МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Производственная практика (эксплуатационная)

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 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		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"
1.6	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:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Методы и средства противодействия террористической деятельности в системах управления значимых объектов КИИ
2.2.2	Практикум по решению эксплуатационных задач профессиональной деятельности
2.2.3	Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами
2.2.4	Защита информации в сети Интернет
2.2.5	Технологии защиты информации в различных отраслях деятельности
2.2.6	Производственная практика (преддипломная)
2.2.7	Производственная практика (технологическая)

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-4: Способен разрабатывать организационно-распорядительные документы и внедрять организационные меры по защите информации в автоматизированных системах	
Знать:	
Уровень 1	правовые основы организации защиты государственной тайны и/или конфиденциальной информации; задачи органов защиты государственной тайны и/или служб защиты информации на предприятии; свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления;
Уровень 2	задачи органов защиты информации на предприятиях; действующие нормативные и методические документы по оформлению рабочей технической документации; понятие и виды террористической деятельности, основы государственной политики Российской Федерации по противодействию терроризму в информационной сфере; нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры;
Уровень 3	категории и характеристики значимых объектов критической информационной инфраструктуры; способы выявления угроз информационной безопасности значимых объектов критической информационной инфраструктуры; нормативные документы Российской федерации в области кибербезопасности; особенности организации подразделения центра управления инцидентами (ЦУИ ИБ) для поддержки информационной безопасности промышленной сети; основы правового обеспечения и основные нормативные правовые акты в области защиты информации в различных отраслях деятельности; организацию работы специалистов с документами в автоматизированных системах электронного документооборота
Уметь:	
Уровень 1	анализировать правовые акты и осуществлять правовую оценку информации, циркулирующей в автоматизированной системе; квалифицированно исследовать состав документации предприятия (организации);
Уровень 2	разрабатывать проекты нормативных и организационно -распорядительных документов, регламентирующих работу по защите информации;

	реализовывать с учетом особенностей функционирования систем управления значимых объектов критической информационной инфраструктуры требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам противодействия террористической деятельности
Уровень 3	разрабатывать предложения по совершенствованию организационно- распорядительных документов по безопасности значимых объектов и представлять их руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу); применять средства юридической защиты информации ограниченного доступа; определять задачи по разработке требований к автоматизированным системам обработки и хранения электронных документов
Владеть:	
Уровень 1	навыком разработки организационно- распорядительных документов по защите информации в автоматизированных системах; навыком формирования требований по защите информации
Уровень 2	навыком применения современной нормативной базы для построения системы организационных и программно -технических мер по выявлению, предупреждению и пресечению террористической деятельности в отношении систем управления значимых объектов критической информационной инфраструктуры
Уровень 3	навыком использования профессиональной терминологии в области защиты информации в различных отраслях деятельности

ПК-5: Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций	
Знать:	
Уровень 1	методы и средства контроля и управления доступом при обеспечении безопасности автоматизированных систем; политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; современные методы предотвращения несанкционированного доступа (НСД) к объектам информатизации, основанные на биометрических технологиях распознавания личности
Уровень 2	принципы организации и структуру систем защиты программного обеспечения автоматизированных систем; средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; принципы формирования политики информационной безопасности автоматизированной системы; основные направления защиты информации в информационно- телекоммуникационных системах в соответствии с законодательством Российской Федерации
Уровень 3	современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; архитектуру автоматизированной системы управления технологическим процессом (АСУ ТП), модели промышленных систем автоматизации, сетевые технологии, используемые в современных АСУ ТП, понятия функциональной и информационной безопасности, их взаимосвязь и противоречия; основы организации своевременной и полноценной обработки инцидентов безопасности
Уметь:	
Уровень 1	использовать устройства контроля и управления доступом при обеспечении безопасности автоматизированных систем; применять политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; использовать устройства контроля доступа на основе биометрических характеристик человека
Уровень 2	регистрировать события, связанные с защитой информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; проводить оценку угроз безопасности информационно- телекоммуникационной системы, подключенной к сети Интернет;
Уровень 3	реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; работать со средствами обеспечения безопасности в системах промышленной автоматизации; настраивать межсетевой экран для обеспечения защиты периметра сети, для обеспечения сегментации внутренней сети
Владеть:	
Уровень 1	навыком использования систем контроля и управления доступом для управления процессами обеспечения безопасности автоматизированных систем; навыком применения инструментов администрирования подсистем информационной безопасности

	автоматизированной системы; навыком использования специальных средств биометрической идентификации личности для управления процессами обеспечения безопасности автоматизированных систем
Уровень 2	навыком обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы; навыком обеспечения работоспособности автоматизированных систем при возникновении нештатных ситуаций; навыком разработки частных политик информационной безопасности автоматизированных систем
Уровень 3	навыком использования антивирусного программного обеспечения для защиты информации в информационно- телекоммуникационных системах, подключенных к сети Интернет; анализом инцидентов кибербезопасности в современных промышленных системах автоматизации

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/	6	4	ПК-4 ПК-5	Л2.1	0	
1.2	Изучение должностных инструкций технического персонала /Ср/	6	20,75	ПК-4 ПК-5		0	
	Раздел 2. Знакомство с оборудованием подразделения						
2.1	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/	6	30	ПК-4 ПК-5		0	
2.2	Изучение используемого современного программного обеспечения /Ср/	6	40	ПК-4 ПК-5		0	

2.3	Знакомство с системами защиты информации: 1. Познакомиться с предоставленными документами по обеспечению защиты информации. 2. Дать описание основных средств и методов обеспечения защиты информации на предприятии (в учреждении, организации). 3. Составить заключение о степени достаточности мер по обеспечению информационной безопасности предприятия. 4. Собрать информационные материалы для всестороннего описание выбранного объекта информатизации (защищаемого помещения) и проведения исследований на предмет его защищенности с целью применения полученных знаний при подготовке курсовых работ по последующей дисциплине "Техническая защита информации": • дать общее описание предприятия и выбранного объекта информатизации (защищаемого помещения) с точки зрения назначения и выполняемых функций; • нарисовать схему контролируемой зоны предприятия и размещения объекта информатизации (защищаемого помещения); • нарисовать схему организационно-штатной структуры предприятия; • составить перечень сведений, подлежащих защите; • сформулировать цели защиты по категориям каналов утечки информации (ПЭМИН, речевая, видовая информация); • нарисовать схему защищаемого помещения; • описать параметры защищаемого помещения (стены, пол, потолок, окна, двери, предметы мебели, технические средства, инженерные и технические коммуникации); • сформулировать угрозы (воздействия и утечки) и источники угроз (внутренние, внешние, случайные) защищаемой информации. /Ср/	6	60	ПК-4 ПК-5		0	
2.4	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/	6	61	ПК-4 ПК-5		0	

	Раздел 3. Обработка и систематизация полученных результатов, материалов. Оформление и защита отчета о производственной практике.						
3.1	Отчет и защита отчета о производственной практики /ИВКР/	6	0,25	ПК-4 ПК-5		0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Какие цели ставились перед вами на практике по эксплуатации защищенных систем?
2. Какие методы мониторинга информационной безопасности вы применяли?
3. Что такое эксплуатация средств защиты информации и как она проводится?
4. Какие инструменты использовались для анализа защищенности систем?
5. В чем особенности администрирования систем информационной безопасности?
6. Какие типы защищенных систем вы обслуживали на практике?
7. Чем отличается эксплуатация межсетевых экранов от систем обнаружения вторжений?
8. Какие признаки позволяют выявить нарушения в работе средств защиты?
9. Что такое журнал событий безопасности и как он анализируется?
10. Как проводится обновление защитного программного обеспечения?
11. Какие методы реагирования на инциденты применялись на практике?
12. Что включает в себя ежедневное обслуживание систем безопасности?
13. Какие виды диагностики защитных систем вам удалось провести?
14. Каковы особенности работы с системами SIEM?
15. Какие конфигурации защитных систем вы настраивали в ходе практики?
16. Что такое политики безопасности и как они применяются в эксплуатации?
17. Какие средства мониторинга использовались во время работы?
18. Какие меры предосторожности соблюдаются при изменении настроек защиты?
19. Как оформляется отчет о работе систем безопасности?
20. Что включает в себя ежедневный отчет администратора безопасности?
21. Какие показатели учитываются при оценке работы защитных систем?
22. Что такое аудит безопасности и как он проводится?
23. Какие уязвимости вы выявляли в ходе эксплуатации систем?
24. Как составляется план технического обслуживания средств защиты?
25. Какие особенности имеет ведение документации по эксплуатации?
26. Как осуществляется резервное копирование конфигураций безопасности?
27. Какие программные средства вы использовали для управления защитой?
28. Что такое система управления обновлениями безопасности?
29. Какие элементы входят в регламент эксплуатации защитных систем?
30. Как определить эффективность работы средств защиты?
31. Что такое нагрузочное тестирование систем защиты и в чем его суть?
32. Как определить уязвимые места в эксплуатируемой системе?
33. Какие методы восстановления после сбоев применяются на практике?
34. Как оформляется отчет об эксплуатации систем защиты?
35. Какие разделы обязательно включает итоговый отчет по практике?
36. В чем заключались трудности при обслуживании защитных систем?
37. Как вы оцениваете свою подготовку к эксплуатационным задачам?
38. Какие новые навыки администрирования вы приобрели?
39. Какие знания, полученные в аудитории, пригодились при эксплуатации?
40. Какой аспект работы показался наиболее сложным и почему?
41. В каком виде вы сдавали отчеты о работе систем (логи, отчеты, скриншоты)?
42. Что такое система ticketing и как с ней работать?
43. Какова роль автоматизации в эксплуатации систем безопасности?
44. Какие методы использовались для оценки эффективности защиты?
45. Какие программные средства использовались для анализа угроз?
46. Что такое матрица доступа в системе безопасности?
47. Какие навыки взаимодействия с другими отделами вы отработали?
48. Какие выводы вы сделали по результатам эксплуатационной практики?
49. Как вы оцениваете значимость полученного опыта для будущей работы?
50. Какие предложения по улучшению процесса эксплуатации вы можете дать?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Производственная практика(эксплуатационная)" 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 6 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	Санкт-Петербург: 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 (эксплуатационная)" 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.