МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Мероприятия по оценке защищенности объектов критической информационной инфраструктуры

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 **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:
в том числе:		экзамены 11
аудиторные занятия	58,35	
самостоятельная работа	58,65	
часов на контроль	27	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**11 (6.1)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	28	28	28	28
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	58,35	58,35	58,35	58,35
Контактная работа	58,35	58,35	58,35	58,35
Сам. работа	58,65	58,65	58,65	58,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является приобретение знаний о проблемах обеспечения кибербезопасности в критических системах и навыков, которые необходимы при работе по обеспечению информационной безопасности АСУ ТП на критических объектах. Дисциплина включает материалы, лежащие на стыке двух отраслей: информационная безопасность и автоматизация производств.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.10
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-3: Способен выполнять работы по мониторингу и аудиту защищенности информации в автоматизированных системах	
Знать:	
Уровень 1	архитектуру промышленных сетей АСУ ТП; физические принципы, на которых строятся системы инженерно-технической защиты объектов; типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП
Уровень 2	средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации; основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями в безопасности SIEM
Уровень 3	принципы работы систем мониторинга информационной безопасности автоматизированных систем; методы и средства обеспечения информационной безопасности в системах электронного документооборота
Уметь:	
Уровень 1	применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП; проводить оптимизацию структуры комплексов инженерно-технической защиты объектов
Уровень 2	проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП; использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности
Уровень 3	формировать правила анализа событий мониторинга информационной безопасности автоматизированных систем; определять необходимые методы и средства обеспечения информационной безопасности в системах электронного документооборота
Владеть:	
Уровень 1	навыком определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП; навыком анализа критериев оценки параметров технических средств охраны объектов
Уровень 2	навыком составления программы испытаний систем инженерно- технической защиты объектов; навыком оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП
Уровень 3	навыком использования методов мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; навыком проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.2	**Уметь:**
3.3	**Владеть:**

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. Введение						
1.1	Эволюция АСУ ТП Технологии современных АСУ ТП /Лек/	11	2	ПК-3	Л1.1	0	

1.2	Введение /Ср/	11	5	ПК-3	Л1.1	0	
	Раздел 2. Объект исследования – интеллектуальная АСУ ТП						
2.1	Основные определения в области промышленной автоматизации. Модель промышленной системы по ФСТЭК. Модель промышленной системы PERA /Лек/	11	2	ПК-3	Л1.1	0	
2.2	Анализ структур различных АСУ ТП /Пр/	11	2	ПК-3	Л1.1	1	
2.3	Объект исследования – интеллектуальная АСУ ТП /Ср/	11	6	ПК-3	Л1.1	0	
	Раздел 3. Функциональная безопасность АСУ ТП						
3.1	Функциональная безопасность в АСУ ТП. Функциональная и информационная безопасность. Их взаимосвязь и противоречие. Дерево сбоев и атак. Единая модель. /Лек/	11	2	ПК-3	Л1.1	0	
3.2	Рассмотрение моделей и расчёт рисков функциональной безопасности /Пр/	11	4	ПК-3	Л1.1	0	
3.3	Функциональная безопасность АСУ ТП /Ср/	11	6	ПК-3	Л1.1	0	
	Раздел 4. Проблема обеспечения кибербезопасности АСУ ТП						
4.1	Нормативные документы Российской федерации в области кибербезопасности. 31 приказ ФСТЭК и другие документы Федеральный закон 187 Международные нормативные документы. Документы NERC CIP, NIST Понятие эшелонированной защиты. Трудности при внедрении эшелонированной защиты. /Лек/	11	2	ПК-3	Л1.1	0	
4.2	Проблемы обеспечения безопасности современных промышленных систем. Атаки на современные промышленные системы – общие положения. Уязвимости современных промышленных системы – причины. Устранение уязвимостей. Обновление программного обеспечения промышленных систем. Проблемы устранения уязвимостей и способы их решения. Отличительные особенности и проблемы обеспечения методов обеспечения кибербезопасности промышленных предприятий. Угрозы информационной безопасности в АСУ ТП. Объекты защиты АСУ ТП /Лек/	11	2	ПК-3	Л1.1	0	
4.3	Анализ проблем защищённости и выработка требований к защите типовых АСУ ТП /Пр/	11	4	ПК-3	Л1.1	1	
4.4	Проблема обеспечения кибербезопасности АСУ ТП /Ср/	11	6	ПК-3	Л1.1	0	
	Раздел 5. Атаки на интеллектуальные АСУ ТП						

5.1	Типовая схема вторжения. Атаки на сети промышленных систем. Сканирование сетевых систем. Средства сканирования сетевых систем. /Лек/	11	2	ПК-3	Л1.1	0	
5.2	Модель атаки и нарушителя АСУ ТП /Пр/	11	4	ПК-3	Л1.1	0	
5.3	Атаки на интеллектуальные АСУ ТП /Ср/	11	6	ПК-3	Л1.1	0	
	Раздел 6. Безопасность сетей АСУ ТП						
6.1	Обзор протоколов сетей АСУ ТП. /Лек/	11	2	ПК-3	Л1.1	0	
6.2	Принципы работы и вопросы безопасности сетей АСУ ТП /Лек/	11	2	ПК-3	Л1.1	0	
6.3	Разбор протоколов сетей АСУ ТП /Пр/	11	2	ПК-3	Л1.1	1	
6.4	Подходы по интеграции в сеть АСУ ТП защитных решений /Пр/	11	2	ПК-3	Л1.1	0	
6.5	Безопасность сетей АСУ ТП /Ср/	11	6	ПК-3	Л1.1	0	
	Раздел 7. Защита изолированных сетей						
7.1	Понятие «воздушного зазора». Способы атак на промышленные системы, не подключенные к сети Интернет. Преодоление «воздушного зазора». Сменные носители. Политика использования сменных носителей Атака со стороны поставщиков и внутренних нарушителей. Методы защиты от атак со стороны поставщиков и внутренних нарушителей. /Лек/	11	2	ПК-3	Л1.1	0	
7.2	Угрозы и защита беспроводных коммуникаций в сетях АСУ ТП. Удаленный доступ и его защита. /Лек/	11	2	ПК-3	Л1.1	0	
7.3	Защита изолированных сетей /Ср/	11	6,65	ПК-3	Л1.1	0	
	Раздел 8. Социальная инженерия						
8.1	Фишинг с использованием электронной почты. Признаки фишинга. Направленный фишинг. Фишинг с использованием социальных сетей. /Лек/	11	2	ПК-3	Л1.1	0	
8.2	Рассмотрение подходов различных видов социальной инженерии /Пр/	11	2	ПК-3	Л1.1	1	
8.3	Социальная инженерия /Ср/	11	5	ПК-3	Л1.1	0	
	Раздел 9. Типовое вредоносное ПО АСУ ТП						
9.1	Разбор известных инцидентов атаки промышленных систем посредством вредоносного ПО. /Лек/	11	4	ПК-3	Л1.1	0	
9.2	Обзор типового вредоносного ПО АСУ ТП /Пр/	11	4	ПК-3	Л1.1	0	
9.3	Типовое вредоносное ПО АСУ ТП /Ср/	11	6	ПК-3	Л1.1	0	
	Раздел 10. Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности						

10.1	Подразделение ИБ АСУ ТП. Особенности организации работы. Задачи подразделения кибербезопасности. Взаимодействие с другими структурами /Лек/	11	2	ПК-3	Л1.1	0	
10.2	Деловая игра по формированию подразделения ИБ АСУ ТП /Пр/	11	4	ПК-3	Л1.1	0	
10.3	Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности /Ср/	11	6	ПК-3	Л1.1	0	
10.4	Экзамен /ИВКР/	11	2,35			0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Эволюция и современные технологии АСУ ТП
1. Какие этапы развития можно выделить в истории АСУ ТП?
2. Чем отличаются традиционные и современные АСУ ТП?
3. Как влияние цифровизации на развитие промышленной автоматизации?
4. Какие современные технологии используются в построении АСУ ТП?
5. В чём особенности внедрения IoT и IIoT в промышленные системы?
Тема 2: Основные понятия и модели промышленных систем
6. Что такое АСУ ТП и какие её основные компоненты?
7. Какова структура промышленной системы по классификации ФСТЭК?
8. Что представляет собой модель промышленной системы PERA?
9. Какие уровни взаимодействия выделяются в промышленных системах?
10. Какие стандарты описывают архитектуру промышленных сетей (например, ISA/IEC 62443)?
Тема 3: Функциональная и информационная безопасность
11. Что понимается под функциональной безопасностью в АСУ ТП?
12. Чем отличается функциональная безопасность от информационной?
13. Какие противоречия могут возникать между ними при внедрении?
14. Что такое дерево сбоев и как оно используется в анализе безопасности?
15. Как строится единая модель анализа рисков и угроз в АСУ ТП?
Тема 4: Нормативно-правовая база РФ и международные стандарты
16. Какие федеральные законы регулируют вопросы кибербезопасности в России?
17. Что регламентирует Приказ ФСТЭК №31?
18. Какой смысл несёт Федеральный закон №187-ФЗ?
19. Какие международные стандарты применяются в области ИБ АСУ ТП?
20. Что представляют собой документы NIST, IEC 62443, NERC CIP?
Тема 5: Эшелонированная защита АСУ ТП
21. Что такое эшелонированная защита и как она реализуется?
22. Какие уровни защиты выделяются в промышленных системах?
23. Какие трудности возникают при внедрении зонирования и разделения сетей?
24. Как организуется защита между различными уровнями АСУ ТП?
25. Как обеспечивается межсетевой экран между IT и OT-средами?
Тема 6: Угрозы и уязвимости в АСУ ТП
26. Какие типичные угрозы существуют для промышленных систем?
27. Почему уязвимы устаревшие протоколы промышленных сетей?
28. Какие последствия может иметь атака на систему SCADA?
29. Какие причины возникновения уязвимостей в промышленных системах?
30. Какие проблемы возникают при обновлении программного обеспечения АСУ ТП?
Тема 7: Особенности обеспечения кибербезопасности промышленных предприятий
31. Чем отличаются подходы к защите промышленных и офисных сетей?
32. Какие объекты требуют особого внимания в АСУ ТП?
33. Какие ограничения накладывает надёжность оборудования на обеспечение безопасности?
34. Как влияет необходимость бесперебойной работы на выбор методов защиты?
35. Как организовать защиту в условиях ограниченной совместимости?
Тема 8: Сценарии вторжения и сетевые атаки
36. Какие типичные сценарии вторжения в промышленные сети?
37. Как осуществляется сканирование и разведка в промышленных сетях?
38. Какие инструменты используются злоумышленниками для аудита сетей?
39. Какие протоколы наиболее уязвимы в промышленных сетях?
40. Как происходит эксплуатация уязвимостей протоколов Modbus, DNP3 и других?
Тема 9: Протоколы и безопасность сетей АСУ ТП

41. Какие протоколы используются в АСУ ТП и почему они уязвимы?
42. Какие особенности работы протоколов влияют на безопасность?
43. Какие меры защиты протоколов применяются в промышленных системах?
44. Какие проблемы связаны с шифрованием данных в промышленных протоколах?
45. Как обеспечивается целостность и конфиденциальность передаваемых данных?

Тема 10: «Воздушный зазор» и его преодоление

46. Что такое «воздушный зазор» и как он применяется в промышленности?
47. Какие способы преодоления воздушного зазора известны?
48. Как USB-носители могут использоваться для передачи вредоносного кода?
49. Какие политики использования сменных носителей рекомендованы?
50. Как предотвратить атаки через сторонних поставщиков и внутренних пользователей?

Тема 11: Беспроводные коммуникации и удалённый доступ

51. Какие беспроводные технологии используются в промышленных системах?
52. Какие угрозы связаны с использованием Wi-Fi и ZigBee в АСУ ТП?
53. Как организовать безопасный удалённый доступ к системам управления?
54. Какие протоколы обеспечивают безопасность удалённого доступа?
55. Какие меры применяются для защиты от несанкционированного доступа через удалённые точки?

Тема 12: Социальная инженерия и фишинг

56. Какие виды социальной инженерии распространены в промышленных средах?
57. Что такое фишинг и как он реализуется через электронную почту?
58. Чем отличается направленный фишинг от массового?
59. Как злоумышленники используют социальные сети для атаки на сотрудников?
60. Какие меры повышают устойчивость персонала к атакам социальной инженерии?

Тема 13: Анализ реальных инцидентов

61. Какие известные случаи атак на промышленные системы произошли?
62. Что собой представляет Stuxnet и как он работал?
63. Как происходила атака BlackEnergy на энергетические объекты Украины?
64. Какие уроки извлеклись после инцидента TRITON?
65. Какие выводы сделаны после анализа реальных кибератак на критическую инфраструктуру?

Тема 14: Организация службы информационной безопасности

66. Как организуется подразделение по защите АСУ ТП в крупной организации?
67. Какие задачи выполняет служба кибербезопасности в промышленной среде?
68. Как строится взаимодействие между ИТ-службой и инженерным персоналом?
69. Какие роли и обязанности должны быть определены в структуре ИБ?
70. Какие метрики эффективности используются для оценки деятельности подразделения?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Мероприятия по оценке защищенности объектов критической информационной инфраструктуры" 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 11 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	Музипов Х. Н., Кузяков О. Н., Хохрин С. А., Чащина М. В., Мартынюк Р. В.	Интегрированные системы проектирования и управления. SCADA	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	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")	
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"	
6.3.2.3	База данных научных электронных журналов "eLibrary"	

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 "Мероприятия по оценке защищенности объектов критической информационной инфраструктуры" 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.