МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Практикум по решению эксплуатационных задач профессиональной деятельности

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	Виды контроля в семестрах:
в том числе:		зачеты 7
аудиторные занятия	32,25	
самостоятельная работа	75,75	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
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.	32,25	32,25	32,25	32,25
Контактная работа	32,25	32,25	32,25	32,25
Сам. работа	75,75	75,75	75,75	75,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цели: Получение практических навыков научно-исследовательской и проектно-конструкторской деятельности в лабораторных и производственных условиях путем непосредственного участия студентов в решении актуальных эксплуатационных задач с раскрытием индивидуальных особенностей и способностей.
1.2	Задачи:
1.3	Подготовка студентов к самостоятельной работе в сфере информационной безопасности.
1.4	Применение студентами знаний и умений, полученных при изучении дисциплин специальности для решения междисциплинарных задач в сфере информационной безопасности.
1.5	Овладение навыками анализа имеющихся ресурсов и управления ими для решения поставленных задач обеспечения защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.10
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	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)
2.2.4	Производственная практика (технологическая)

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	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;
3.1.3	правовые основы организации защиты государственной тайны и/или конфиденциальной информации; задачи органов защиты государственной тайны и/или служб защиты информации на предприятии, 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
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;
3.2.3	анализировать правовые акты и осуществлять правовую оценку информации, циркулирующей в автоматизированной системе, 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;
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;
3.3.3	разработки организационно-распорядительных документов по защите информации в автоматизированных системах, применения инструментов администрирования подсистем информационной безопасности автоматизированной системы;

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. Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность)						
1.1	Разработка Модели нарушителя /Пр/	7	6	ПК-5	Л1.1 Л1.2	0	
1.2	Изучение требований к ТЗ /Пр/	7	4	ПК-5	Л1.1 Л1.2	4	
1.3	Разработка ТЗ на обеспечение безопасности ИСПДн /Пр/	7	6	ПК-5	Л1.1 Л1.2	0	
1.4	Разработка ТЗ на обеспечение безопасности ГИС (МИС) /Пр/	7	4	ПК-5	Л1.1 Л1.2	0	
1.5	Организационные аспекты реализации ТЗ /Пр/	7	6	ПК-5	Л1.1 Л1.2	0	

1.6	Защита ТЗ /Пр/	7	6	ПК-5	Л1.1 Л1.2	0	
1.7	Поиск и аналитико-синтетическая обработка информации по проблемам ИБ /Ср/	7	75,75	ПК-5	Л1.1 Л1.2	0	
1.8	зачет /ИВКР/	7	0,25	ПК-5	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

1. Какие методы научно-исследовательской работы применимы в информационной безопасности?
2. Каковы особенности проектно-конструкторской деятельности в ИБ?
3. Какие типы эксплуатационных задач характерны для сферы информационной безопасности?
4. В чем заключается отличие лабораторной и производственной среды при выполнении ИБ-проектов?
5. Как организовать практическую деятельность по ИБ в производственных условиях?
6. Какие подходы используются для выявления актуальных проблем в области информационной безопасности?
7. Как оценить актуальность задачи в ИБ и приоритет её решения?
8. Какие этапы включает научно-исследовательский процесс в области защиты информации?
9. Какие источники информации и данные можно использовать для исследований в сфере ИБ?
10. Как оформляются результаты научных исследований по ИБ?
11. Какие инструменты применяются при проектировании технических решений по ИБ?
12. Как документируются проектно-конструкторские решения в области ИБ?
13. Что такое эксплуатационная надёжность в контексте информационной безопасности?
14. Как анализируются проблемы эксплуатации ИБ-систем?
15. Какие методы используются для оптимизации эксплуатации ИБ-средств?
16. Как решать задачи адаптации ИБ-систем под специфические условия объекта?
17. В чем заключается роль студента в решении эксплуатационных задач по ИБ?
18. Как раскрываются индивидуальные особенности студента при работе над ИБ-проектами?
19. Какие методы анализа эффективности проектных решений по ИБ существуют?
20. Как оценить влияние человеческого фактора на выполнение проектных задач в ИБ?
21. Какие компетенции необходимы для самостоятельной работы в сфере информационной безопасности?
22. Как определить степень готовности к самостоятельной работе в области ИБ?
23. Какие знания и умения наиболее востребованы для решения задач информационной безопасности?
24. Как применять полученные знания по программированию при проектировании ИБ-средств?
25. Как используются знания сетевых технологий при решении задач ИБ?
26. Как междисциплинарные знания влияют на качество решений в ИБ?
27. Как организовать междисциплинарную командную работу в сфере ИБ?
28. Какие риски возникают при решении ИБ-задач междисциплинарного характера?
29. Какие методы применяются для оценки уязвимостей информационных систем?
30. Как анализировать угрозы информационной безопасности при разработке проекта?
31. Какие подходы существуют к выбору ИБ-средств с учетом имеющихся ресурсов?
32. Как оценивать доступность ресурсов при проектировании защиты информации?
33. Какие типы ресурсов критически важны при проектировании и внедрении ИБ-систем?
34. Как управлять ограниченными ресурсами в условиях реального проекта по ИБ?
35. Как оценить рентабельность внедрения средств защиты информации?
36. В чем специфика ИБ-проектов в коммерческом и государственном секторе?
37. Какие методы управления проектами наиболее применимы в ИБ?
38. Как формулировать цели и задачи в рамках проектной деятельности по ИБ?
39. Как обосновать выбор технического решения в проекте по защите информации?
40. Какие стандарты и нормативные документы регулируют проектирование ИБ-систем?
41. Какие существуют подходы к валидации и верификации решений по ИБ?
42. В чем заключается контроль качества в проектно-исследовательской работе по ИБ?
43. Как составляется отчет о выполненной проектной или исследовательской работе по ИБ?
44. Какие формы представления результатов применимы в ИБ-деятельности?
45. Какие современные технологии целесообразно включать в ИБ-проекты?
46. Какова роль этики и правовых аспектов при решении эксплуатационных задач в ИБ?
47. Какие компетенции развиваются у студента при участии в ИБ-проекте?
48. Как оценить прогресс в практической подготовке студента в сфере ИБ?
49. Какие ИБ-инструменты наиболее подходят для студентов на этапе подготовки?
50. Как планировать развитие индивидуальной траектории в научно-проектной деятельности по ИБ?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Практикум по решению эксплуатационных задач профессиональной деятельности" 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	Зенков А. В.	Методы оптимальных решений: учебное пособие для вузов	Москва: Юрайт, 2024
Л1.2	Петренко В. И., Мандрица И. В.	Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов	Санкт-Петербург: Лань, 2025

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 "Практикум по решению эксплуатационных задач профессиональной деятельности" 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.