МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Производственная практика (научно-исследовательская работа)

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 **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 4,25
самостоятельная работа 211,75

Виды контроля в семестрах:
зачеты 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	14 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	4	4	4	4
Иные виды контактной работы	0,25	0,25	0,25	0,25
Итого ауд.	4,25	4,25	4,25	4,25
Контактная работа	4,25	4,25	4,25	4,25
Сам. работа	211,75	211,75	211,75	211,75
Итого	216	216	216	216

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	-освоение студентами методов теоретических и прикладных исследований проблем
1.2	обеспечения информационной безопасности автоматизированных систем для
1.3	повышения научно-практического потенциала будущих специалистов по защите
1.4	информации;
1.5	- приобретение студентами умений и навыков самостоятельной практической работы
1.6	в области информационной безопасности и защиты информации;
1.7	- получение студентами практических навыков выполнения мероприятий по
1.8	организационной, правовой и технической защите информации, овладение методами
1.9	работы с программами, обеспечивающими информационную безопасность.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Электромагнитные поля и волны
2.1.2	Практикум по решению научно-исследовательских задач профессиональной деятельности
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика (преддипломная)

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-1: Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	
Знать:	
Уровень 1	методы проведения физических исследований, технические и программные средства, применяемые при анализе электромагнитных полей и волн; уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов;
Уровень 2	назначение, функции и структуру информационных и библиографических систем; методы поиска, изучения и обобщения научно-технической литературы, нормативных и методических материалов; основные методы исследования по теме своей научно- исследовательской работы; основы теории цифровой обработки сигналов как теоретической базы для разработки и исследования методов обработки, приема и передачи данных в системах обеспечения информационной безопасности автоматизированных систем управления; актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности; цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;
Уровень 3	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления; области задач организации информационных технологий и современные инструменты построения интеллектуальных систем, обеспечивающих информационную безопасность; основные принципы и проблематику теории обучения машин, основные современные методы обучении по прецедентам — классификации, кластеризации и регрессии; принципы организации информационных систем в соответствии с требованиями по защите информации; основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана); уязвимости современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП; основные виды математических моделей информационных потоков и систем защиты информации и методы их построения;
Уметь:	
Уровень 1	использовать методы проведения физических исследований, технические и программные средства для анализа электромагнитных полей технических средств автоматизированных систем; использовать методы исследования электромагнитных полей для оценки физических характеристик

	технических средств автоматизированных систем; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; определять параметры информационной системы и ее структуру в соответствии с заданными функциями;
Уровень 2	составлять обзоры по вопросам обеспечения информационной безопасности по теме своей научно-исследовательской работы; применять методы исследования по теме своей научно-исследовательской работы; формировать математическое описание дискретных систем в виде алгоритмов; выполнять компьютерное моделирование дискретных систем на основе их математического описания; анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации; анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации; формулировать основные задачи, возникающие при анализе данных, пути их решения, выбирать адекватные алгоритмы решения задачи анализа данных, оценивать качество получаемых решений, обеспечивающих информационную безопасность;
Уровень 3	формализовать постановки прикладных задач анализа данных, применять основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование; оценивать информационные риски в информационных системах; решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей; анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии; на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ;
Владеть:	
Уровень 1	навыком применения методик исследования электромагнитных полей; навыком применения исследовательских методов электродинамики и распространения радиоволн; навыками поиска и изучения научно-технической литературы, а также изложения и оформления результатов своей научно- исследовательской работы; навыком составления математических моделей дискретных систем и сигналов;
Уровень 2	навыком разработки алгоритмов цифровой обработки сигналов в системах информационной безопасности; навыком выбора методов проведения и обработки экспериментальных исследований, оформления научно-технических отчётов, обзоров, докладов, статей; навыком выбора и обоснованием критериев эффективности функционирования защищенных информационных систем;
Уровень 3	навыком применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ; навыком разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети; навыком применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей;
3.1.2	методы проведения физических исследований, технические и программные средства, применяемые при анализе электромагнитных полей и волн;
3.1.3	принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов;
3.2	**Уметь:**
3.2.1	использовать методы исследования электромагнитных полей для оценки физических характеристик технических средств автоматизированных систем;
3.2.2	использовать методы проведения физических исследований, технические и программные средства для анализа электромагнитных полей технических средств автоматизированных систем;
3.2.3	определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе;
3.3	**Владеть:**
3.3.1	применения исследовательских методов электродинамики и распространения радиоволн;

3.3.2	применения методик исследования электромагнитных полей;

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. Тема 1.						
1.1	ИзучениезаданияпоНИРитребованийке ёвыполнению /Лек/	8	4	ПК-1	Л2.1	0	
	Раздел 2. Тема 2.						
2.1	Реферированиенаучныхтекстов,вт.ч. на иностранных языках. /Ср/	8	60	ПК-1	Л2.1	0	
	Раздел 3. Тема 3.						
3.1	Участие в работе научно-исследовательских и проектных групп по актуальным направлениям современной теории и практики информационной безопасности /Ср/	8	70	ПК-1	Л2.1	0	
	Раздел 4. Тема 4.						
4.1	Разработка и проведение научных исследований: сбор, анализ и обобщение научной информации; участие в проведении теоретических и экспериментальных научных исследований в области информационной безопасности /Ср/	8	50	ПК-1	Л2.1	0	
	Раздел 5. Тема 5.						
5.1	Сопоставлениеианализсведенийизразл ичных источников /Ср/	8	10	ПК-1	Л2.1	0	
	Раздел 6. Тема 6.						
6.1	Обобщениеинформациисоценкойдосто верности. Работа с информационно-справочными системами /Ср/	8	6	ПК-1	Л2.1	0	
	Раздел 7. Тема 7.						
7.1	Составлениеотчетаизаполнениедневни ка практики /Ср/	8	15,75	ПК-1	Л2.1	0	
7.2	Зачет /ИВКР/	8	0,25	ПК-1	Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

1. Что входит в понятие информационной безопасности в автоматизированных системах?
2. Какие основные угрозы информационной безопасности существуют в современных ИТ-системах?
3. В чем заключается значение теоретических методов исследования в области информационной безопасности?
4. Какие прикладные исследования наиболее актуальны для обеспечения информационной безопасности?
5. Каковы принципы построения систем защиты информации в автоматизированных системах?
6. Что такое политика безопасности информации и какие бывают её типы?
7. Какие существуют подходы к классификации угроз информационной безопасности?
8. Как формируется модель угроз в информационной системе?
9. Какие этапы включает анализ рисков в ИБ?
10. В чем состоит отличие между угрозой и уязвимостью в информационных системах?
11. Что такое политика разграничения доступа и как она реализуется?
12. Какова роль криптографических методов в обеспечении информационной безопасности?
13. Какие бывают виды шифрования и как они применяются на практике?
14. В чем особенности симметричных и асимметричных алгоритмов шифрования?
15. Как осуществляется управление ключами в криптографических системах?
16. Что такое цифровая подпись и каковы ее функции?
17. Какие методы аутентификации пользователей применяются в ИБ?
18. Каковы признаки несанкционированного доступа к информации?
19. В чем разница между идентификацией и аутентификацией?
20. Что такое контроль целостности данных и какие методы применяются для этого?

21. Какие программные средства предназначены для защиты информации на ПК?
22. Какую роль играют антивирусные программы в информационной безопасности?
23. Что такое межсетевой экран и как он обеспечивает защиту информации?
24. Как работает система обнаружения вторжений (IDS)?
25. В чем отличие IDS от IPS?
26. Каковы основные принципы построения защищенных сетей?
27. Какие существуют организационные меры по защите информации?
28. Какие существуют правовые нормы в области защиты информации?
29. Каков порядок классификации информации по уровню конфиденциальности?
30. Какие меры принимаются при утечке информации?
31. В чем заключается отличие нормативного и технического обеспечения информационной безопасности?
32. Какие требования предъявляются к персоналу в сфере ИБ?
33. Как организуются мероприятия по защите информации на предприятии?
34. Какова роль инструкций и регламентов в обеспечении ИБ?
35. Что такое аудит информационной безопасности и как он проводится?
36. Какие документы входят в систему документации по ИБ?
37. Какие существуют международные стандарты в области ИБ (например, ISO/IEC 27001)?
38. Каковы особенности защиты информации в облачных технологиях?
39. Какие угрозы характерны для мобильных устройств?
40. Какие методы используются для защиты данных на съёмных носителях?
41. Как обеспечивается защита информации при удалённой работе?
42. Какие требования предъявляются к разработке безопасного программного обеспечения?
43. В чем суть принципа минимальных привилегий?
44. Как реализуется принцип «отказ по умолчанию» в ИБ?
45. Что такое резервное копирование и зачем оно нужно в ИБ?
46. Как организовать восстановление информации после инцидента?
47. В чем заключается принцип непрерывности бизнеса в контексте ИБ?
48. Какие инструменты применяются для мониторинга состояния безопасности системы?
49. Как осуществляется обучение сотрудников основам ИБ?
50. Почему важно регулярно обновлять программное обеспечение и антивирусные базы?

5.2. Темы письменных работ

не предусмотрено

5.3. Оценочные средства

Рабочая программа "Производственная практика (научно-исследовательская работа)" 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 8 семестре.

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

6.1. Рекомендуемая литература

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Кривошеин Д. А., Дмитренко В. П., Горькова Н. В.	Безопасность жизнедеятельности: учебное пособие для вузов	Лань, 2023

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	
3	Специализированная многофункциональная учебная аудитория № 3 для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Компьютерные столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Стеллаж для учебно-методических материалов, в том числе учебно-наглядных пособий; Многофункциональное устройство (принтер, сканер, ксерокс); Интерактивная доска; Мультимедийный проектор; Ноутбуки 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	
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 "Производственная практика (научно-исследовательская работа)" 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.