МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Основы технической эксплуатации значимых 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	**5 ЗЕТ**

Часов по учебному плану	180	Виды контроля в семестрах:
в том числе:		экзамены 10
аудиторные занятия	100,35	
самостоятельная работа	52,65	
часов на контроль	27	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	14 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	70	70	70	70
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	100,35	100,35	100,35	100,35
Контактная работа	100,35	100,35	100,35	100,35
Сам. работа	52,65	52,65	52,65	52,65
Часы на контроль	27	27	27	27
Итого	180	180	180	180

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является знакомство студентов с принципами, особенностями и способами обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры.
1.2	Задачами дисциплины являются:
1.3	- изучение системы государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;
1.4	- обучение принципам анализа с целью выявления потенциальных уязвимостей безопасности значимых объектов критической информационной инфраструктуры;
1.5	- выработка умений классифицировать и оценивать угрозы безопасности значимых объектов критической информационной инфраструктуры , эффективно использовать различные методы и средства защиты информации;
1.6	- изучение основных средств и способов обеспечения безопасности значимых объектов критической информационной инфраструктуры , принципов построения систем защиты информации.

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-6: Способен обнаруживать, идентифицировать и устранять инциденты, возникшие в процессе эксплуатации автоматизированных систем	
Знать:	
Уровень 1	организационные и технические основы построения систем безопасности значимых объектов критической информационной инфраструктуры и обеспечения их функционирования; угрозы безопасности информации в автоматизированных системах управления и информационных системах;
Уровень 2	порядок проведения расследования компьютерных инцидентов на значимых объектах критической информационной инфраструктуры
Уровень 3	меры по восстановлению функционирования и проверке работоспособности значимого объекта критической информационной инфраструктуры в ходе ликвидации последствий компьютерных атак;
Уметь:	
Уровень 1	осуществлять реагирование на компьютерные инциденты в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;
Уровень 2	определять источники и причины возникновения компьютерных инцидентов
Уровень 3	определять порядок анализа внештатных ситуаций и принимать меры по недопущению их повторного возникновения;
Владеть:	
Уровень 1	навыками обеспечения действий в нештатных ситуациях в ходе эксплуатации значимого объекта критической информационной инфраструктуры;
Уровень 2	реагирования на компьютерные инциденты в ходе эксплуатации значимого объекта критической информационной инфраструктуры;
Уровень 3	навыком проведения расследования инцидентов на средствах вычислительной техники и телекоммуникационном оборудовании значимых объектов критической информационной инфраструктуры

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
3.1.2	программно- аппаратные средства защиты информации, входящие в состав систем безопасности значимых объектов критической информационной инфраструктуры;
3.1.3	способы и методы эксплуатации автоматизированных систем в защищенном исполнении при обеспечении безопасности значимых объектов критической информационной инфраструктуры
3.2	**Уметь:**
3.2.1	обеспечивать реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;
3.2.2	обеспечивать в соответствии с требованиями по безопасности реализацию организационных мер и эксплуатацию средств защиты информации;

3.2.3	готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры
3.3	**Владеть:**
3.3.1	технической эксплуатации средств защиты информации при обеспечении безопасности значимых объектов критической информационной инфраструктуры

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. Основные направления государственной политики в области обеспечения безопасности объектов критической инфраструктуры Российской Федерации						
1.1	Понятие критической информационной инфраструктуры Российской Федерации (КИИ РФ). Перечень показателей критериев значимости объектов КИИ РФ. /Лек/	10	1	ПК-6	Л1.1 Л1.2	0	
1.2	Организационные основы обеспечения информационной безопасности КИИ РФ. /Лек/	10	1	ПК-6	Л1.1 Л1.2	0	
1.3	Права и обязанности субъектов КИИ. Государственный контроль и надзор в области обеспечения безопасности объектов КИИ. /Лек/	10	1	ПК-6	Л1.1 Л1.2	0	
1.4	Ответственность за нарушение требований обеспечения безопасности значимых объектов КИИ. /Лек/	10	1	ПК-6	Л1.1 Л1.2	0	
1.5	Понятие критической информационной инфраструктуры Российской Федерации (КИИ РФ). Перечень показателей критериев значимости объектов 2 КИИ РФ и и их значения. /Пр/	10	4	ПК-6	Л1.1 Л1.2	0	
1.6	Организационные основы обеспечения информационной безопасности КИИ РФ. /Пр/	10	4	ПК-6	Л1.1 Л1.2	0	
1.7	Права и обязанности субъектов КИИ. Государственный контроль и надзор в области обеспечения безопасности объектов КИИ. /Пр/	10	4	ПК-6	Л1.1 Л1.2	0	
1.8	Ответственность за нарушение требований обеспечения безопасности значимых объектов КИИ. /Пр/	10	4	ПК-6	Л1.1 Л1.2	0	
1.9	Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия /Ср/	10	17,55	ПК-6	Л1.1 Л1.2	0	
	Раздел 2. Особенности обеспечения информационной безопасности на различных этапах жизненного цикла объектов критической информационной инфраструктуры						
2.1	Перечень показателей критериев значимости объектов объектов КИИ. Порядок категорирования объектов КИИ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
2.2	Стадии жизненного цикла безопасности объектов КИИ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	

2.3	Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
2.4	Анализ угроз безопасности информации и разработка модели угроз безопасности объектов КИИ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
2.5	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
2.6	Перечень показателей критериев значимости объектов объектов КИИ. Порядок категорирования объектов КИИ. Стадии жизненного цикла безопасности объектов КИИ. /Пр/	10	4	ПК-6	Л1.1 Л1.2	4	
2.7	Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования. /Пр/	10	4	ПК-6	Л1.1 Л1.2	0	
2.8	Анализ угроз безопасности информации и разработка модели угроз безопасности объектов КИИ. /Пр/	10	6	ПК-6	Л1.1 Л1.2	0	
2.9	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ. /Пр/	10	6	ПК-6	Л1.1 Л1.2	0	
2.10	Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия /Ср/	10	17,55	ПК-6	Л1.1 Л1.2	0	
	Раздел 3. Силы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.						
3.1	Силы обеспечения безопасности значимых объектов КИИ. Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
3.2	Политики обеспечения безопасности значимых объектов КИИ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
3.3	Программно-технические средства обеспечения безопасности значимых объектов КИИ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
3.4	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
3.5	Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
3.6	Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	
3.7	Порядок реагирования и обмена информацией о компьютерных инцидентах между субъектами КИИ РФ. /Лек/	10	2	ПК-6	Л1.1 Л1.2	0	

3.8	Силы обеспечения безопасности значимых объектов КИИ. Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ. /Пр/	10	6	ПК-6	Л1.1 Л1.2	0	
3.9	Политики обеспечения безопасности значимых объектов КИИ. Программно-технические средства обеспечения безопасности значимых объектов КИИ. /Пр/	10	6	ПК-6	Л1.1 Л1.2	0	
3.10	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. /Пр/	10	6	ПК-6	Л1.1 Л1.2	0	
3.11	Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак. /Пр/	10	4	ПК-6	Л1.1 Л1.2	0	
3.12	Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак. /Пр/	10	6	ПК-6	Л1.1 Л1.2	0	
3.13	Порядок реагирования и обмена информацией о компьютерных инцидентах между субъектами КИИ РФ. /Пр/	10	6	ПК-6	Л1.1 Л1.2	0	
3.14	Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия /Ср/	10	17,55	ПК-6	Л1.1 Л1.2	0	
3.15	Экзамен /ИВКР/	10	2,35	ПК-6	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема:1. Понятие КИИ РФ и критерии значимости объектов
1. Что такое критическая информационная инфраструктура (КИИ)? Приведите примеры объектов, входящих в КИИ РФ.
2. Какие критерии значимости объектов КИИ определены в законодательстве РФ (ФЗ-187)? Как они связаны с угрозами экономике, общественной безопасности и жизни людей?
3. Какие ключевые показатели используются для оценки значимости объектов КИИ (например, масштаб воздействия, уровень зависимости от информационных систем)?
4. Как проводится категорирование объектов КИИ? Какие уровни защищенности установлены?
5. Какие последствия могут возникнуть при компрометации объектов КИИ (например, остановка энергетических систем, утечка стратегических данных)?
Тема:2. Организационные основы обеспечения ИБ КИИ РФ
6. Какие структуры и органы отвечают за обеспечение ИБ КИИ в РФ (например, ФСТЭК, ФСБ, Минцифры)?
7. Какие этапы включает жизненный цикл безопасности объектов КИИ (идентификация, анализ рисков, реализация мер, мониторинг)?
8. Как строится система управления рисками на объектах КИИ (например, методологии OCTAVE, FAIR)?
9. Какие стандарты и руководства регулируют безопасность КИИ (например, ГОСТ Р 57580, РД ГКЭ 017-2020)?
10. Какие документы обязательны для разработки и реализации политики безопасности объектов КИИ?
Тема:3. Права и обязанности субъектов КИИ
11. Какие обязанности возлагаются на операторов объектов КИИ согласно ФЗ-187?
12. Какие права имеют субъекты КИИ при взаимодействии с государственными органами (например, доступ к информации, поддержка)?
13. Как организовано взаимодействие между операторами КИИ и федеральными органами (например, ФСТЭК, ФСБ)?
14. Какие меры государственного контроля и надзора применяются к объектам КИИ (например, проверки, сертификация)?
15. Какие требования предъявляются к обучению персонала и тестированию готовности к инцидентам?
Тема:4. Ответственность за нарушение требований ИБ
16. Какие виды ответственности предусмотрены за нарушение требований к ИБ КИИ (административная, уголовная, гражданская)?
17. Какие статьи УК и КоАП применяются к нарушениям в области КИИ?
18. Какие последствия могут быть у утечки данных или остановки технологического процесса на объекте КИИ?
19. Какие санкции применяются к организациям за несоблюдение требований ФЗ-187?
20. Как государство обеспечивает поддержку субъектам КИИ в случае кибератак?

Тема:5. Категорирование объектов КИИ
21. Какие этапы включает процесс категорирования объектов КИИ? Какие документы оформляются?
22. Какие параметры определяют уровень защищенности объекта КИИ (например, критичность, вероятность угроз, ущерб при компрометации)?
23. Какие критерии используются для присвоения категории 1, 2 или 3 объектам КИИ?
24. Какие требования к документированию результатов категорирования?
25. Как часто пересматриваются категории объектов КИИ и защищенности?
Тема:6. Жизненный цикл безопасности объектов КИИ
26. Какие этапы включает жизненный цикл безопасности объектов КИИ (проектирование, внедрение, эксплуатация, обновление)?
27. Какие меры безопасности должны быть реализованы на этапе проектирования АС?
28. Как организуется мониторинг и обновление мер ИБ в рамках эксплуатации объекта КИИ?
29. Какие аспекты учитываются при выводе объекта КИИ из эксплуатации?
30. Какие проблемы возникают при переходе от традиционных систем к защищенным АС на объектах КИИ?
Тема:7. Требования к системам безопасности объектов КИИ
31. Какие функции безопасности обязательны для систем КИИ (например, защита от НСД, целостность данных, доступность)?
32. Какие технические средства защиты должны использоваться на объектах КИИ (например, МЭ, СОВ, САВЗ)?
33. Какие нормативные документы регламентируют выбор и сертификацию СЗИ (например, РД ФСТЭК, ГОСТ Р 57580)?
34. Какие требования к резервному копированию и аварийному восстановлению на объектах КИИ?
35. Как организуется взаимодействие с внешними поставщиками и подрядчиками на объектах КИИ?
Тема:8. Анализ угроз и моделирование угроз
36. Какие источники угроз наиболее критичны для объектов КИИ (APT, insider threats, DDoS)?
37. Какие методологии используются для анализа угроз (например, MITRE ATT&CK для КИИ)?
38. Как строится модель угроз для объекта КИИ (например, сценарии атак, векторы проникновения)?
39. Какие параметры учитываются при оценке вероятности реализации угроз (например, уровень зрелости ИБ, уязвимости)?
40. Какие метрики позволяют оценить эффективность мер против угроз?
Тема:9. Планирование и реализация мер безопасности
41. Какие этапы включает разработка плана мероприятий по обеспечению ИБ на объекте КИИ?
42. Какие меры защиты реализуются для систем АСУ ТП, энергетики, транспорта?
43. Какие приоритеты при выборе программно-технических средств защиты?
44. Как организуется распределение бюджета на безопасность КИИ?
45. Какие кейсы известны по внедрению СЗИ на объектах КИИ (например, защита АЭС, железнодорожных систем)?
Тема:10. Силы обеспечения безопасности и взаимодействие с органами власти
46. Какие структуры обеспечивают безопасность КИИ внутри организации (например, службы ИБ, отделы физической охраны)?
47. Как организовано взаимодействие с Центром реагирования на компьютерные инциденты (ЦРКИ)?
48. Какие функции выполняет ФСТЭК России при сертификации и контроле КИИ?
49. Какие обязательства у субъектов КИИ по обмену информацией о киберугрозах?
50. Как взаимодействуют субъекты КИИ с правоохранительными органами при инцидентах?
Тема:11. Политики безопасности объектов КИИ
51. Какие элементы включает политика ИБ на объекте КИИ (цели, ограничения, ответственность)?
52. Как политики ИБ согласуются с требованиями ФЗ-187 и стандартами ФСТЭК?
53. Какие меры по контролю за соблюдением политик применяются (например, аудит, обучение персонала)?
54. Как политики ИБ адаптируются под изменения в угрозной среде?
55. Какие ошибки часто допускаются при разработке политик безопасности для КИИ?
Тема:12. Программно-технические средства обеспечения безопасности
56. Какие средства защиты обязательны для объектов КИИ (например, межсетевые экраны, СОВ, антивирусы)?
57. Какие классы защищенности установлены для средств защиты (например, МЭ, СОВ, САВЗ)?
58. Какие требования к шифрованию данных на объектах КИИ (например, ГОСТ Р 34.12-2018, ГОСТ Р 34.10-2018)?
59. Какие технологии используются для контроля целостности и доступа к информации (например, замкнутые программные среды, криптошлюзы)?
60. Какие угрозы возникают из-за устаревших технологий на объектах КИИ?
Тема:13. Государственная система обнаружения и реагирования на атаки
61. Как функционирует государственная система обнаружения, предупреждения и ликвидации последствий атак?
62. Какие требования предъявляются к средствам обнаружения и реагирования на атаки (например, интеграция с ЦРКИ)?
63. Какие технические и организационные меры реализуются для обмена данными о киберугрозах?
64. Как происходит обнародование угроз и уязвимостей между субъектами КИИ?
65. Какие протоколы используются для обмена информацией о компьютерных инцидентах (например, TAXII, STIX)?
Тема:14. Реагирование на инциденты и обмен информацией
66. Какие этапы включает процесс реагирования на инциденты ИБ на объектах КИИ (обнаружение, локализация, восстановление)?
67. Какие формы отчетности используются для передачи информации о киберинцидентах в ЦРКИ?
68. Как организован обмен информацией между субъектами КИИ при массовых атаках (например, через платформы CSIRT)?
69. Какие метрики позволяют оценить эффективность реагирования (например, MTTD, MTTR)?
70. Какие проблемы возникают при синхронизации действий между различными организациями КИИ?

Тема:15. Современные вызовы и перспективы
71. Как искусственный интеллект и машинное обучение используются для обнаружения атак на объектах КИИ?
72. Какие угрозы связаны с утечкой данных через побочные каналы (TEMPEST, акустический шум)?
73. Как квантовые вычисления могут повлиять на криптографические средства защиты на объектах КИИ?
74. Какие риски связаны с интеграцией ОТ и IT-систем (например, уязвимости в протоколах Modbus, IEC 61850)?
75. Какие меры защиты внедряются для IoT-устройств на объектах КИИ?
Тема:16. Практические аспекты и кейсы
76. Какие этапы включает подготовка к атаке на объект КИИ (например, разработка сценариев, пентестинг)?
77. Как организовать симуляцию атаки (red team/blue team) на объекте КИИ?
78. Какие ошибки чаще всего приводят к утечкам данных на объектах КИИ?
79. Какие меры реагирования на атаку Ransomware в энергетических системах?
80. Как подготовить отчет по результатам инцидента (структура, содержание, передача в ФСТЭК)?
Тема:17. Международный опыт и сравнение
81. Какие отличия в подходах к защите КИИ в ЕС (NIS, NIS2), США (CISA) и России (ФЗ-187)?
82. Какие стандарты и фреймворки используются за рубежом для управления рисками (например, NIST Cybersecurity Framework, ISO/IEC 27001)?
83. Какие уроки из зарубежных инцидентов (например, Colonial Pipeline, SolarWinds) применимы к российским объектам КИИ?
84. Как международное сотрудничество (INTERPOL, ENISA) помогает в борьбе с киберугрозами?
85. Какие ограничения у российских подходов к защите КИИ по сравнению с зарубежными?
Тема: 18. Перспективные технологии и стратегии
86. Как технологии Zero Trust применяются для защиты объектов КИИ?
87. Как цифровые двойники используются для тестирования устойчивости КИИ к атакам?
88. Как блокчейн может быть применен для обеспечения целостности данных на объектах КИИ?
89. Какие меры защиты разрабатываются для гибридных систем (локальные + облачные)?
90. Какие тренды будут определять развитие ИБ в КИИ в ближайшие 5 лет (например, защита IIoT, AI-мониторинг)?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Основы технической эксплуатации значимых 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 10 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	Баланов А. Н.	Защита информационных систем. Кибербезопасность: учебное пособие для вузов	Санкт-Петербург: Лань, 2025
Л1.2	Баланов А. Н.	Кибербезопасность: 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 "Основы технической эксплуатации значимых 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.