU General Public Licence / проприетарная EULA;
- доступ к ресурсам сети «Интернет».

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

1. http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/ - электронный каталог библиотеки БГАРФ
2. https://www.it.ru - Официальный сайт компании АйТи
3. http://elibrary.ru - электронная библиотека Elibrary
4. http://www.bibloclub.ru. электронно-библиотечная система «Университетская библиотека онлайн»:
5. http://elibrary.ru/projects/subscription/rus_titles_open.asp - БД российских научных журналов на Elibrary.ru (РУНЭБ)

6. http://www.garant.ru/ - сайт правовой информационной системы «Гарант»;
7. http://rugost.com – электронный каталог ГОСТов.

11. Материально-техническое обеспечение дисциплины

11.1. Материально-техническое обеспечение для лекционных занятий

Аудитория для проведения лекционных занятий укомплектована необходимой специализированной учебной мебелью и техническими средствами для представления учебной информации студентам. В частности, лекционная аудитория № 302 оснащена следующим образом: 16 учебных парт на 48 посадочных мест, грифельная доска (1 шт.), проекционный экран марки DA-LITE (1 шт.), видеопроектор NEC (1 шт.), телевизора LG (2 шт), стол письменный (2 шт.), стул (2 шт.), персональный компьютер Intel (R) Pentium (1 шт.). На ПК установлено лицензионное программное обеспечение Microsoft Desktop Education, Microsoft Office 2016, Kaspersky Total Space Security Russian Edition.

11.2. Материально-техническое обеспечение для лабораторных занятий

Проведение лабораторных занятий осуществляется в компьютерном классе №248, число компьютеров в рассчитано на 15 рабочих мест.

Состав оборудования: столы учебные – 19 шт., стол преподавательский – 1 шт., стулья учебные – 23 шт., стул преподавательский – 1 шт., шкаф для учебных пособий – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор ViewSonic – 1 шт.; ноутбук Acer Extensa – 1 шт.; проекционный экран Redleaf – 1 шт.

Компьютеры Intel Pentium (системный блок, монитор LG, мышь, клавиатура) – 15 шт., оснащенные программным обеспечением, указанным в разделе 10.

11.3. Материально-техническое обеспечение для самостоятельной работы

Для организации самостоятельной работы обучающихся используется библиотечный фонд вуза, библиотека.

Помещение для самостоятельной работы – читальный зал, оснащенный компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза. В случае необходимости студенты могут заниматься самоподготовкой и в компьютерном классе №248 во внеучебное время.

11.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема и передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов

(например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

12. Фонд оценочных средств для проведения аттестации по дисциплине

Фонд оценочных средств для проведения аттестации по дисциплине представлен в Приложении к рабочей программе.

13. Особенности преподавания и освоения дисциплины

Особенность преподавания и освоения дисциплины «Безопасность систем баз данных» заключается в том, что она опирается на знания, полученные студентами при изучении ряда дисциплин базового цикла, связанных с основами информационной безопасности, безопасности ОС, языками программирования и информатикой. Ряд ключевых понятий уже знаком студентам по предыдущим курсам.

Лекционный курс по дисциплине построен с целью формирования у студентов ориентировочной основы для последующего усвоения материала методом самостоятельной работы с привлечением учебно-методической литературы и электронных источников, а также стандартов и руководящих документов, регламентирующих процессы обеспечения информационной безопасности.

Содержание дисциплины отвечает следующим дидактическим требованиям:

– изложение материала - от простого к сложному, от известного к неизвестному;

– логичность, четкость и ясность в изложении материала;

– возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности студента;

– тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью студентов.

Лабораторные занятия курса проводятся по ключевым и наиболее важным разделам и темам учебной программы. Они построены как на содержании одной, так и нескольких лекций, а также требуют выполнения практических заданий на компьютере.

При подготовке к лабораторным занятиям предусмотрено при необходимости проведение консультаций для студентов. Для подготовки к занятию студентам даются рекомендации о последовательности изучения литературы (учебники, учебные пособия, конспекты лекций, статьи, справочники, информационные сборники, нормативные документы и др.). При подготовке к занятию возможно использование набора наглядных пособий и специального оборудования.

Используемые критерии оценки ответов:

- полнота и конкретность ответа;
- последовательность и логика изложения;
- связь теоретических положений с практикой;
- обоснованность и доказательность излагаемых положений;
- наличие качественных и количественных показателей;
- наличие программного кода на языке SQL;
- уровень культуры речи, владение профессиональной терминологией;
- использование наглядных пособий и т.д.

В конце занятия дается его оценка, где обращается особое внимание на следующие аспекты:

- качество подготовки;
- результаты выполненной работы и отчетных материалов;
- степень усвоения знаний;
- активность;
- положительные стороны в работе студентов;
- ценные и конструктивные предложения;
- недостатки в работе студентов и пути их устранения.

Руководство работой студентов со стороны преподавателя осуществляется в следующих формах:

- требование вести конспекты, обучение конспектированию;
- контроль выполнения: просмотр конспектов – по ходу лекции, после лекции, на лабораторных занятиях;
- использование приемов управления вниманием: контрольные вопросы, риторические вопросы, варьирование интонацией, другие ораторские приемы;
- использование приемов закрепления: повторение основных положений и выводов с использованием различных формулировок, вопросы к аудитории на проверку внимания;
- проведение тестовых самостоятельных работ по вопросам предыдущих лекций, относительно изученного раздела.

Форма проверки знаний студентов (степени овладения компетенциями) по результатам работы на практических занятиях включает контроль непосредственного участия студента в работе на лабораторном занятии (присутствие), выполнение заданий.

Общая оценка успеваемости студента складывается из посещаемости занятий, выполнения всех лабораторных заданий на компьютере, оформлении и защите отчетов по итогам работы, подготовки самостоятельных заданий, ответов студентов на контрольные вопросы..

Программой курса предусмотрено выполнение курсовой работы по проектированию защищенной базы данных.

При полном выполнении всех требований это дает право на допуск студента к экзамену.

14. Методические указания по освоению дисциплины

Лекция является основной формой обучения в высшем учебном заведении. Записи лекций в конспектах должны быть избирательными, полностью следует записывать только определения. В конспекте рекомендуется при менять сокращение слов, что ускоряет запись. Вопросы, возникающие в ходе лекции, рекомендуется записывать на полях и после окончания лекции обратиться за разъяснением к преподавателю.

Необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях. Конспекты лекций следует использовать при подготовке к практическим занятиям, при подготовке к зачету, при выполнении самостоятельных заданий и домашних работ.

Самостоятельная работа студентов в рамках изучения дисциплины «Безопасность систем баз данных» регламентируется общим графиком учебной работы, предусматривающим посещение лабораторных занятий и выполнение предусмотренных заданий.

Формы самостоятельной работы студентов:

- конспектирование;
- подготовка докладов, сообщений рефератов, презентаций;

- выполнение заданий поисково-исследовательского характера;
- углубленный анализ научно-методической литературы;
- работа с лекционным материалом: проработка конспекта лекций, работа на полях конспекта с терминами, дополнение конспекта материалами из рекомендованной литературы;
- оформление отчетов по итогам выполнения лабораторных заданий на компьютере в той или иной программной среде;
- освоение работы в той или иной программной среде с использование справочных систем.

Виды самостоятельной работы:

- познавательная деятельность во время основных аудиторных занятий;
- внеаудиторная самостоятельная работа студентов по выполнению домашних заданий учебного и творческого характера (в том числе с электронными ресурсами);
- самостоятельное овладение студентами конкретных учебных тем и вопросов, предложенных для самостоятельного изучения;
- самостоятельная работа студентов по поиску материала, который может быть использован для написания контрольных, конспектов, рефератов, курсовой работы;
- учебно-исследовательская работа;
- научно-исследовательская работа.

При организации самостоятельной работы по дисциплине «Безопасность систем баз данных» студенту следует:

1. Внимательно изучить материалы, характеризующие курс и тематику самостоятельного изучения, что изложено в учебно-методическом комплексе по дисциплине. Это позволит четко представить как круг изучаемых тем, так и глубину их постижения.

2. Составить подборку литературы, достаточную для изучения предлагаемых тем. В программе дисциплины представлены списки основной и дополнительной литературы. Они носят рекомендательный характер, это означает, что всегда есть литература, которая может не входить в данный список, но является необходимой для освоения темы. При этом следует иметь в виду, что нужна литература различных видов: учебники, учебные и учебно-методические пособия; первоисточники, монографии, сборники научных статей, публикации в журналах, любой эмпирический материал; справочная литература – энциклопедии, словари, тематические, терминологические справочники, раскрывающие категориально-понятийный аппарат. Для более глубокого изучения нормативной документации, регламентирующей вопросы обеспечения безопасности систем баз данных, следует пользоваться справочными информационными системами «Косультант Плюс» или «Гарант».

3. Основное содержание той или иной проблемы следует уяснить, изучая учебную литературу.

4. Абсолютное большинство проблем носит не только теоретический, умозрительный характер, но и тесно связано с практикой. Это предполагает наличие у студентов не только знания категорий и понятий, но и умения использовать их в качестве инструмента для анализа проблем профессиональной деятельности. Иными словами, студент должен совершать собственные, интеллектуальные усилия, а не только механически заучивать понятия и положения.

5. Соотнесение изученных закономерностей с практической работой, умение достигать аналитического знания предполагает у студента мировоззренческой культуры. Формулирование выводов осуществляется, прежде всего, в процессе дискуссии, протекающей с соблюдением методологических требований к научному познанию.

Рабочая программа дисциплины «Безопасность систем баз данных» представляет собой компонент образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных систем» и соответствует учебному плану, утвержденному 31 января 2018 и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор программы к.п.н., доцент кафедры «Информационная безопасность»
_____ Чикунова Н.Ф.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры «Информационная безопасность»
(протокол № 9 от 14.06 2018 г.)

Заведующий кафедрой _____ /Н.Я. Великите/

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии Совета РТФ

(протокол № 6 от 27.06 2018 г.)

Председатель методической комиссии _____ /А.Г. Жестовский