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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____А. В. Замятин
« 16 » ____июня_____ 2023 г.

Рабочая программа дисциплины

Основы построения защищённых баз данных

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

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

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2023

Код дисциплины в учебном плане: Б1.О.06.06

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

– ОПК-14 – Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации.

– ОПК-16 – Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

– ПК-3 – Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.

ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных.

ИОПК-14.3 Оценивает состояние и эффективность системы безопасности на уровне базы данных, разворачивает и настраивает средства защиты базы данных от несанкционированного доступа.

ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик.

ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик.

ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты информации в компьютерных системах и сетях.

ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием.

2. Задачи освоения дисциплины

– Приобретение системного подхода к проблеме аппарата защиты информации в СУБД.

– Освоение понятийного аппарата защиты информации в СУБД для решения практических задач профессиональной деятельности.

– Изучение моделей и механизмов защиты информации в СУБД.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль "Специализация".

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Восьмой семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам:

- Введение в компьютерную безопасность»
- «Основы информационной безопасности»
- «Системы управления базами данных»

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
- лекции: 20 ч.
- лабораторные: 12 ч.
  в том числе практическая подготовка: 12 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Теоретические основы безопасности в БД

Рассматриваются вопросы:
- классификации угроз информационной безопасности баз данных;
- номенклатуры возможных средств защиты.

Тема 2. Управление доступом к данным

Рассматриваются вопросы:
- управления доступом;
- техники и технологии управления доступом;
- номенклатуры средств идентификации и аутентификации.

Тема 3. Обеспечение целостности данных

Рассматриваются вопросы:
- модель транзакции и управление транзакциями;
- уровни изолированности пользователей, сериализация транзакций;
- ссылочная целостность;
- хранимые процедуры;
- триггеры.

Тема 4. Защита данных в распределенных системах

Рассматриваются вопросы:
- модель «клиент–сервер» в системах баз данных;
- распределенные базы данных;
- резервное копирование и восстановление БД.

Тема 5. Нереляционные базы данных

Рассматриваются вопросы:
- навигационные и объектно-ориентированные базы данных;
- объектно-реляционные СУБД.

Темы лабораторных работ:
- Установка, создание БД в среде MySQL.
- Средства идентификации и аутентификации.
- Ссылочная целостность.
- Хранимые процедуры.
- Триггеры.

- Резервное копирование и восстановление БД.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, тестов по лекционному материалу и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных лабораторных работ.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет по дисциплине проводится в виде ответов на вопросы билета (2 вопроса из разных разделов дисциплины). Перечень вопросов приведен в Приложении 1.

Разделы, выносимые на зачет:

Раздел «Клиент-серверная архитектура»

Раздел «Общие положения обеспечения информационной безопасности»

Раздел «Условия ограничения целостности»

Раздел «Задачи обеспечения безопасности АИС»

Раздел «Модели доступа»

Раздел «Процесс администрирования баз данных»

Раздел «Управление транзакциями»

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=10178

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Баранова Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. М.: РИОР: ИНФРА-М 2022 г., 336с.

– Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие /М.: ИНФРА-М, 2022 г., 201с.

б) дополнительная литература:

– Кузнецов С. Д. Базы данных: учебник для вузов по направлению подготовки "Прикладная математика и информатика" Академия, Серия: Университетский учебник 2012 г., 490с.

– Жарова А. К., Петровская О. В. Обеспечение целостности, доступности и достоверности данных в информационной безопасности: Информационное право. Республиканский научно-исследовательский институт интеллектуальной собственности 2021, 39-44с.

в) ресурсы сети Интернет:

– Основные методы защиты данных: [Электронный ресурс] // Управление пользователями ИНТУИТ. URL: https://www.intuit.ru/studies/courses/5/5/lecture/154

– Лихоносов А.Г. Интернет-курс по курсу «Безопасность баз данных»: [Электронный ресурс] // Московский финансово-промышленный университет «Синергия». URL: http://www.e-biblio.ru/book/bib/01_informatika/b_baz_dan/sg.html

– Общероссийская Сеть КонсультантПлюс Справочная правовая система. http://www.consultant.ru

13. Перечень информационных технологий

а) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/

– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Головчинер Михаил Наумович, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности.