МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Защита информации от утечки по техническим каналам

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
в том числе:
аудиторные занятия 83,35
самостоятельная работа 69,65
часов на контроль 27

Виды контроля в семестрах:
экзамены 7
курсовые работы 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Практические	32	32	32	32
Иные виды контактной работы	3,35	3,35	3,35	3,35
В том числе инт.	8	8	8	8
Итого ауд.	83,35	83,35	83,35	83,35
Контактная работа	83,35	83,35	83,35	83,35
Сам. работа	69,65	69,65	69,65	69,65
Часы на контроль	27	27	27	27
Итого	180	180	180	180

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью дисциплины «Защита информации от утечки по техническим каналам» является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях. Задачами дисциплины является изучение:
1.2	- технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
1.3	- технических каналов утечки акустической (речевой) информации;
1.4	- способов и средств защиты информации, обрабатываемой техническими средствами;
1.5	- способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
1.6	- методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
1.7	- основ организации технической защиты информации на объектах информатизации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Инженерная и компьютерная графика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Комплексное обеспечение защиты информации объектов информатизации
2.2.2	Эксплуатация автоматизированных систем в защищенном исполнении
2.2.3	Контроль безопасности автоматизированных систем

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-8: Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	
Знать:	
Уровень 1	методы и средства измерения физических величин;
Уровень 2	методы обработки экспериментальных данных;
Уровень 3	цели, задачи и основные методы научных исследований при решении задач профессиональной деятельности
Уметь:	
Уровень 1	работать с измерительными приборами; выполнять физический эксперимент, обрабатывать результаты измерений, строить графики и проводить графический анализ опытных данных;
Уровень 2	считать систематические и случайные ошибки прямых и косвенных измерений, приборные ошибки; применять современное физическое оборудование и приборы при решении практических задач;
Уровень 3	использовать стандартные вероятностно-статистические методы анализа экспериментальных данных; обобщать, анализировать и систематизировать научную информацию в области информационной безопасности;
Владеть:	
Уровень 1	навыками организации, планирования, проведения и обработки результатов экспериментов и экспериментальных исследований; навыками проведения физического эксперимента и умения применять конкретное физическое содержание в прикладных задачах будущей специальности;
Уровень 2	навыками проведения расчетов, как при решении задач, так и при научном эксперименте; навыком оформления отчетов по результатам исследований;
Уровень 3	навыками подбора, изучения и обобщения научно- технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

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;

ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	
Знать:	
Уровень 1	риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки; организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы; классификацию и количественные характеристики технических каналов утечки информации;
Уровень 2	способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности; организацию защиты информации от утечки по техническим каналам на объектах информатизации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах;
Уровень 3	способы обеспечения контроля безопасности автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
Уметь:	
Уровень 1	анализировать и оценивать угрозы информационной безопасности автоматизированных систем; осуществлять управление и администрирование защищенных автоматизированных систем;
Уровень 2	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; использовать средства инструментального контроля показателей эффективности технической защиты информации;
Уровень 3	осуществлять планирование, организацию и контроль над безопасностью автоматизированной системы с учетом требований по защите информации; восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;

Владеть:	
Уровень 1	навыками анализа информационной инфраструктуры автоматизированных систем; навыками разработки политик информационной безопасности автоматизированных систем;
Уровень 2	навыками проектирования системы защиты объекта информатизации от утечек по техническим каналам; навыками применения способов обеспечения контроля безопасности автоматизированных систем;
Уровень 3	навыками разработки документов для обеспечения контроля безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности); навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементы компьютерного дизайна и
3.1.2	графического отображения объектов в виде чертежей или рисунков;
3.1.3	принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки;
3.2	**Уметь:**
3.2.1	применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), применять методы построения компьютерных моделей изделий;
3.2.2	разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных систем;
3.3	**Владеть:**
3.3.1	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;
3.3.2	управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем;

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. Технические каналы утечки информации						
1.1	Основные понятия и определения /Лек/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
1.2	Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами /Лек/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
1.3	Технические каналы утечки акустической (речевой) информации /Лек/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
1.4	Методика оценки угроз утечки информации по оптическому каналу /Пр/	7	6	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
1.5	Методика оценки угроз утечки информации по каналу, возникающему за счет побочных электромагнитных излучений и наводок (ПЭМИН) /Пр/	7	6	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
1.6	Методика оценки угроз утечки акустической (речевой) информации /Пр/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
1.7	Технические средства разведки и перехвата информации /Пр/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	

1.8	Моделирование защищаемого объекта. Проектирование системы защиты информации объекта информатизации /Пр/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
1.9	Исследование звукоизоляции и виброизоляции защищаемого помещения /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
1.10	Побочные электромагнитные излучения средств вычислительной техники /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
1.11	Побочные электромагнитные наводки от средств вычислительной техники в линейных коммуникациях /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
	Раздел 2. Способы и средства защиты информации от утечки по техническим каналам						
2.1	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами /Лек/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
2.2	Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам /Лек/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
2.3	Средства защиты информации от утечки по каналу, возникающему за счет ПЭМИН /Пр/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
2.4	Средства защиты информации от акустической речевой разведки (АРР) /Пр/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
2.5	Виброакустическая защита речевой информации /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
2.6	Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
2.7	Защита от побочных электромагнитных наводок в линейных коммуникациях /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
2.8	Подготовка к практическим занятиям, оформление результатов /Ср/	7	30,25	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
	Раздел 3. Методы и средства контроля эффективности технической защиты информации						
3.1	Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами /Лек/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
3.2	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам /Лек/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
3.3	Методы и средства выявления электронных устройств негласного получения информации /Лек/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	

3.4	Средства обнаружения технических каналов утечки информации /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
3.5	Подготовка к лабораторным работам, оформление результатов /Ср/	7	39,4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
	Раздел 4. Организация технической защиты информации						
4.1	Организация технической защиты информации на объектах информатизации /Лек/	7	4	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
4.2	Нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации от утечек по техническим каналам /Лаб/	7	2	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	1	
4.3	Курсовая работа /КР/	7	27	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	
4.4	Экзамен /ИВКР/	7	3,35	ОПК-9 ОПК-13 ОПК-8	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Основные понятия и определения
1. Что такое техническая защита информации (ТЗИ)?
2. Какие виды утечки информации существуют?
3. Что понимается под техническим каналом утечки информации?
4. Какие объекты информатизации требуют технической защиты?
5. Каково значение ТЗИ в системе комплексной защиты информации?
Тема 2: Технические каналы утечки информации в СВТ и АС
6. Какие основные технические каналы утечки информации существуют в средствах вычислительной техники?
7. Что такое побочные электромагнитные излучения и как они возникают?
8. Как информация может утекать через линии питания и заземления?
9. Как происходит утечка информации через кабельные линии связи?
10. Какие угрозы связаны с использованием периферийных устройств?
Тема 3: Технические каналы утечки акустической (речевой) информации
11. Какие пути утечки речевой информации существуют в помещениях?
12. Что такое акустическое излучение оборудования и его роль в утечке данных?
13. Как происходит передача речи через стены, окна, вентиляцию?
14. Какие технические средства могут быть использованы для перехвата речи?
15. В чём особенность утечки речевой информации через системы видеонаблюдения?
Тема 4: Способы и средства защиты информации в СВТ и АС
16. Какие меры применяются для снижения уровня побочных электромагнитных излучений?
17. Что такое экранирование и как оно используется в ТЗИ?
18. Как осуществляется фильтрация сигналов на входах/выходах?
19. Как используются программно-аппаратные комплексы для защиты информации?
20. Что такое "чистые сигналы" и их применение в защите информации?
Тема 5: Защита выделенных помещений от утечки речевой информации
21. Какие помещения считаются выделенными в контексте ТЗИ?
22. Какие меры принимаются для защиты от акустических утечек в выделенных помещениях?
23. Как обеспечивается звукоизоляция стен, потолков, полов?
24. Что такое активное шумоподавление и как оно используется?
25. Как организуется защита от наведённых вибраций через оконные конструкции?
Тема 6: Методы и средства контроля эффективности технической защиты информации
26. Какие параметры используются для оценки эффективности ТЗИ?
27. Как проводится измерение уровня побочных излучений?
28. Какие приборы используются для диагностики электромагнитной обстановки?
29. Как оценивается уровень звукоизоляции помещений?
30. Как строится система постоянного мониторинга защищённости информации?
Тема 7: Контроль эффективности защиты помещений от утечки речевой информации
31. Какие нормативные документы регламентируют требования к защите речевой информации?
32. Как измеряется коэффициент звукоизоляции ограждающих конструкций?
33. Как проводится тестирование на наличие виброакустических утечек?
34. Какие методики используются для проверки герметичности вентиляционных систем?

35. Как оценивается эффективность средств активной борьбы с прослушиванием?
Тема 8: Методы и средства выявления электронных устройств негласного получения информации
36. Какие типы закладных устройств существуют?
37. Как проводится радиопоиск скрытых микрофонов и жучков?
38. Как используются тепловизоры и металлоискатели для поиска устройств?
39. Как анализируется сетевое оборудование на наличие несанкционированных подключений?
40. Какие программные средства применяются для обнаружения скрытых камер и микрофонов?
Тема 9: Организация технической защиты информации на объектах информатизации
41. Как разрабатывается комплексная система технической защиты информации?
42. Какие этапы включает проектирование системы ТЗИ?
43. Какие требования предъявляются к защищённым рабочим местам?
44. Как организуется взаимодействие ТЗИ с другими системами безопасности?
45. Как обеспечивается соответствие объекта требованиям ФСТЭК России?

5.2. Темы письменных работ

Темы, связанные с акустической утечкой информации
1. Исследование акустических утечек через оконные конструкции и методы их предотвращения.
2. Разработка программного обеспечения для анализа акустического поля в помещении.
3. Влияние вентиляционных систем на дальность распространения речевой информации.
4. Оценка эффективности активного шумоподавления в условиях реального офиса.
5. Анализ возможностей передачи речи через стены и перекрытия зданий.
Темы, связанные с защитой информации в СВТ и АС
6. Экранирование кабельных линий как мера защиты от побочных электромагнитных излучений.
7. Применение фильтров подавления наводок в сетях Ethernet для предотвращения утечки данных.
8. Анализ эффективности использования "чистых сигналов" в защищённых компьютерных системах.
9. Современные средства диагностики уровня побочных излучений в офисной технике.
10. Методы снижения уровня наведённых сигналов в цепях питания вычислительной техники.
Темы, связанные с защитой выделенных помещений от утечки речевой информации
11. Проектирование защищённого помещения класса А по требованиям ФСТЭК России.
12. Использование многослойных конструкций стен для повышения звукоизоляции.
13. Особенности проектирования герметичных вентиляционных систем в защищённых помещениях.
14. Сравнительный анализ различных типов звукоизолирующих окон.
15. Оценка влияния внутренней отделки помещения на уровень акустической утечки.
Темы, связанные с контролем эффективности ТЗИ в СВТ и АС
16. Разработка методики тестирования фильтрующих устройств в реальных условиях.
17. Измерение уровня побочных электромагнитных излучений от ПК и серверов.
18. Создание системы автоматического мониторинга электромагнитной обстановки.
19. Анализ соответствия используемых средств ТЗИ современным нормативным документам.
20. Оценка эффективности экранированных кабелей при передаче конфиденциальной информации.
Темы, связанные с контролем эффективности защиты помещений от утечки речевой информации
21. Измерение коэффициента звукоизоляции строительных материалов в лабораторных условиях.
22. Методы проверки герметичности дверных проёмов в защищённых помещениях.
23. Использование инфракрасной термографии для поиска источников виброакустических утечек.
24. Разработка программного комплекса для расчёта акустических характеристик помещения.
25. Оценка эффективности использования пористых материалов в борьбе с акустическими утечками.
Темы, связанные с обнаружением закладных устройств
26. Сравнительный анализ приборов радиопоиска скрытых микрофонов и камер.
27. Обнаружение GSM-закладок с использованием программно-определяемого радио (SDR).
28. Методы обнаружения несанкционированных подключений к телефонным линиям.
29. Использование тепловизионных систем для выявления спрятанных электронных устройств.
30. Разработка мобильного приложения для анализа беспроводного эфира в офисе.

5.3. Оценочные средства

Рабочая программа "Защита информации от утечки по техническим каналам" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 7 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Васильева И. Н.	Криптографические методы защиты информации: учебник и практикум для вузов	Москва: Юрайт, 2023
Л1.2	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: учебник для вузов	Москва: Юрайт, 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	

4-48	Лаборатория технической защиты информации № 4-48	Лабораторные столы; Стулья; Магнитно-маркерная доска; Специализированное оборудование по защите информации от утечки по техническим каналам, техническими средствами контроля эффективности защиты информации от утечки по техническим каналам в составе: Генераторы высокочастотных сигналов; Измерительные приемники; Измерительные антены. Учебный лабораторный комплекс для обеспечения исследований ПЭМИ СВТ; Учебный лабораторный комплекс для обеспечения исследований типовых средств электрических и электромагнитных измерений и вспомогательного оборудования Стенды с образцами фильтрующих и поглощающих свойств материалов для защиты информации от электрических воздействий Стенды разъясняющие способы защиты информации от специальных электромагнитных и электрических воздействий Учебный лабораторный комплекс для проведения аттестационных испытаний объектов информатизации на соответствие требованиям по защите информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок Учебный лабораторный комплекс для обеспечения исследований акустоэлектрических каналов утечки информации Учебный лабораторный комплекс для обеспечения исследований систем пространственного и линейного электромагнитного зашумления Учебный Лабораторный комплекс для обеспечения исследований характеристик помехоподавляющих фильтров Учебный лабораторный комплекс для обеспечения исследований характеристик средств защиты ОТСС и ВТСС от утечки информации по техническим каналам Учебный лабораторный комплекс для обеспечения	Лаб

		исследований типовых сертифицированных технических и программно-технических средств защиты информации от утечки по техническим каналам Учебный лабораторный комплекс для демонстрации способов защиты информации от утечки по техническим каналам Учебный лабораторный комплекс для обеспечения исследований акустических и вибрационных каналов утечки информации Учебный лабораторный комплекс для обеспечения исследований типовых средств виброакустических измерений и вспомогательного оборудования Учебный лабораторный комплекс для обеспечения исследований характеристик систем вибрационной защиты Учебный лабораторный комплекс для проведения акустических и вибрационных измерений.	
3-79	Аудитория (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну № 3-79	рулонные шторы; система виброакустической защиты информации; столы аудиторные для обучающихся, стол преподавателя и стол для размещения компьютера; стулья, доска маркерная; экран; компьютер (в исполнении - моноблок со встроенным или подключаемым DVD/CD-дисководом); проектор; кондиционер; экраны на батареи.	
3-79 А	Специальная библиотека (библиотека литературы ограниченного доступа), предназначенная для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа № 3-79 А	рулонная штора; стол письменный; стул; шкаф металлический (двудверный) для хранения ДСП материалов; шкаф металлический для хранения мобильных телефонов типа ШСТ-26; экраны на батареи.	

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 "Защита информации от утечки по техническим каналам" 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.