МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Комплексное обеспечение защиты информации объектов информатизации

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 86,35
самостоятельная работа 30,65
часов на контроль 27

Виды контроля в семестрах:
экзамены 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	14 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	56	56	56	56
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	86,35	86,35	86,35	86,35
Контактная работа	86,35	86,35	86,35	86,35
Сам. работа	30,65	30,65	30,65	30,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель изучения дисциплины студентами – углублённое изучение основ создания КСЗИ на предприятии и методов управления ею.
1.2	Задачи изучения дисциплины студентами:
1.3	уметь применять полученные теоретические и практические знания;
1.4	знать основную терминологию курса, уметь создать проект КСЗИ, обеспечить его внедрение и управлять КСЗИ на этапе её эксплуатации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Защита информации от утечки по техническим каналам
2.1.2	Организационное и правовое обеспечение информационной безопасности
2.1.3	Иностранный язык (английский)
2.1.4	Инженерная и компьютерная графика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Знать:	
Уровень 1	систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации;
Уровень 2	задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
Уровень 3	принципы формирования комплекса мер по защите информации ограниченного доступа объектов информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Уметь:	
Уровень 1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; засекречивать и рассекречивать сведения и их носители;
Уровень 2	использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России; определять комплекс мер для обеспечения защиты информации объектов информатизации;
Уровень 3	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
Владеть:	
Уровень 1	навыком анализа информационной инфраструктуры информационной системы и ее безопасности объектов информатизации; навыками применения основных законов, связанных с организационно-правовым обеспечением информационной безопасности в профессиональной деятельности;
Уровень 2	навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности;
Уровень 3	методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации;

ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	
Знать:	
Уровень 1	основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой

	системы программной документации (ЕСПД); типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации; принципы организации информационных систем в соответствии с требованиями по защите информации; особенности комплексного подхода к обеспечению информационной безопасности организации;
Уровень 2	программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; базовые понятия и определения киберфизической системы, базовые принципы теории управления системами, формирования целей, методов и критериев качества управления, формализованных стратегий основы, понятия и определения информационно-управляющих систем;
Уровень 3	основы теории сетевой организации информационно-вычислительных распределенных систем и компьютерных сетей, архитектуры и иерархии сетевой организации; основы модели знаний, базовые понятия теории формирования баз данных и баз знаний; подходы к построению платформы киберфизической системы как гибридной сетевой среды с интегрированными вычислительными и физическими возможностями
Уметь:	
Уровень 1	применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД); проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
Уровень 2	разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности; анализировать подходы к построению гибридной информационно-управляющей среды, ориентированной на решение широкого класса прикладных задач, в том числе связанных с обеспечением информационной безопасности;
Уровень 3	ставить задачи формирования архитектуры, принципов построения и функционирования киберфизической системы; ставить задачи проведение аналитики киберугроз и оценки уязвимостей и рисков киберфизической системы
Владеть:	
Уровень 1	навыками разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД); навыками использования современных сетевых технологий;
Уровень 2	навыками проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передачи информации;
Уровень 3	методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; навыками применения полученных знаний на практике;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях;
3.1.2	основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементы компьютерного дизайна и
3.1.3	графического отображения объектов в виде чертежей или рисунков;
3.1.4	типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации, классификацию и количественные характеристики технических каналов утечки информации;способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности;организацию защиты информации от утечки по техническим каналам на объектах информатизации;

3.1.5	содержание основных нормативных правовых актов в сфере противодействия коррупции, основы правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации;основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; статус и порядок работы основных правовых информационно-справочных систем; основы организации и деятельности органов государственной власти в Российской Федерации, систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
3.2	**Уметь:**
3.2.1	конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности;
3.2.2	применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), применять методы построения
3.2.3	компьютерных моделей изделий;
3.2.4	проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации, использовать средства инструментального
3.2.5	контроля показателей эффективности технической защиты информации;
3.2.6	соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей, применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных
3.2.7	прав;анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно- распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и
3.2.8	аттестации по требованиям безопасности информации;формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы;формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации,
3.2.9	использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России;
3.3	**Владеть:**
3.3.1	проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа;
3.3.2	разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементарных геометрических построений при помощи средств компьютерной графики; построения двухмерных и трехмерных (3D) изображений изделий;
3.3.3	проектирования системы защиты объекта информатизации от утечек по техническим каналам;
3.3.4	применения основных нормативных правовых актов в сфере противодействия коррупции, работы с нормативными правовыми актами;

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. Понятие и основные направления комплексной системы защиты информации (КСЗИ).						
1.1	Организационная система обеспечения информационной безопасности Российской Федерации. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	

1.2	Организационная система обеспечения информационной безопасности Российской Федерации. /Пр/	8	8	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	1	
1.3	Виды защищаемой информации. Нормативно правовые акты РФ и национальные стандарты РФ в сфере защщиты информации. /Пр/	8	8	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Порядок разработки и внедрения КСЗИ в информационных системах.						
2.1	Понятие КСЗИ. Определение задач, рещение которых необходимо для создания КСЗИ. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
2.2	Принципы организации и этапы разработки КСЗИ. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
2.3	Основные требования и состав документации при проектировании КСЗИ. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
2.4	Понятие КСЗИ. Определение задач, рещение которых необходимо для создания КСЗИ. /Пр/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	1	
2.5	Принципы организации и этапы разработки КСЗИ. /Пр/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	1	
2.6	Основные требования и состав документации при проектировании КСЗИ. /Пр/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
	Раздел 3. Аналитический этап построения КСЗИ.						
3.1	Разработка модели актуальных угроз. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
3.2	Определение компонентов КСЗИ. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
3.3	Определение объктов защиты. Разработка технического паспорта объекта защиты. /Пр/	8	6	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
3.4	Разработка модели угроз безопасности защищаемой информации. /Пр/	8	6	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
3.5	Определение компонентов КСЗИ. /Пр/	8	6	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
	Раздел 4. Практический этап построения КСЗИ.						
4.1	Основные требования к составным частям создаваемой КСЗИ. /Лек/	8	4	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
4.2	Программно-аппаратное, организационное, материально-техническое и кадровое обеспечение функционирования КСЗИ. /Лек/	8	6	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
4.3	Моделирование системы управления КСЗИ /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
4.4	Составление техгического задания на создание или модернизацию КСЗИ. /Пр/	8	4	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
4.5	Разработка локальных документов по ЗИ. /Пр/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
4.6	Определение правовых и организационных мер ЗИ. /Пр/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
4.7	Определение программно-аппаратных и инженерно-технических средств ЗИ. /Пр/	8	4	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	1	
4.8	Проект КСЗИ организации /Ср/	8	30,65	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	

	Раздел 5. Оценка эффективности КСЗИ и управление КСЗИ в процессе эксплуатации.						
5.1	Методы оценки эффективности КСЗИ. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
5.2	Управление КСЗИ в чрезвычайных ситуациях. /Лек/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
5.3	Методы оценки эффективности КСЗИ. /Пр/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
5.4	Управление КСЗИ в чрезвычайных ситуациях. /Пр/	8	2	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	
5.5	Экзамен /ИВКР/	8	2,35	ОПК-6 ОПК-9	Л1.1 Л1.2Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Организационная система обеспечения ИБ в Российской Федерации
1. Какова структура государственной системы обеспечения информационной безопасности?
2. Какие органы власти отвечают за обеспечение информационной безопасности в РФ?
3. Какие функции выполняет ФСТЭК России в сфере ИБ?
4. Как взаимодействуют между собой ФСБ, Минцифры и другие ведомства?
5. Какие меры государственной политики реализуются в области защиты информации?
Тема 2: Виды защищаемой информации. Нормативно-правовая база
6. Какие виды информации требуют специальной защиты?
7. Что такое информация ограниченного доступа и как она классифицируется?
8. Какие нормативные правовые акты регулируют вопросы ИБ в РФ?
9. Каково значение национальных стандартов ГОСТ Р в области защиты информации?
10. Как федеральное законодательство регулирует защиту персональных данных и государственной тайны?
Тема 3: Понятие и задачи комплексной системы защиты информации (КСЗИ)
11. Что понимается под комплексной системой защиты информации?
12. Какие основные цели и задачи решаются при создании КСЗИ?
13. Почему важно интегрировать различные компоненты ИБ в единую систему?
14. Как КСЗИ соотносится с требованиями законодательства и стандартов?
15. Какие риски можно минимизировать с помощью КСЗИ?
Тема 4: Принципы организации и этапы разработки КСЗИ
16. На каких принципах строится организация КСЗИ?
17. Какие этапы включает процесс создания комплексной системы защиты?
18. Какие роли играют технические, программные и административные средства?
19. Какие документы формируются на каждом этапе разработки КСЗИ?
20. Как осуществляется тестирование и внедрение КСЗИ?
Тема 5: Требования к документации при проектировании КСЗИ
21. Какие документы необходимы при проектировании КСЗИ?
22. Что включает политика информационной безопасности организации?
23. Как оформляются процедуры управления доступом и инцидентами?
24. Какие руководящие документы разрабатываются для сотрудников?
25. Как документируется модель угроз и план реагирования?
Тема 6: Объекты защиты и защищаемая информация
26. Как определяются объекты информатизации, требующие защиты?
27. Как классифицируется информация по степени конфиденциальности?
28. Какие данные попадают под категорию «персональные»?
29. Как определяется принадлежность информации к государственной тайне?
30. Какие факторы влияют на выбор уровня защищённости объекта?
Тема 7: Модель актуальных угроз
31. Что такое модель угроз и зачем она нужна?
32. Какие источники угроз учитываются при построении модели?
33. Как оцениваются вероятность и потенциальный ущерб от угроз?
34. Как строится дерево угроз или карта рисков?
35. Как модель угроз влияет на выбор мер защиты?
Тема 8: Компоненты КСЗИ
36. Какие элементы входят в состав комплексной системы защиты информации?
37. Какие технические средства используются для защиты информации?
38. Какие организационные меры обеспечивают безопасность информации?
39. Какие программные решения применяются в КСЗИ?
40. Какие физические меры защиты информации используются?
Тема 9: Обеспечение функционирования КСЗИ

41. Что входит в программно-аппаратное обеспечение КСЗИ?
42. Какие организационные мероприятия обеспечивают устойчивость системы?
43. Какие материально-технические средства используются в КСЗИ?
44. Как обеспечивается кадровое сопровождение системы защиты?
45. Как проводится обучение персонала вопросам информационной безопасности?
Тема 10: Управление КСЗИ
46. Как организуется система управления комплексной защитой информации?
47. Какие метрики используются для оценки состояния системы?
48. Как строится система мониторинга и анализа событий безопасности?
49. Какие механизмы ответственности и контроля внедряются?
50. Как происходит обновление и развитие КСЗИ?
Тема 11: Оценка эффективности КСЗИ
51. Какие методы используются для оценки эффективности КСЗИ?
52. Как рассчитывается уровень защищённости информации?
53. Какие показатели используются при анализе эффективности защиты?
54. Как проводится внутренний и внешний аудит КСЗИ?
55. Какие выводы делаются на основе результатов оценки?
Тема 12: Управление КСЗИ в чрезвычайных ситуациях
56. Какие типы чрезвычайных ситуаций могут повлиять на информационную безопасность?
57. Как организуется система реагирования на инциденты ИБ?
58. Как разрабатывается и внедряется план реагирования на ЧС?
59. Какие действия предпринимаются при утечке информации или атаке?
60. Как восстанавливается работа КСЗИ после ЧС?

5.2. Темы письменных работ

Не предусмотрены

5.3. Оценочные средства

Рабочая программа "Комплексное обеспечение защиты информации объектов информатизации" 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 8 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	Чистов Д. В., Мельников П. П., Золотарюк А. В., Ничепорук Н. Б.	Проектирование информационных систем: учебник и практикум для вузов	Москва: Юрайт, 2024
Л1.2	Золкин А. Л.	Инструментальные средства разработки интеллектуальных информационных систем: учебник для вузов	Санкт-Петербург: Лань, 2025

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Никулин В. В., Олейников А. А., Сорокин А. А., Олейникова А. В.	Разработка серверной части веб-ресурса: учебное пособие для вузов	Санкт-Петербург: Лань, 2023

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	База данных научных электронных журналов "eLibrary"
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
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 "Комплексное обеспечение защиты информации объектов информатизации" 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.