МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Киберфизические системы

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 64,25
самостоятельная работа 43,75

Виды контроля в семестрах:
зачеты 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
Практические	32	32	32	32
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	64,25	64,25	64,25	64,25
Контактная работа	64,25	64,25	64,25	64,25
Сам. работа	43,75	43,75	43,75	43,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Знакомство с общей концепцией и принципами построения киберфизических систем (КФС) как новой технологической платформы формирования универсальной информационно-управляющей среды, объединяющей ключевые тренды развития сквозных информационных и информационно-прикладных технологий, и предназначенной для решения широкого класса задач промышленной автоматизации, управления и кибербезопасности

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Инженерная и компьютерная графика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Комплексное обеспечение защиты информации объектов информатизации

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	
Знать:	
Уровень 1	основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД); типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации; принципы организации информационных систем в соответствии с требованиями по защите информации; особенности комплексного подхода к обеспечению информационной безопасности организации;
Уровень 2	программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; базовые понятия и определения киберфизической системы, базовые принципы теории управления системами, формирования целей, методов и критериев качества управления, формализованных стратегий основы, понятия и определения информационно-управляющих систем;
Уровень 3	основы теории сетевой организации информационно-вычислительных распределенных систем и компьютерных сетей, архитектуры и иерархии сетевой организации; основы модели знаний, базовые понятия теории формирования баз данных и баз знаний; подходы к построению платформы киберфизической системы как гибридной сетевой среды с интегрированными вычислительными и физическими возможностями
Уметь:	
Уровень 1	применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД); проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
Уровень 2	разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности; анализировать подходы к построению гибридной информационно-управляющей среды, ориентированной на решение широкого класса прикладных задач, в том числе связанных с обеспечением информационной безопасности;
Уровень 3	ставить задачи формирования архитектуры, принципов построения и функционирования киберфизической системы; ставить задачи проведение аналитики киберугроз и оценки уязвимостей и рисков киберфизической системы
Владеть:	
Уровень 1	навыками разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД);т навыками использования современных сетевых технологий;
Уровень 2	навыками проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передачи информации;

Уровень 3	методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; навыками применения полученных знаний на практике;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации, классификацию и количественные характеристики технических каналов утечки информации;
3.1.2	способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности;
3.1.3	организацию защиты информации от утечки по техническим каналам на объектах информатизации
3.2	**Уметь:**
3.2.1	проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации, использовать средства инструментального контроля показателей эффективности технической защиты информации
3.3	**Владеть:**
3.3.1	проектирования системы защиты объекта информатизации от утечек по техническим каналам

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. Киберфизические системы: основные понятия						
1.1	Понятие киберфизической системы (КФС). Области применения киберфизических систем. Концептуальная модель КФС /Лек/	7	6	ОПК-9	Л1.1 Л1.2Л2.1	0	
1.2	Основные принципы организации и функционирования КФС. Системный подход к анализу и синтезу структур КФС /Лек/	7	6	ОПК-9	Л1.1 Л1.2Л2.1	0	
1.3	Понятие КФС. Примеры киберфизических систем и объектов. Уровни концептуальной модели КФС. Функциональные признаки модели /Пр/	7	8	ОПК-9	Л1.1 Л1.2Л2.1	1	
1.4	Подготовка к зачету /Ср/	7	16	ОПК-9	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Теория автоматического управления и информационно- управляющие системы						
2.1	Базовые понятия теории автоматического управления (ТАУ). Формализация постановки задачи и выбора стратегий управления /Лек/	7	6	ОПК-9	Л1.1 Л1.2Л2.1	0	
2.2	Информационно-управляющие системы: понятия, определения, особенности /Лек/	7	6	ОПК-9	Л1.1 Л1.2Л2.1	0	
2.3	Информационно-вычислительные распределенные системы: принципы сетевой организации, архитектура и иерархия /Лек/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	0	
2.4	Инженерия знаний: модели знаний, базовые понятия теории формирования баз данных и баз знаний /Лек/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	0	
2.5	Базовые понятия ТАУ: объект управления, алгоритмы и критерии качества управления /Пр/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	0	
2.6	Постановка задачи и выбора стратегий управления. Целевые функции при синтезе КФС /Пр/	7	6	ОПК-9	Л1.1 Л1.2Л2.1	0	

2.7	Примеры информационно-управляющих систем. Анализ особенностей /Пр/	7	6	ОПК-9	Л1.1 Л1.2Л2.1	1	
2.8	Архитектура и иерархия сетевой организации вычислительной распределенной системы /Пр/	7	4	ОПК-9	Л1.1 Л1.2Л2.1	0	
2.9	Модели знаний /Пр/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	1	
2.10	Подготовка к контрольным работам /Ср/	7	11,75	ОПК-9	Л1.1 Л1.2Л2.1	0	
	Раздел 3. Индустриальные киберфизические системы. Кибербезопасность						
3.1	Индустриальные КФС (ИКФС), сферы применения ИКФС. подходы к разработке и анализу, оперативное планирование и управление /Лек/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	0	
3.2	Кибербезопасность КФС /Лек/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	0	
3.3	Интеллектуальные фабрики. Промышленные интеллектуальные данные и сервисы /Пр/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	1	
3.4	Подходы к разработке и анализу интеллектуальных производственных систем с позиций кибербезопасности /Пр/	7	2	ОПК-9	Л1.1 Л1.2Л2.1	0	
3.5	Подготовка к практическим занятиям /Ср/	7	16	ОПК-9	Л1.1 Л1.2Л2.1	0	
3.6	Зачет /ИВКР/	7	0,25	ОПК-9	Л1.1 Л1.2Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Понятие киберфизической системы. Области применения
1. Что такое киберфизическая система (КФС)?
2. Какие основные компоненты входят в состав КФС?
3. В каких отраслях находят применение КФС?
4. Какова роль КФС в концепции Индустрии 4.0?
5. Приведите примеры использования КФС в реальной жизни.

Тема 2: Концептуальная модель и принципы организации КФС
6. Как устроена концептуальная модель киберфизической системы?
7. Чем отличается централизованная и децентрализованная архитектура КФС?
8. Какие уровни взаимодействия выделяются в структуре КФС?
9. Как осуществляется обмен данными между физическими и кибернетическими компонентами?
10. Какие технологии лежат в основе реализации КФС?

Тема 3: Системный подход к анализу и синтезу КФС
11. Что понимается под системным подходом при проектировании КФС?
12. Какие этапы включает жизненный цикл разработки КФС?
13. Как строится модель поведения киберфизической системы?
14. Как учитываются требования надёжности и отказоустойчивости при синтезе КФС?
15. Какие методики используются для верификации проектных решений?

Тема 4: Основы теории автоматического управления
16. Какие базовые понятия используются в теории автоматического управления?
17. Что такое обратная связь и как она используется в КФС?
18. Какие типы регуляторов применяются в автоматизированных системах?
19. Как формулируется задача управления в контексте КФС?
20. Как выбирается стратегия управления для конкретного процесса?

Тема 5: Информационно-управляющие системы
21. Что такое информационно-управляющая система?
22. Какие функции выполняет ИУС в составе КФС?
23. Как организуется сбор, обработка и передача данных в ИУС?
24. Как обеспечивается синхронизация действий в распределённой ИУС?
25. Какие протоколы и интерфейсы используются в информационно-управляющих системах?

Тема 6: Информационно-вычислительные распределённые системы
26. Что такое распределённая информационно-вычислительная система?
27. Какова сетевая организация таких систем?
28. Какие топологии наиболее часто используются в КФС?
29. Как строится иерархия управления в распределённой системе?
30. Какие проблемы возникают при масштабировании распределённых КФС?
Тема 7: Инженерия знаний в КФС
31. Что такое инженерия знаний и зачем она нужна в КФС?
32. Какие виды моделей знаний используются в системах управления?
33. Чем отличаются базы данных от баз знаний?
34. Как организуется представление знаний в системах принятия решений?
35. Как интегрируются системы искусственного интеллекта в КФС?
Тема 8: Индустриальные киберфизические системы (ИКФС)
36. Что такое индустриальная киберфизическая система (ИКФС)?
37. Где применяются ИКФС в промышленности?
38. Какие особенности проектирования имеют ИКФС?
39. Как организуется оперативное планирование и управление в ИКФС?
40. Какие стандарты используются при внедрении ИКФС на производстве?
Тема 9: Кибербезопасность киберфизических систем
41. Какие уникальные угрозы существуют для КФС?
42. Почему классические средства защиты не всегда эффективны в КФС?
43. Как обеспечить защиту от атак на физическую часть системы?
44. Какие меры безопасности необходимы для сетевых компонентов КФС?
45. Как строится многоуровневая защита критически важных КФС?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Киберфизические системы" 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	Лаврищева Е. М.	Программная инженерия и технологии программирования сложных систем: учебник для вузов	Москва: Юрайт, 2023
Л1.2	Гаврилова Т. А., Кудрявцев Д. В., Муромцев Д. И.	Инженерия знаний. Модели и методы: учебник для вузов	Санкт-Петербург: Лань, 2023

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Ватаманюк И. В., Левоневский Д. К., Малов Д. А., Яковлев Р. Н., Савельев А. И.	Модели и способы взаимодействия пользователя с киберфизическим интеллектуальным пространством: монография	Санкт-Петербург: Лань, 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	

		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 "Киберфизические системы" представлены в Приложении 2 и включают в себя:

1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.