Документ подписан простой электронной подписью
Информация о владельце:
ФИО: ПАНОВ Юрий Петрович
Должность: Ректор
Дата подписания: 09.06.2025 11:34:26
Уникальный программный ключ:
e30ba4f0895d1683ed43800960e77389e6cbff62

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Измерительная аппаратура контроля защищенности 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	3 ЗЕТ		
Часов по учебному плану	108	Виды контроля в семестрах:	
в том числе:		зачеты 9	
аудиторные занятия	48,25		
самостоятельная работа	59,75		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	9 (5.1)		Итого	
	уп	рп	уп	рп
Неделя	16			
Вид занятий	уп	рп	уп	рп
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	48,25	48,25	48,25	48,25
Контактная работа	48,25	48,25	48,25	48,25
Сам. работа	59,75	59,75	59,75	59,75
Итого	108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является подготовка специалистов в области технической защиты информации и привитие навыков контроля работоспособности и эффективности применяемых технических средств защиты информации.
1.2	Задачи дисциплины:
1.3	Изучение:
1.4	- измерительной аппаратуры контроля защищённости технических каналов утечки информации;
1.5	- методов контроля защищенности объектов информатизации;
1.6	- методов анализа технических каналов утечки информации проектируемых и эксплуатируемых объектов информатизации;
1.7	Формирование у студентов навыков:
1.8	- использования измерительной аппаратуры контроля защищенности объектов информатизации;
1.9	- использования поисковой аппаратуры для обнаружения каналов передачи различных подслушивающих устройств.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
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)

ОПК-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

Знать:

Уровень 1	методы администрирования вычислительных сетей; методы администрирования и принципы работы операционных систем семейств UNIX и Windows; принципы формирования политики информационной безопасности в автоматизированных системах; методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы;
Уровень 2	средства обеспечения безопасности данных; основные угрозы безопасности информации и модели нарушителя объекта информатизации; цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью; принципы формирования политики информационной безопасности объекта информатизации;
Уровень 3	методы и средства контроля защищенности объектов информатизации; узлы автоматизированной системы для измерения параметров информативных сигналов технических средств обработки информации; измерительную аппаратуру, применяемую для контроля защищенности объектов информатизации;

Уметь:

Уровень 1	администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети; настраивать политику безопасности операционных систем семейств UNIX и Windows; разрабатывать частные политики информационной безопасности автоматизированных систем;
Уровень 2	осуществлять диагностику и мониторинг систем защиты автоматизированных систем; администрировать базы данных; разрабатывать модели угроз и модели нарушителя объекта информатизации;
Уровень 3	оценивать информационные риски объекта информатизации; разрабатывать порядок проведения измерений параметров информативных сигналов технических средств обработки информации; обрабатывать и интерпретировать результаты измерений параметров информативных сигналов технических средств обработки информации;

Владеть:

Уровень 1	навыками администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности; навыками администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; навыками управления процессами обеспечения безопасности автоматизированных систем;
Уровень 2	навыками администрирования баз данных с учетом требований по обеспечению информационной

	безопасности; навыками эксплуатации измерительной аппаратуры контроля защищенности объектов информатизации с учетом требований по обеспечению информационной безопасности;
Уровень 3	навыками применения методов математической обработки результатов измерений параметров информативных сигналов технических средств обработки информации; навыками экспертизы состояния защищенности информации на объектах информатизации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
3.1.1	принципы формирования политики информационной безопасности в автоматизированных системах, риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки;
3.1.2	методы проектирования вычислительных сетей, методы администрирования вычислительных сетей;
3.1.3	методы администрирования и принципы работы операционных систем семейств UNIX и Windows, устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows;
3.1.4	методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы, организационную структуру и функциональную
3.1.5	часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы;
3.1.6	назначение, функции и структуру систем управления базами данных, средства обеспечения безопасности данных;
3.1.7	основные документы по стандартизации в сфере управления ИБ; принципы формирования политики информационной безопасности в автоматизированных системах; требования информационной безопасности при эксплуатации автоматизированной системы, основные угрозы безопасности информации и модели нарушителя объекта информатизации;
3.1.8	цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью; принципы
3.1.9	формирования политики информационной безопасности объекта информатизации;
3.2	Уметь:
3.2.1	разрабатывать частные политики информационной безопасности автоматизированных систем, анализировать и оценивать угрозы информационной безопасности автоматизированных систем;
3.2.2	проектировать вычислительные сети, администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети;
3.2.3	настраивать политику безопасности операционных систем семейств UNIX и Windows, использовать средства управления работой операционной системы; формулировать политику безопасности операционных систем семейств UNIX и Windows;
3.2.4	осуществлять диагностику и мониторинг систем защиты автоматизированных систем, осуществлять управление и администрирование защищенных автоматизированных систем;
3.2.5	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
3.2.6	эксплуатировать базы данных; создавать объекты базы данных; выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами
3.2.7	данных, администрировать базы данных;
3.2.8	формировать политики информационной безопасности организации; выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности
3.2.9	автоматизированной системы, разрабатывать модели угроз и модели нарушителя объекта информатизации; оценивать информационные риски объекта информатизации;
3.3	Владеть:
3.3.1	управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем;
3.3.2	эксплуатации локальных вычислительных сетей, администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности; администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности, установки операционных систем семейств Windows и Unix;
3.3.3	разработки политик информационной безопасности автоматизированных систем;
3.3.4	эксплуатации баз данных с учетом требований по обеспечению информационной безопасности, администрирования баз данных с учетом требований по обеспечению информационной безопасности;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
-------------	---	----------------	-------	-------------	------------	------------	------------

	Раздел 1. Введение						
1.1	Введение /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
1.2	Введение /Ср/	9	7	ОПК-15	Л1.1 Л1.2	0	
	Раздел 2. Измерительная аппаратура контроля защищённости технических каналов утечки информации						
2.1	Технические каналы утечки информации /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
2.2	Акустический канал утечки информации /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
2.3	Виброакустический канал утечки информации /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
2.4	Канал утечки за счет побочных электромагнитных излучений и наводок /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
2.5	Обзор измерительной аппаратуры контроля защищенности объектов информатизации /Ср/	9	7,1	ОПК-15	Л1.1 Л1.2	0	
2.6	Технические каналы утечки информации /Ср/	9	7,2	ОПК-15	Л1.1 Л1.2	0	
	Раздел 3. Средства защиты информации и демаскирующие признаки устройств негласного съема информации						
3.1	Альтернативные измерительные площадки /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
3.2	Демаскирующие признаки устройств негласного съема информации /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
3.3	Пассивные средства защиты информации /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
3.4	Активные средства защиты информации. /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
3.5	Поиск устройств негласного съема информации /Лаб/	9	2	ОПК-15	Л1.1 Л1.2	1	
3.6	Активные средства защиты информации /Лаб/	9	2	ОПК-15	Л1.1 Л1.2	1	
3.7	Демаскирующие признаки устройств негласного съема информации /Ср/	9	7,2	ОПК-15	Л1.1 Л1.2	0	
3.8	Канал утечки за счет побочных электромагнитных излучений и наводок /Ср/	9	9,75	ОПК-15	Л1.1 Л1.2	0	
	Раздел 4. Методики проведения акустического, виброакустического и за счет ПЭМИН контроля защищенности объектов информатизации						
4.1	Обзор измерительной аппаратуры контроля защищенности объектов информатизации /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
4.2	Методика проведения акустического и виброакустического контроля защищенности объектов информатизации /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
4.3	Методика проведения контроля защищенности объектов информатизации за счет обнаружения побочных электромагнитных излучений и наводок /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
4.4	Поисковые мероприятия с помощью нелинейного локатора /Лаб/	9	2	ОПК-15	Л1.1 Л1.2	1	

4.5	Виброакустический канал утечки информации /Ср/	9	7,4	ОПК-15	Л1.1 Л1.2	0	
Раздел 5. Поисковые комплексы контроля защищённости объектов информатизации							
5.1	Изучение комплекса «Навигатор» /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
5.2	Изучение комплекса «Спрут-мини» /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
5.3	Изучение комплекса «Пиранья» /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
5.4	Поверка измерительной аппаратуры /Лек/	9	2	ОПК-15	Л1.1 Л1.2	0	
5.5	Проведение акустического и виброакустического контроля защищённости объектов информатизации с помощью комплекса «Спрут-мини» /Лаб/	9	4	ОПК-15	Л1.1 Л1.2	0	
5.6	Проведение контроля защищённости объектов информатизации за счет обнаружения побочных электромагнитных излучений и наводок с помощью комплекса «Навигатор» /Лаб/	9	4	ОПК-15	Л1.1 Л1.2	1	
5.7	Поисковые мероприятия с помощью комплекса «Пиранья» /Лаб/	9	2	ОПК-15	Л1.1 Л1.2	0	
5.8	Акустический канал утечки информации /Ср/	9	7	ОПК-15	Л1.1 Л1.2	0	
5.9	Методика проведения акустического и виброакустического контроля защищённости объектов информатизации /Ср/	9	7,1	ОПК-15	Л1.1 Л1.2	0	
5.10	Зачет /ИВКР/	9	0,25	ОПК-15	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Введение

1. Что такое техническая защита информации (ТЗИ) и почему она важна?
2. Какие виды утечки информации выделяются в рамках ТЗИ?
3. Какова роль ТЗИ в системе комплексной безопасности?
4. Какие основные задачи решает техническая разведка и контрразведка?
5. Какие категории объектов требуют обеспечения технической защищённости?

Тема 2: Технические каналы утечки информации

6. Что понимается под техническим каналом утечки информации?
7. Какие типы технических каналов утечки информации существуют?
8. Как происходит утечка информации через линии связи и электропитания?
9. Какие угрозы связаны с использованием периферийного оборудования?
10. Как классифицируются каналы утечки информации по физическим факторам?

Тема 3: Акустический канал утечки информации

11. Как осуществляется утечка речевой информации через воздушную среду?
12. Как звуковые волны могут быть преобразованы в сигнал для передачи информации?
13. Какие технические устройства могут использоваться для перехвата акустической информации?
14. Как влияет акустика помещения на вероятность утечки?
15. Какие меры применяются для противодействия прослушиванию через акустические каналы?

Тема 4: Виброакустический канал утечки информации

16. Что такое виброакустическая утечка информации?
17. Как звуковая волна может вызывать механические колебания стекла и стен?
18. Какие устройства используются для считывания вибраций с оконных стёкол?
19. Как обнаружить наличие виброакустического канала утечки?
20. Какие методы борьбы с виброакустическими утечками применяются на практике?

Тема 5: Канал утечки за счёт ПЭМИН

21. Что означает аббревиатура ПЭМИН?
22. Как возникают побочные электромагнитные излучения и наводки?
23. Как информация может утекать через электромагнитное поле вокруг оборудования?
24. Какие компоненты ЭВМ наиболее уязвимы с точки зрения ПЭМИН?
25. Как проводится диагностика уровня ПЭМИН на реальных объектах?

Тема 6: Альтернативные измерительные площадки

26. Что такое альтернативная измерительная площадка?
27. Какие требования предъявляются к таким площадкам?
28. Как проводятся испытания средств вычислительной техники на ПЭМИН?
29. Какие параметры измеряются на альтернативной площадке?
30. Какие стандарты регламентируют проведение испытаний?

Тема 7: Демаскирующие признаки устройств негласного съёма информации

31. Что такое демаскирующий признак закладного устройства?
32. Какие виды демаскирующих признаков существуют?
33. Как обнаружить скрытое устройство по его электромагнитному излучению?
34. Как тепловые, оптические и акустические признаки помогают в поиске закладок?
35. Какие современные технологии повышают скрытность закладных устройств?

Тема 8: Пассивные средства защиты информации

36. Что относится к пассивным средствам ТЗИ?
37. Как работает экранирование помещений и кабельных трасс?
38. Какие материалы используются для снижения уровня ПЭМИН?
39. Как звукоизоляция используется как пассивная защита от прослушивания?
40. Какие преимущества и недостатки у пассивных методов защиты?

Тема 9: Активные средства защиты информации

41. Что такое активные средства защиты информации?
42. Как работают генераторы шума для подавления акустических утечек?
43. Какие системы используются для создания помех ПЭМИН?
44. Как реализуется система активного шумоподавления в помещениях?
45. Какие технические характеристики имеют современные активные средства защиты?

Тема 10: Обзор измерительной аппаратуры

46. Какие цели преследует использование измерительной аппаратуры при контроле защищённости?
47. Какие приборы используются для анализа ПЭМИН?
48. Какие устройства применяются для поиска радиозакладок?
49. Как работает тепловизор в задачах обнаружения электронных устройств?
50. Какие функции выполняет комплекс технического осмотра помещений?

Тема 11: Методика акустического и виброакустического контроля

51. Как проводится акустический контроль защищённости помещения?
52. Какие инструменты используются для виброакустического тестирования?
53. Как определяется чувствительность оконных конструкций к вибрациям?
54. Какие параметры регистрируются при проведении тестирования?
55. Как интерпретируются результаты измерений?

Тема 12: Методика контроля за счётём ПЭМИН

56. Как проводится анализ уровня побочных электромагнитных излучений?
57. Какие этапы включает методика контроля ПЭМИН?
58. Какие антенны и измерительные приборы используются?
59. Как определяется уровень допустимых излучений?
60. Как оформляются результаты контроля и даётся оценка защищённости?

Тема 13: Изучение комплексов «Навигатор», «Спрут-Мини», «Пиранья»

61. Каково назначение и состав комплекса «Навигатор»?
62. Какие функции выполняет аппаратно-программный комплекс «Спрут-Мини»?
63. В чём особенности работы с комплексом «Пиранья»?
64. Как эти комплексы используются при проведении технического обследования?
65. Какие измерительные возможности предоставляют данные комплексы?

Тема 14: Поверка измерительной аппаратуры

66. Что такое поверка средств измерений и зачем она нужна?
67. Какие организации проводят поверку измерительной аппаратуры?
68. Как часто необходимо проводить поверку приборов ТЗИ?
69. Какие документы оформляются после успешной поверки?
70. Как влияет отсутствие поверки на достоверность результатов измерений?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Измерительная аппаратура контроля защищенности 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 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
Л1.2	Краковский Ю. М.	Методы и средства защиты информации: 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	
---	--	---	--

4-48	<p>Специализированная многофункциональная учебная лаборатория № 4-48 для проведения лабораторных и практических занятий</p>	<p>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 антенны. 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</p>	Лаб
------	---	---	-----

		<p>ВТСС от утечки информации по техническим каналам</p> <p>Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных технических и программно-технических средств защиты информации от утечки по техническим каналам</p> <p>Учебный лабораторный комплекс для демонстрации способов защиты информации от утечки по техническим каналам</p> <p>Учебный лабораторный комплекс для обеспечения исследований акустических и вибрационных каналов утечки информации</p> <p>Учебный лабораторный комплекс для обеспечения исследований типовых средств виброакустических измерений и вспомогательного оборудования</p> <p>Учебный лабораторный комплекс для обеспечения исследований характеристик систем вибрационной защиты</p> <p>Учебный лабораторный комплекс для проведения акустических и вибрационных измерений.</p>	
--	--	---	--

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 "Измерительная аппаратура контроля защищенности 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.