МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ Н.А. Андреева
«29» 04 2024 г.

Безопасность систем баз данных Б1.О.36.04

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/7 сем
Контактная работа, в том числе (по семестрам, курсам):		68/7 сем
Лекции		34/7 сем
Лабораторных работ		18/7 сем
Практических занятий		16/7 сем
Семинаров		
Самостоятельная работа		40/7 сем
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		1/7 сем
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:
Доцент кафедры ИВТ, к.т.н., доцент Чикалов А.Н.

Рецензенты:
Ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи»,
д.т.н., доцент Погорелов В.А.

Рабочая программа дисциплины
«Безопасность систем баз данных»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины **"Безопасность систем баз данных"** является изучение особенностей защищенного хранения больших массивов структурированной информации в автоматизированных системах, современных концепций безопасности баз данных, критериев и методов оценивания надежности механизмов защиты систем баз данных, особенностей организации средств защиты в распределенных системах управления базами данных.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационной деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-1.3: способен администрировать средства защиты информации в компьютерных системах и сетях
Знать:
- принципы администрирования средств защиты информации при работе с базами данных в соответствии с требованиями по защите информации
Уметь:
- использовать средства администрирования различных баз данных, web-ресурсов и проводить оценку угроз их информационной безопасности
Владеть:
- навыками администрирования различных систем управления базами данных в соответствии с требованиями по защите информации, создания защищенных баз данных для получения, обработки, хранения и использования информации веб-ресурсов.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.В.06 Базы данных
2	Б1.О.30 Программно-аппаратные средства защиты информации
3	Б1.О.29 Методы и средства криптографической защиты информации
4	Б1.О.27 Основы информационной безопасности
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях
2	Б1.О.33 Комплексное обеспечение защиты информации объекта информатизации
3	Б1.В.01 Обеспечение безопасности персональных данных в информационных системах

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 68 аудиторных часов, 40 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1. Основы построения защищенных информационных систем					
1.1	Лекция 1. ***Принципы построения защищенных информационных систем***. Задачи обеспечения безопасности. Критерии качества безопасности. Сущность безопасности данных. Архитектура СУБД. Структура безопасности	Л1	2	ОПК-1.3	Л1.1 Л1.2 Л1.3
1.2	Базы данных и их место в архитектуре автоматизированных систем. Структура процесса проектирования систем БД и критерии качества	Ср	3	ОПК-1.3	Л1.1 Л1.2 Л1.3
1.3	Лекция 2***. Угрозы информационной безопасности БД***. Источники угроз безопасности. Классификация угроз безопасности БД и СУБД. Модели безопасности	Л2	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
1.4	Требования к системе обеспечения безопасности баз данных. Задачи и средства администратора безопасности баз данных	Ср	7	ОПК-1.3	Л1.1 Л1.2 Л1.3
1.5	Лекция 3. ***Политика безопасности БД***. Цель формализации политики безопасности. Принципы построения защищенных систем БД. Стратегия применения средств обеспечения безопасности	Л3	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
1.6	Практическое занятие 1. Обоснование политики безопасности БД	Пр1	4	ОПК-1.3	Л3.2
1.7	Лекция 4. ***Управление доступом к БД***. Защита от несанкционированных действий. Способы разграничения доступа. Защита от вывода. Ролевое и мандатное управление доступом. Авторизация доступом	Л4	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
1.8	Управление доступом к базам данных SQL Server. Роли БД по умолчанию. Управление ролями. Роли приложений. Разрешения на доступ к таблице и столбцам	Ср	10	ОПК-1.3	Л1.1 Л1.2 Л1.3
1.9	Лабораторная работа 1. ***Исследование процедур управления доступом пользователей к БД***	Лр1	6	ОПК-1.3	Л3.1
1.10	Лабораторная работа 2. ***Исследование процедур управления доступом к БД приложений пользователя***	Лр2	6	ОПК-1.3	Л3.1
Модуль 2. Механизмы реализации защитных мероприятий для БД					
2.1	Лекция 5. ***Обеспечение целостности БД***. Причины угроз целостности. Уровни целостности БД. Триггеры. Управление транзакциями. Откат транзакций. Параллельное выполнение транзакций. Сериализация. Языковые средства ограничения целостности	Л5	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
	Принципы обеспечения целостности данных. Модель Кларка-Вильсона. Модель Биба. Совместное использование моделей безопасности. Операторы языка SQL задания ограничений целостности	Ср	6	ОПК-1.3	Л1.1 Л1.2 Л1.3

	Практическое занятие 2. Разработка БД с использованием механизмов защиты целостности	Пр2	6	ОПК-1.3	Л3.2
	Лабораторная работа 3. Исследование механизмов управления транзакциями	Лр3	4	ОПК-1.3	Л3.1
	Лекция 6. ***Аудит событий БД***. Задачи аудита. Состав контролируемых процедур и механизмов управления. Организация аудита событий в системах БД	Л6	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
	Лекция 7. ***Механизмы поддержания высокой готовности БД***. Средства поддержания готовности БД. Файл журнала. Задачи и средства администрирования	Л7	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
	Лекция 8. ***Средства восстановления БД***. Причины потери данных. Принципы восстановления данных. Средства восстановления БД. Журнализация. Механизмы резервного копирования.. Модели восстановления	Л8	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
	Организация восстановления данных в СУБД MS SQL Server. Создание отказоустойчивых систем. RAID массивы. Уровни массивов. Варианты резервного копирования. Языковые инструкции копирования и восстановления данных	Ср	6	ОПК-1.3	Л1.1 Л1.2 Л1.3
	Лабораторная работа 4. Исследование механизмов создания резервных копий БД	Лр4	2	ОПК-1.3	Л3.1
	Практическое занятие 3. Восстановление утраченных данных БД	Пр3	6	ОПК-1.3	Л3.2
	Лекция 9. ***Перемещение и тиражирование БД***. Необходимость размещения данных в нескольких местах. Факторы, влияющие на использование методов переноса данных. Инструменты переноса данных.	Л9	4	ОПК-1.3	Л1.1 Л1.2 Л1.3
	Архитектура системы безопасности SQL Server. Система безопасности уровня сервера. Аутентификация ОС. Аутентификация сервера. Система безопасности уровня БД	Ср	8	ОПК-1.3	Л1.1 Л1.2 Л1.3
	Практическое занятие 4. Оперативное администрирование БД	Пр4	4	ОПК-1.3	Л3.2
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Белов Е. Б. Лось, В.П. Мещеряков Р.В. Шелупанов А. А	Основы информационной безопасности	М.: Гор. линия-Телеком, 2011. - 558 с.: ил.; 60х88 1/16. - (Специальность; Учебное пособие для высших учебных заведений	Э1
Л1.2	Баранчиков А.И.,	Алгоритмы и модели ограничения до-	М.: Гор. линия-	Э2

	Баранчиков П.А., Пылькин А.Н.	ступа к записям баз данных	Телеком, 2016. - 182 с.:	
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э3

5.1.2. Дополнительная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Лихоносов А.Г.	Интернет-курс по дисциплине "Безопасность баз данных"	МФПУ "Синергия", 2011. -http://www.ebiblio.ru/book/bib/01_informatika/b_baz_dan/sg.html#_Toc327430723	Э4
Л2.2	Полищук Ю.В., Боровский А.С.	Базы данных и их безопасность: учебное пособие	Москва: ИНФРА-М, 2022. — 210 с.	Э5
Л2.3	Скрыпников А. В., Родин С. В. Перминов Г. В. Чернышова Е. В.	Безопасность систем баз данных : учеб. пособие	Воронеж : ВГУ-ИТ, 2015. - 139 с. - ISBN 978-5-00032-122-5.	Э6
	Смирнов С.Н.	Безопасность систем баз данных	М.:Гелиос АРВ, 2007г.-352с.	Э7

5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1		Безопасность систем баз данных. Методические указания к лабораторным работам	Ростов-на-Дону: МТУСИ.	Э8
Л3.2		Безопасность систем баз данных. Методические указания к практическим занятиям	Ростов-на-Дону, СКФ МТУСИ	Э9

5.2. Электронные образовательные ресурсы

Э1	https://www.techbook.ru/book.php?id_book=63
Э2	https://www.techbook.ru/book.php?id_book=56
Э3	https://www.iprbookshop.ru/87995.html
Э4	http://www.e-biblio.ru/book/bib/01_informatika/b_baz_dan/sg.html
Э5	https://znanium.com/catalog/document?id=379704
Э6	https://www.iprbookshop.ru/50628
Э7	https://oracle-patches.com/libr/book/db/безопасность-систем-баз-данных или http://it-ebooks.ru/publ/it_secutity/security_system_of_databases/15-1-0-754
Э8	http://www.skf-mtusi.ru/?page_id=659
Э9	http://www.skf-mtusi.ru/?page_id=659

5.3. Программное обеспечение

П.1	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Kaspersky Endpoint Security (лицензия)

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интер-

	нет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное по-

собие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

Использование Интернет-ресурсов

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

Рекомендации по подготовке к рубежным аттестациям

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к зачету осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к зачету необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые

должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к зачету, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе