МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Производственная практика (технологическая)

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				
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	- закрепление и конкретизация результатов теоретического обучения;
1.2	- приобретение студентами умений и навыков самостоятельной практической работы в области информационной безопасности и защиты информации;
1.3	- получение студентами практических навыков выполнения мероприятий по организационной, правовой и технической защите информации, овладение методами работы с программами, обеспечивающими информационную безопасность;
1.4	- развитие у студентов навыков проведения анализа деятельности предприятий и организаций по усовершенствованию их работы с позиции защиты информации;
1.5	- всестороннее описание объекта информатизации и проведение исследований на предмет его защищенности с целью применения полученных знаний при подготовке курсовых работ по последующим дисциплинам "Техническая защита информации" и "Программно-аппаратные средства обеспечения информационной безопасности", а также с целью формирования будущей темы выпускной квалификационной работы.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Биометрические технологии контроля доступа
2.1.2	Средства и системы контроля и управления доступом
2.1.3	Практикум по решению эксплуатационных задач профессиональной деятельности
2.1.4	Производственная практика (эксплуатационная)
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информации в сети Интернет
2.2.2	Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами
2.2.3	Производственная практика (преддипломная)

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-5: Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций	
Знать:	
Уровень 1	основы правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации; основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;
Уровень 2	статус и порядок работы основных правовых информационно-справочных систем; основы организации и деятельности органов государственной власти в Российской Федерации; основные документы по стандартизации в сфере управления ИБ; принципы формирования политики информационной безопасности в автоматизированных системах;
Уровень 3	требования информационной безопасности при эксплуатации автоматизированной системы; требования нормативных документов к составу, содержанию и оформлению технической документации объекта информатизации; виды и состав документации современной организации, особенности документирования профессиональной деятельности;
Уметь:	
Уровень 1	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно- распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;

Уровень 2	формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; формировать политики информационной безопасности организации
Уровень 3	выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы; разрабатывать техническую документацию объекта информатизации; определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы;
Владеть:	
Уровень 1	понятийно-категориальным аппаратом юриспруденции; навыками установления фактических обстоятельств, юридической основы и квалификации;
Уровень 2	навыком работы с нормативными правовыми актами различной юридической силы; навыками применения основных законов, связанных с организационно-правовым обеспечением информационной безопасности в профессиональной деятельности;
Уровень 3	навыками организации и обеспечения режима секретности; методами организации и управления служб защиты информации на предприятии; методами формирования требований по защите информации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	современные методы предотвращения несанкционированного доступа (НСД) к объектам информатизации, основанные на биометрических технологиях распознавания личности;
3.1.2	методы и средства контроля и управления доступом при обеспечении безопасности автоматизированных систем
3.2	**Уметь:**
3.2.1	использовать устройства контроля доступа на основе биометрических характеристик человека;
3.2.2	использовать устройства контроля и управления доступом при обеспечении безопасности автоматизированных систем
3.3	**Владеть:**
3.3.1	использования специальных средств биометрической идентификации личности для управления процессами обеспечения безопасности автоматизированных систем;
3.3.2	использования систем контроля и управления доступом для управления процессами обеспечения безопасности 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. начало практики						
1.1	Общее знакомство с деятельностью и структурой предприятия /Лек/	8	4	ПК-5	Л2.1	0	
1.2	Изучение должностных инструкций технического персонала /Ср/	8	60,75	ПК-5	Л2.1	0	

1.3	Знакомство с информационной системой предприятия: 1. Познакомиться и записать историю развития предприятия. 2. Составить паспорт предприятия с точки зрения обеспечения информационной безопасности. 3. Познакомиться с информационной системой (ИС) предприятия с целью применения полученных знаний при подготовке курсовой работы по последующей дисциплине "Программно-аппаратные средства обеспечения информационной безопасности": • описать аппаратные средства ИС; • описать программные средства ИС; • выделить и описать элементы ИС, требующие защиты информации и элементы, предназначенные для защиты информации. /Ср/	8	60	ПК-5	Л2.1	0	
	Раздел 2. Изучение используемого современного программного обеспечения.						
2.1	Участие в практической работе по обеспечению защиты информации: Приобрести практические навыки по настройке и установке различных видов программных и аппаратных средств защиты информации с учетом политики информационной безопасности предприятия /Ср/	8	91	ПК-5	Л2.1	0	
	Раздел 3. Обработка и систематизация полученных результатов, материалов. Оформление и защита отчета о производственной практике.						
3.1	Оформление и защита отчета о производственной практике /ИВКР/	8	0,25	ПК-5	Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

1.Какие цели и задачи ставились перед вами на практике?
2 .Какие методы анализа защищенности информационных систем вы применяли?
3. Как проводилось тестирование на проникновение в ходе практики?
4. Какие инструменты для сканирования уязвимостей вы использовали?
5. Какие виды кибератак моделировались при проверке системы?
6. Как оценивалась критичность обнаруженных уязвимостей?
7. Какие системы обнаружения вторжений изучали на практике?
8. Как настраивались правила межсетевого экрана?
9. Какие решения для мониторинга безопасности вы исследовали?
10. Как организовано резервное копирование данных в организации?
11. Какие средства криптографической защиты применялись?
12. Как реализован контроль доступа к информационным ресурсам?
13. Какие методы защиты от DDoS-атак использовались?
14. Как обеспечивалась защита рабочих станций и серверов?
15. Какие средства защиты применялись для мобильных устройств?
16. Как обеспечивалась безопасность облачных сервисов?
17. Какие алгоритмы шифрования использовались в организации?
18. Как организовано управление ключами шифрования?
19. Какие методы электронной подписи применялись?
20. Как реализована инфраструктура открытых ключей (PKI)?

21. Какие политики безопасности действовали в организации?
22. Как проводился инструктаж персонала по вопросам ИБ?
23. Какие регламенты работы с конфиденциальной информацией вы изучили?
24. Как организован контроль доступа в помещения?
25. Какие меры защиты от инсайдерских угроз применялись?
26. Какие инциденты информационной безопасности были зафиксированы?
27. Какова процедура реагирования на инциденты в организации?
28. Какие протоколы журналирования событий безопасности велись?
29. Как проводилось расследование инцидентов?
30. Какие меры принимались для восстановления после инцидентов?
31. Какие требования ФЗ-187 "О безопасности КИИ" реализованы?
32. Как выполнялись требования приказов ФСТЭК/ФСБ?
33. Какие международные стандарты (ISO 27001) учитывались?
34. Как проводилась аттестация объектов информатизации?
35. Какие разделы включал ваш отчет по практике?
36. Как оформлялись схемы защищенной сети?
37. Какие модели угроз вы разрабатывали?
38. Как представлялись рекомендации по улучшению защиты?
39. Какие новые профессиональные компетенции вы приобрели?
40. Какие предложения по улучшению организации практики вы можете внести?
41. Какие методы аутентификации пользователей применялись в системе?
42. Как осуществлялся контроль целостности данных?
43. Какие меры защиты применялись для съемных носителей информации?
44. Как организована защита информации при удаленной работе?
45. Какие требования предъявлялись к разработке защищенного ПО?
46. Как реализовывался принцип минимальных привилегий?
47. Какие инструменты использовались для анализа защищенности сетевого трафика?
48. Как проводилась оценка соответствия системы требованиям ИБ?
49. Какие методы защиты от социальной инженерии применялись?
50. Как оценивалась эффективность применяемых мер защиты информации?

изводственная практика (научно-исследовательская работа)

5.2. Темы письменных работ

не предусмотрено

5.3. Оценочные средства

Рабочая программа "Производственная практика (технологическая)" 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: зачета 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 (технологическая)" 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.