МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Обеспечение безопасности 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 **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 67,35
самостоятельная работа 49,65
часов на контроль 27

Виды контроля в семестрах:
экзамены 9
курсовые работы 9

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Иные виды контактной работы	3,35	3,35	3,35	3,35
В том числе инт.	4	4	4	4
Итого ауд.	67,35	67,35	67,35	67,35
Контактная работа	67,35	67,35	67,35	67,35
Сам. работа	49,65	49,65	49,65	49,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является знакомство студентов с принципами, особенностями и способами обеспечения информационной безопасности всего жизненного цикла на критически важных объектах.
1.2	Задачами дисциплины являются:
1.3	- изучение системы государственного контроля в области обеспечения информационной безопасности на критически важных объектах и системы признаков критически важных объектов;
1.4	- обучение принципам анализа с целью выявления потенциальных уязвимостей информационной безопасности на критически важных объектах;
1.5	- выработка умений классифицировать и оценивать угрозы информационной безопасности для критически важных объектов, эффективно использовать различные методы и средства защиты информации;
1.6	- изучение основных средств и способов обеспечения информационной безопасности на критически важных объектах, 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-2: Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
Знать:	
Уровень 1	основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; основные алгоритмы при цифровой обработке сигналов, факторы, определяющие связь эксплуатационных свойств систем цифровой обработки сигналов с их техническими характеристиками; цели и задачи проектирования систем инженерно-технической защиты объектов; основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов
Уровень 2	основные принципы проектирования систем инженерно-технической защиты объектов; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование
Уровень 3	базовые алгоритмы анализа данных: k-средних, метод опорных векторов, линейная регрессия, ассоциативные правила, деревья решений, анализ выбросов или анализ аномалий, искусственные нейронные сети; меры, операции и приемы, направленные на предотвращение утечки защищаемой информации, несанкционированного и непреднамеренного воздействия на защищаемую информацию в сферах федерального, регионального управления и электронной коммерции; основные этапы реализации проектных решений в области автоматизированных систем электронного документооборота
Уметь:	
Уровень 1	определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; обоснованно оценивать необходимые параметры дискретизации и квантования, интерполяции и децимации сигналов; объяснять принцип методов оценки параметров сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления; изучать научно-техническую информацию, отечественный и зарубежный опыт и организовывать работы по практическому использованию новых технологий в области цифровой обработки сигналов
Уровень 2	проводить анализ вероятных угроз охраняемому объекту; выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту; выбирать технические средства для решения задачи охраны объекта; определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации; реализовывать в виде программного кода базовые алгоритмы анализа данных: k- средних, метод опорных векторов, линейная регрессия, ассоциативные правила, искусственные нейронные сети
Уровень 3	способы построения систем с нечеткой логикой; изучать научно-техническую информацию, отечественный и зарубежный опыт и организовывать работы по практическому использованию новых технологий в области интеллектуального анализа данных; вырабатывать и принимать организационно- технические решения, адекватные степени угроз, в различных

	отраслях деятельности; разрабатывать защищенные системы электронного документооборота
Владеть:	
Уровень 1	навыком применения типовых прикладных пакетов для синтеза алгоритмов цифровой обработки сигналов, используемых в системах обеспечения информационной безопасности автоматизированных систем управления; навыком разработки проектов нормативных документов, регламентирующих работу по защите информации
Уровень 2	навыком разработки алгоритмов интеллектуального анализа данных в системах информационной безопасности; навыком разработки предложений по совершенствованию систем информационной безопасности предприятий и организаций, комплексно обеспечивающих повышение ее уровня
Уровень 3	навыком разработки и анализом проектных решений в области автоматизированных систем электронного документооборота

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:**
3.2	**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. Объекты критической информационной инфраструктуры РФ						
1.1	Основные направления государственной политики в области обеспечения безопасности критически важных объектов инфраструктуры Российской Федерации /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
1.2	Организационные основы обеспечения информационной безопасности критической информационной инфраструктуры. /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
	Раздел 2. Порядок категорирования объектов критической информационной инфраструктуры						
2.1	Общий порядок категорирования. Виды категорий значимости /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
2.2	Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
2.3	Права и обязанности субъектов критической информационной инфраструктуры /Лек/	9	1	ПК-2 ПК-5	Л1.1	0	
2.4	Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры /Лек/	9	1	ПК-2 ПК-5	Л1.1	0	
2.5	Определение принадлежности организации к субъектам критической информационной инфраструктуры /Пр/	9	2	ПК-2 ПК-5	Л1.1	1	
2.6	Определение критических процессов, нарушение и/или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка /Пр/	9	2	ПК-2 ПК-5	Л1.1	0	
2.7	Формирование сводного перечня объектов критической информационной инфраструктуры в организации /Пр/	9	2	ПК-2 ПК-5	Л1.1	0	

2.8	Формирование исходных данных на каждый объект критической информационной инфраструктуры /Пр/	9	4	ПК-2 ПК-5	Л1.1	2	
2.9	Категорирование объектов критической информационной инфраструктуры в соответствии с перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений /Пр/	9	2	ПК-2 ПК-5	Л1.1	1	
	Раздел 3. Особенности обеспечения информационной безопасности для всего жизненного цикла объектов критической информационной инфраструктуры.						
3.1	Стадии жизненного цикла безопасности объектов критической информационной инфраструктуры в целом /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
3.2	Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры и обеспечению их функционирования . /Лек/	9	4	ПК-2 ПК-5	Л1.1	0	
3.3	Анализ угроз безопасности информации и разработка модели угроз безопасности информации /Пр/	9	4	ПК-2 ПК-5	Л1.1	0	
3.4	Рассмотрение возможных действий нарушителей, иных источников угроз безопасности. Анализ угроз и уязвимостей. Подготовка модели угроз. /Пр/	9	6	ПК-2 ПК-5	Л1.1	0	
3.5	Подготовка формы направления сведений о результатах присвоения объекту одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий /Пр/	9	2	ПК-2 ПК-5	Л1.1	0	
3.6	Разработка требований к оформлению концепции для всего жизненного цикла обеспечения информационной безопасности объекта. /Пр/	9	2	ПК-2 ПК-5	Л1.1	0	
3.7	Выполнение заданий поисково – исследовательского характера /Ср/	9	24,5	ПК-2 ПК-5	Л1.1	0	
	Раздел 4. Организационно-технические и режимные меры информационной безопасности на объектах критической информационной инфраструктуры.						
4.1	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
4.2	Силы обеспечения безопасности значимых объектов /Лек/	9	1	ПК-2 ПК-5	Л1.1	0	
4.3	Установление требований к обеспечению безопасности значимого объекта /Лек/	9	3	ПК-2 ПК-5	Л1.1	0	
4.4	Политики информационной безопасности критически важных объектов /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	

4.5	Составление плана мероприятий по обеспечению безопасности на значимом объекте /Пр/	9	0	ПК-2 ПК-5	Л1.1	0	
4.6	Разработка организационно-распорядительных документов по безопасности значимых объектов критической информационной инфраструктуры /Пр/	9	4	ПК-2 ПК-5	Л1.1	0	
	Раздел 5. Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности.						
5.1	Средства защиты информации, использующиеся на значимых объектах и оценка их эффективности. /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
5.2	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации /Лек/	9	4	ПК-2 ПК-5	Л1.1	0	
5.3	Выбор средств защиты информации /Пр/	9	2	ПК-2 ПК-5	Л1.1	0	
5.4	Проработка лекционного материала /Ср/	9	25,15	ПК-2 ПК-5	Л1.1	0	
	Раздел 6. Государственный контроль и надзор в области обеспечения информационной безопасности на значимых объектах.						
6.1	Контроль мер обеспечения информационной безопасности на значимых объектах. /Лек/	9	2	ПК-2 ПК-5	Л1.1	0	
6.2	Курсовая работа /КР/	9	27	ПК-2 ПК-5	Л1.1	0	
6.3	Экзамен /ИВКР/	9	3,35	ПК-2 ПК-5	Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Основные направления государственной политики в области безопасности КИИ
1. Каково значение критической информационной инфраструктуры для национальной безопасности?
2. Какие цели и задачи государства в сфере обеспечения безопасности КИИ?
3. Какие федеральные органы участвуют в обеспечении безопасности КИИ?
4. Какие нормативно-правовые акты регулируют вопросы защиты КИИ?
5. Какова роль Концепции противодействия киберугрозам в России?
Тема 2: Организационные основы обеспечения ИБ КИИ
6. Что понимается под системой обеспечения информационной безопасности КИИ?
7. Как организуется взаимодействие между государственными и частными субъектами КИИ?
8. Как строится система управления рисками ИБ в организациях КИИ?
9. Какие функции выполняет служба информационной безопасности на значимых объектах?
10. Как проводится внутренний и внешний аудит системы ИБ?
Тема 3: Общий порядок категорирования. Виды категорий значимости
11. Что такое категорирование объектов КИИ и как оно проводится?
12. Какие категории значимости установлены законодательством РФ?
13. Как определяется уровень значимости объекта?
14. Какие параметры учитываются при отнесении объекта к той или иной категории?
15. Какие документы требуются для прохождения процедуры категорирования?
Тема 4: Показатели значимости объектов КИИ
16. Какие критерии используются для определения значимости объекта?
17. Как влияет экономическая, социальная и стратегическая значимость на категорию объекта?
18. Как учитывается потенциальный ущерб от нарушения функционирования объекта?
19. Какие последствия могут возникнуть при компрометации информации КИИ?
20. Какие примеры показателей значимости приведены в методических рекомендациях?

Тема 5: Права и обязанности субъектов КИИ
21. Какие организации считаются субъектами КИИ?
22. Какие права имеют субъекты КИИ?
23. Какие обязательства несут субъекты КИИ перед государством?
24. Как организуется сотрудничество с ФСТЭК, ФСБ и другими структурами?
25. Какие меры ответственности предусмотрены за нарушение требований?
Тема 6: Взаимодействие с федеральным органом исполнительной власти
26. С каким органом взаимодействует субъект КИИ?
27. Как осуществляется обмен информацией о компьютерных инцидентах?
28. Какие формы отчетности предусмотрены для субъектов КИИ?
29. Как происходит согласование планов построения и модернизации систем ИБ?
30. Как организуется участие в мероприятиях по тестированию готовности к угрозам?
Тема 7: Жизненный цикл безопасности объектов КИИ
31. Какие этапы жизненного цикла безопасности выделяются?
32. Как планируется защита на этапе проектирования?
33. Как обеспечивается непрерывное сопровождение мер безопасности?
34. Как организовано обновление и развитие систем ИБ?
35. Как проводится ликвидация или переход к новым технологиям?
Тема 8: Требования к созданию и функционированию систем безопасности значимых объектов КИИ
36. Какие требования предъявляются к системам защиты информации?
37. Какие технические меры должны быть реализованы?
38. Как организуется управление доступом и учёт действий пользователей?
39. Как обеспечивается резервирование и восстановление после инцидентов?
40. Какие меры физической и административной безопасности применяются?
Тема 9: Анализ угроз и разработка модели угроз безопасности информации
41. Что представляет собой модель угроз и зачем она нужна?
42. Какие источники угроз учитываются при её построении?
43. Как классифицируются угрозы по уровню сложности и масштабу воздействия?
44. Как формируется дерево угроз и карта рисков?
45. Как модель угроз используется при выборе средств защиты?
Тема 10: Планирование и реализация мероприятий по обеспечению ИБ
46. Как разрабатываются мероприятия по защите объектов КИИ?
47. Как строится план обеспечения безопасности?
48. Какие меры являются первоочередными?
49. Как организуется внедрение комплекса мер по защите информации?
50. Какие документы оформляются при проведении работ?
Тема 11: Силы обеспечения безопасности значимых объектов
51. Какие силы обеспечивают защиту значимых объектов КИИ?
52. Какие функции выполняют службы безопасности и внешние эксперты?
53. Как организовано взаимодействие с правоохранительными органами?
54. Какие полномочия имеет персонал при реагировании на инциденты?
55. Как строится система обучения и повышения квалификации специалистов?
Тема 12: Установление требований к обеспечению ИБ значимого объекта
56. Какие требования к ИБ устанавливаются законодательством?
57. Какие технические, программные и организационные меры обязательны?
58. Как устанавливается соответствие требованиям стандартов и нормативов?
59. Как требования трансформируются в конкретные действия?
60. Как проверяется выполнение установленных требований?
Тема 13: Политики информационной безопасности критически важных объектов
61. Что такое политика информационной безопасности и каково её назначение?
62. Какие разделы должна содержать политика ИБ?
63. Как политика связана с нормативной и правовой базой?
64. Как организовать обучение сотрудников политике ИБ?
65. Как политика влияет на выбор технических решений?
Тема 14: Средства защиты информации и их эффективность
66. Какие виды средств защиты информации применяются на объектах КИИ?
67. Какие средства шифрования, контроля доступа и обнаружения вторжений используются?
68. Как проводится сертификация и оценка соответствия используемых средств?
69. Как оценивается эффективность средств защиты?
70. Как происходит выбор наиболее подходящих решений?
Тема 15: Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)
71. Что представляет собой ГосСОПКА и какие задачи она решает?
72. Какова структура и состав участников ГосСОПКА?
73. Какие функции выполняет Центр мониторинга и реагирования?
74. Как происходит сбор, анализ и распространение информации о киберугрозах?
75. Как взаимодействует ГосСОПКА с субъектами КИИ?
Тема 16: Контроль мер обеспечения ИБ на значимых объектах

76. Как организован контроль за соблюдением требований ИБ на значимых объектах?
77. Какие виды проверок и инспекций проводятся?
78. Какие документы изучаются при проверке?
79. Как оценивается степень защищенности объекта?
80. Какие действия необходимо предпринять при выявлении нарушений?

5.2. Темы письменных работ

Часть 1: Государственная политика и нормативно-правовая база
1. Анализ государственной политики в области защиты критической информационной инфраструктуры РФ.
2. Сравнительный анализ законодательства РФ и стран ЕС в сфере ИБ КИИ.
3. Роль ФСТЭК России в обеспечении безопасности критических информационных систем.
4. Оценка влияния Федерального закона №187-ФЗ на организацию защиты КИИ.
5. Правовые основы категорирования объектов КИИ в Российской Федерации.
Часть 2: Категорирование объектов КИИ
6. Методика категорирования объектов КИИ: анализ показателей значимости.
7. Проблемы и сложности при прохождении процедуры категорирования.
8. Автоматизация процесса категорирования объектов КИИ.
9. Сравнение подходов к оценке значимости объектов в различных отраслях.
10. Оценка потенциального ущерба как ключевого фактора категорирования.
Часть 3: Жизненный цикл безопасности и организация ИБ
11. Этапы жизненного цикла безопасности объектов КИИ и их особенности.
12. Разработка модели управления рисками для объектов критической инфраструктуры.
13. Особенности построения системы управления ИБ на значимых объектах.
14. Внедрение международных стандартов ИБ (ISO/IEC 27001) в КИИ.
15. Управление изменениями в системе безопасности значимых объектов.
Часть 4: Политики безопасности и модель угроз
16. Разработка политики информационной безопасности для организации — субъекта КИИ.
17. Создание модели актуальных угроз для предприятия горнодобывающей промышленности.
18. Сравнение моделей угроз по MITRE ATT&CK и собственным разработкам.
19. Построение дерева угроз для транспортной системы в рамках КИИ.
20. Интеграция модели угроз в систему управления рисками объекта КИИ.
Часть 5: Технические меры защиты и средства ИБ
21. Оценка эффективности средств обнаружения вторжений (IDS/IPS) на объектах КИИ.
22. Применение шифрования данных в системах управления технологическими процессами.
23. Использование межсетевых экранов нового поколения в защите КИИ.
24. Организация резервного копирования и восстановления информации на значимых объектах.
25. Сравнительный анализ аппаратных и программных средств защиты информации на КИИ.
Часть 6: Взаимодействие с ГосСОПКА и контроль защищенности
26. Взаимодействие с ГосСОПКА: практика и проблемы.
27. Анализ требований ФСТЭК к предоставлению информации в ГосСОПКА.
28. Роль автоматизированных систем реагирования в составе ГосСОПКА.
29. Организация внутреннего контроля выполнения требований по ИБ на объектах КИИ.
30. Практические рекомендации по подготовке к проверкам органов государственного надзора.

5.3. Оценочные средства

Рабочая программа "Обеспечение безопасности 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 9 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	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов	Москва: Юрайт, 2024

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 "Обеспечение безопасности 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.