МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Безопасность систем баз данных

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 50,35
самостоятельная работа 30,65
часов на контроль 27

Виды контроля в семестрах:
экзамены 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	50,35	50,35	50,35	50,35
Контактная работа	50,35	50,35	50,35	50,35
Сам. работа	30,65	30,65	30,65	30,65
Часы на контроль	27	27	27	27
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является подготовка специалистов в области разработки и эксплуатации систем баз данных с учетом требований по обеспечению информационной безопасности. В задачи дисциплины входит формирование необходимого минимума специальных теоретических знаний и практических навыков по следующим аспектам:
1.2	- проектирование баз данных; - разработка прикладных программ для систем баз данных;
1.3	- эксплуатация систем баз данных; - обеспечение информационной безопасности систем баз данных.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Измерительная аппаратура контроля защищенности объектов информатизации
2.2.2	Управление информационной безопасностью

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-12: Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	
Знать:	
Уровень 1	методы проектирования вычислительных сетей;
Уровень 2	устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows;
Уровень 3	назначение, функции и структуру систем управления базами данных;
Уметь:	
Уровень 1	-проектировать вычислительные сети; -использовать средства управления работой операционной системы; -формулировать политику безопасности операционных систем семейств UNIX и Windows;
Уровень 2	-эксплуатировать базы данных; -создавать объекты базы данных;
Уровень 3	-выполнять запросы к базе данных; -разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;
Владеть:	
Уровень 1	навыками эксплуатации локальных вычислительных сетей;
Уровень 2	навыками установки операционных систем семейств Windows и Unix;
Уровень 3	навыком эксплуатации баз данных с учетом требований по обеспечению информационной безопасности;

ОПК-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	
Знать:	
Уровень 1	-методы администрирования вычислительных сетей; -методы администрирования и принципы работы операционных систем семейств UNIX и Windows; -принципы формирования политики информационной безопасности в автоматизированных системах; -методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы;
Уровень 2	-средства обеспечения безопасности данных; -основные угрозы безопасности информации и модели нарушителя объекта информатизации; -цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью; -принципы формирования политики информационной безопасности объекта информатизации;
Уровень 3	-методы и средства контроля защищенности объектов информатизации; -узлы автоматизированной системы для измерения параметров информативных сигналов технических средств обработки информации; -измерительную аппаратуру, применяемую для контроля защищенности объектов информатизации;
Уметь:	
Уровень 1	-администрировать вычислительные сети; -реализовывать политику безопасности вычислительной сети; -настраивать политику безопасности операционных систем семейств UNIX и Windows;

	-разрабатывать частные политики информационной безопасности автоматизированных систем;
Уровень 2	-осуществлять диагностику и мониторинг систем защиты автоматизированных систем; -администрировать базы данных; -разрабатывать модели угроз и модели нарушителя объекта информатизации;
Уровень 3	-оценивать информационные риски объекта информатизации; -разрабатывать порядок проведения измерений параметров информативных сигналов технических средств обработки информации; -обрабатывать и интерпретировать результаты измерений параметров информативных сигналов технических средств обработки информации;
Владеть:	
Уровень 1	-навыками администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности; -навыками администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; -навыками управления процессами обеспечения безопасности автоматизированных систем;
Уровень 2	-навыками администрирования баз данных с учетом требований по обеспечению информационной безопасности; -навыками эксплуатации измерительной аппаратуры контроля защищенности объектов информатизации с учетом требований по обеспечению информационной безопасности;
Уровень 3	-навыками применения методов математической обработки результатов измерений параметров информативных сигналов технических средств обработки информации; -навыками экспертизы состояния защищенности информации на объектах информатизации.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	методы администрирования и принципы работы операционных систем семейств UNIX и Windows, устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows;
3.1.2	методы проектирования вычислительных сетей, методы администрирования вычислительных сетей;
3.1.3	принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки;
3.2	**Уметь:**
3.2.1	настраивать политику безопасности операционных систем семейств UNIX и Windows, использовать средства управления работой операционной системы; формулировать политику безопасности операционных систем семейств UNIX и Windows;
3.2.2	проектировать вычислительные сети, администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети;
3.2.3	разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных систем;
3.3	**Владеть:**
3.3.1	администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности, установки операционных систем семейств Windows и Unix;
3.3.2	эксплуатации локальных вычислительных сетей, администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности;
3.3.3	управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Основы систем баз данных						
1.1	История развития, назначение и роль систем баз данных /Лек/	7	2	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.2	Основы теории баз данных /Лек/	7	4	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.3	Реляционные базы данных /Лек/	7	4	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.4	Проектирование баз данных /Лек/	7	4	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.5	Физическая организация баз данных /Лек/	7	4	ОПК-12 ОПК-15	Л1.1 Л1.2	0	

1.6	Средства поддержания интерфейса с различными категориями пользователей /Лек/	7	4	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.7	Понятие транзакции. Основные свойства транзакций. /Лаб/	7	2	ОПК-12 ОПК-15	Л1.1 Л1.2	1	
1.8	Триггеры и правила. /Лаб/	7	2	ОПК-12 ОПК-15	Л1.1 Л1.2	1	
1.9	Операции над отношениями /Лаб/	7	2	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.10	Нормализация базы данных /Ср/	7	17	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.11	Разработка запросов /Ср/	7	6	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
1.12	Проектирование учебной базы данных /Ср/	7	7,65	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
	Раздел 2. Безопасность систем баз данных						
2.1	Концепция безопасности баз данных /Лек/	7	4	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
2.2	Средства обеспечения целостности баз данных /Лек/	7	4	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
2.3	Средства обеспечения конфиденциальности баз данных /Лек/	7	2	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
2.4	Концепция безопасности баз данных /Лаб/	7	3	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
2.5	Угрозы целостности информации. Способы противодействия. /Лаб/	7	3	ОПК-12 ОПК-15	Л1.1 Л1.2	1	
2.6	Средства управления доступом. Виды привилегий /Лаб/	7	2	ОПК-12 ОПК-15	Л1.1 Л1.2	1	
2.7	Аудит связанных с безопасностью событий /Лаб/	7	2	ОПК-12 ОПК-15	Л1.1 Л1.2	0	
2.8	Экзамен /ИВКР/	7	2,35	ОПК-12 ОПК-15	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: История развития, назначение и роль систем баз данных
1. Какова история возникновения и развития систем баз данных?
2. Что такое система управления базами данных (СУБД) и каково её назначение?
3. Какие основные задачи решают системы баз данных?
4. В чём отличие между файловой системой хранения данных и СУБД?
5. Какую роль играют базы данных в современных информационных системах?
Тема 2: Основы теории баз данных
6. Какие модели данных используются в СУБД?
7. Что такое схема и экземпляр базы данных?
8. Чем отличаются логическая и физическая модель данных?
9. Что такое нормализация баз данных и зачем она нужна?
10. Какие понятия используются в теории реляционных БД?
Тема 3: Реляционные базы данных
11. Как устроена реляционная модель данных?
12. Что такое отношение, кортеж, домен в контексте реляционных БД?
13. Какие операции алгебры реляций вы знаете?
14. Что такое SQL и какие его функции?
15. Какие ключевые особенности реляционных СУБД?
Тема 4: Проектирование баз данных
16. Какие этапы включает процесс проектирования БД?
17. Что такое диаграмма "сущность-связь" и как она используется?
18. Как осуществляется переход от ER-модели к реляционной схеме?
19. Какие принципы учитываются при проектировании таблиц?
20. Как обеспечивается связность и согласованность данных?
Тема 5: Физическая организация баз данных
21. Как данные хранятся на уровне физического представления?
22. Что такое индексирование и как оно влияет на производительность?

23. Как организуются файлы данных в СУБД?
24. Какие типы структур данных используются для хранения?
25. Как происходит управление диском и буферизация в СУБД?
Тема 6: Средства поддержания интерфейса с различными категориями пользователей
26. Какие категории пользователей взаимодействуют с БД?
27. Какие средства предоставляет СУБД для работы пользователей разного уровня?
28. Что такое клиент-серверная архитектура БД?
29. Как обеспечиваются удобство и доступность работы с данными?
30. Какие средства визуализации и анализа данных поддерживаются в СУБД?
Тема 7: Концепция безопасности баз данных
31. Что понимается под безопасностью баз данных?
32. Какие виды угроз существуют в контексте БД?
33. Какие цели и задачи обеспечения безопасности БД?
34. Какие компоненты входят в систему защиты БД?
35. Как законодательство регулирует вопросы безопасности баз данных?
Тема 8: Средства обеспечения целостности баз данных
36. Что такое целостность данных и почему она важна?
37. Какие типы ограничений целостности реализуются в СУБД?
38. Что такое первичный и внешний ключи?
39. Как работает механизм триггеров для обеспечения целостности?
40. Как транзакции влияют на сохранение консистентности данных?
Тема 9: Средства обеспечения конфиденциальности баз данных
41. Что такое конфиденциальность данных в БД?
42. Какие меры применяются для защиты конфиденциальной информации?
43. Как реализуется разграничение доступа к данным?
44. Какие методы шифрования применяются в СУБД?
45. Как осуществляется аудит действий пользователей в БД?

5.2. Темы письменных работ

Не предусмотрены

5.3. Оценочные средства

Рабочая программа "Безопасность систем баз данных" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 7 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Стружкин Н. П., Годин В. В.	Базы данных: проектирование: учебник для вузов	Москва: Юрайт, 2022
Л1.2	Илюшечкин В. М.	Основы использования и проектирования баз данных: учебник для вузов	Москва: Юрайт, 2022

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	База данных научных электронных журналов "eLibrary"
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	Лаб

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины «Безопасность систем баз данных» представлены в Приложении 2 и включают в
себя:
Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы
формирования компетенций.