МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Основы аттестации объектов информатизации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план b090302_25_BIS25.plx
09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 0
в том числе:
аудиторные занятия 0
самостоятельная работа 0

Виды контроля в семестрах:

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	48	32	48
Иные виды контактной работы	2,35	2,35	2,35	2,35
Итого ауд.	66,35	82,35	66,35	82,35
Контактная работа	66,35	82,35	66,35	82,35
Сам. работа	50,65	34,65	50,65	34,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель - освоение технологий аттестации объектов информатизации критически важных объектов.
1.2	Задачи:
1.3	-освоение базовых понятий в области аттестации объектов информатизации критически важных объектов;
1.4	-изучение нормативной правовой базы аттестации объектов информатизации критически важных объектов;
1.5	-знакомство с организационной структурой аттестации объектов информатизации;
1.6	-поэтапное освоение методики аттестации объектов информатизации; изучение системы документационного обеспечения аттестации объектов информатизации;
1.7	-освоение специфики аттестации объектов информатизации критически важных объектов.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Организационное и правовое обеспечение информационной безопасности
2.1.2	Управление информационной безопасностью
2.1.3	Экономика
2.1.4	Разработка и эксплуатация автоматизированных систем в защищенном исполнении
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Технология подготовки выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-3.3: Способен проводить тестирование ПО по разработанным тестовым случаям
Знать:
Уметь:
Владеть:

ПК-9.3: Разработка технического задания на Систему
Знать:
Уметь:
Владеть:

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основы построения, расчета и анализа современной системы показателей, характеризующих деятельность хозяйствующих субъектов на микроуровне, подходы к классификации факторов внешней среды организации и их влияние на деятельность организации;
3.1.2	основные документы по стандартизации в сфере управления ИБ;
3.1.3	принципы формирования политики информационной безопасности в автоматизированных системах;требования информационной безопасности при эксплуатации автоматизированной системы, основные угрозы безопасности информации и модели нарушителя объекта информатизации;
3.1.4	цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью;
3.1.5	принципы формирования политики информационной безопасности объекта информатизации;
3.1.6	критерии оценки защищенности автоматизированной системы;основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, основные меры по защите информации в автоматизированных системах;
3.1.7	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем;
3.1.8	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;
3.1.9	основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации;

3.1.10	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;
3.1.11	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;
3.1.12	статус и порядок работы основных правовых информационно-справочных систем;
3.1.13	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;
3.1.14	систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации;
3.1.15	задачи органов защиты государственной тайны и служб защиты информации на предприятиях
3.2	**Уметь:**
3.2.1	осуществлять расчет себестоимости продукции;
3.2.2	рассчитывать влияние факторов на различные виды расходов;
3.2.3	осуществлять расчет потребности в инвестициях, формулировать управленческие решения по результатам анализа внешней и внутренней среды организации;
3.2.4	формировать политики информационной безопасности организации;
3.2.5	выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, разрабатывать модели угроз и модели нарушителя объекта информатизации; оценивать информационные риски объекта информатизации;
3.2.6	контролировать уровень защищенности в автоматизированных системах, настраивать программное обеспечение системы защиты информации автоматизированной системы;
3.2.7	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;
3.2.8	обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;
3.2.9	анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;
3.2.10	формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;
3.2.11	формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы;
3.2.12	формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации, использовать систему организационных мер, направленных на защиту информации
3.2.13	ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России
3.3	**Владеть:**
3.3.1	владения методами распределения накладных затрат и оценки эффективности проектных решений, методами оценки экономической эффективности результатов хозяйственной деятельности различных субъектов экономической системы;
3.3.2	анализа событий, связанных с защитой информации в автоматизированных системах, выявления и анализа уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации;
3.3.3	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. Аттестация объектов информатизации критически важных объектов: базовые понятия, общая характеристика						
1.1	Базовые понятия аттестации объектов информатизации КВО /Лек/	7	4		Л1.2 Л1.1	0	

1.2	Общая характеристика процесса аттестации ОИ КВО /Лек/	7	2		Л1.2 Л1.1	0	
	Раздел 2. Нормативная правовая база по аттестации объектов информатизации, в том числе - критически важных объектов						
2.1	Нормативная правовая база по аттестации объектов информатизации /Лек/	7	4		Л1.2 Л1.1	0	
2.2	Нормативная правовая база по аттестации объектов информатизации критически важных объектов /Лек/	7	2		Л1.2 Л1.1	0	
	Раздел 3. Организационная структура аттестации объектов информатизации в России						
3.1	Организационная структура аттестации ОИ: общая характеристика /Лек/	7	2		Л1.2 Л1.1	0	
3.2	Организационная структура системы аттестации ОИ в РФ: характеристика отдельных подсистем /Лек/	7	2		Л1.2 Л1.1	0	
	Раздел 4. Этапы аттестации объектов информатизации критически важных объектов и их реализация						
4.1	Этапы аттестации ОИ КВО: общая характеристика /Лек/	7	2		Л1.2 Л1.1	0	
4.2	Подача заявки на рассмотрение и проведение аттестации.Анализ исходных данных по аттестуемому объекту информатизации. Проведение предварительного специального обследования аттестуемогообъекта информатизации. Разработка программы и методики аттестационных испытаний. Заключение договоров на аттестацию. Испытание несертифицированных средств и систем защиты информации,используемых на аттестуемом объекте /Лек/	7	2		Л1.2 Л1.1	0	
4.3	Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации.Проведение аттестационных испытаний ОИ. Оформление, регистрация и выдача «Аттестата соответствия». Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных ОИ. Рассмотрение апелляций. /Лек/	7	2		Л1.2 Л1.1	0	
4.4	Подача заявки на рассмотрение и проведение аттестации. Анализ исходных данных по аттестуемому объекту информатизации. /Пр/	7	8		Л1.2 Л1.1	0	

4.5	Проведение предварительного специального обследования аттестуемого объекта информатизации. Разработка программы и методики аттестационных испытаний /Пр/	7	8		Л1.2 Л1.1	0	
4.6	Заключение договоров на аттестацию. Испытание несертифицированных средств и систем защиты информации,используемых на аттестуемом объекте. /Пр/	7	6		Л1.2 Л1.1	0	
4.7	Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации. /Пр/	7	6		Л1.2 Л1.1	0	
4.8	Проведение аттестационных испытаний объекта информатизации. /Пр/	7	4		Л1.2 Л1.1	0	
4.9	Оформление, регистрация и выдача «Аттестата соответствия» /Пр/	7	4		Л1.2 Л1.1	0	
4.10	Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации. Рассмотрение апелляций. /Пр/	7	2		Л1.2 Л1.1	0	
	Раздел 5. Документационное сопровождение аттестации объектов информатизации критически важных объектов						
5.1	Система документационного соспровождения аттестации ОИ КВО: общая характеристика /Лек/	7	4		Л1.2 Л1.1	0	
5.2	Заключение аттестационной проверки,Протокол аттестационных испытаний, «Аттестат соответствия» на объект информатизации, отвечающий требованиямпо безопасности информации:Структура, содержание. /Лек/	7	4		Л1.2 Л1.1	0	
5.3	Специфика процедуры аттестации ОИ КВО /Лек/	7	2		Л1.2 Л1.1	0	
5.4	Заключение аттестационной проверки: структура, содержание /Пр/	7	4		Л1.2 Л1.1	0	
5.5	Протокол аттестационного испытания /Пр/	7	4		Л1.2 Л1.1	0	
5.6	Аттестат соответствия ОИ КВО требованиям безопасности /Пр/	7	2		Л1.2 Л1.1	0	
5.7	Разработка базы данных "Система документации по аттестации ОИ" /Ср/	7	34,65		Л1.2 Л1.1	0	
5.8	Экзамен /ИВКР/	7	2,35		Л1.2 Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Базовые понятия аттестации ОИ КВО

1. Что такое объект информатизации (ОИ)? Какие его характеристики определяют необходимость аттестации?
2. Каково определение критически важного объекта (КВО)? Приведите примеры КВО в России.
3. Какие цели и задачи аттестации ОИ КВО? Как она связана с обеспечением информационной безопасности?
4. Какие ключевые термины и понятия используются в аттестации ОИ (например, «аттестат соответствия», «специальные проверки»)?

5. Как связаны аттестация ОИ и сертификация средств защиты информации (СЗИ)?
Тема: 2. Общая характеристика процесса аттестации
6. Какие этапы включает процесс аттестации ОИ КВО? Какие документы оформляются на каждом этапе?
7. Какие роли участвуют в процессе аттестации (заказчик, аттестационная комиссия, ФСТЭК РФ)?
8. Какие параметры системы оцениваются при аттестации (конфиденциальность, целостность, доступность)?
9. Какие последствия наступают при несоответствии ОИ установленным требованиям ИБ?
10. Как аттестация ОИ КВО влияет на допуск к работе с защищенными данными?
Тема: 3. Нормативно-правовая база аттестации
11. Какие нормативные документы регулируют аттестацию ОИ КВО (ФЗ-187, ФЗ-149, указы Президента РФ)?
12. Какие требования к аттестации ОИ установлены в ГОСТ Р 57580-2017 и других стандартах?
13. Как уголовное и административное законодательство РФ связано с нарушением требований аттестации (например, ст. 272.1, ст. 13.11 КоАП)?
14. Как международные стандарты (например, ISO/IEC 15408, NIST SP 800-171) соотносятся с российскими нормами аттестации?
15. Какие изменения в законодательстве РФ за последние 5 лет затронули процесс аттестации ОИ КВО?
Тема: 4. Организационная структура аттестации
16. Какова роль ФСТЭК России в системе аттестации объектов информатизации?
17. Как организованы аттестационные комиссии? Какие этапы их работы?
18. Как взаимодействуют Минцифры РФ, ФСБ и Роскомнадзор в процессе аттестации?
19. Какие функции выполняют аккредитованные испытательные лаборатории (ЦЛС) в аттестации ОИ?
20. Как организуется инспекционный контроль за эксплуатацией аттестованных ОИ?
Тема: 5. Этапы аттестации ОИ КВО
21. Какие этапы включает процесс аттестации ОИ КВО (подготовка, обследование, испытания, оформление аттестата)?
22. Как подается заявка на аттестацию? Какие документы обязательны?
23. Как проводится предварительное специальное обследование ОИ? Какие параметры оцениваются?
24. Как разрабатывается программа и методика аттестационных испытаний (ПМИ)?
25. Какие критерии учитываются при выборе специалистов для проведения аттестации?
Тема: 6. Проверки и испытания на соответствие требованиям ИБ
26. Какие виды специальных проверок проводятся для выявления устройств перехвата информации?
27. Как организуются аттестационные испытания несертифицированных СЗИ, применяемых на ОИ КВО?
28. Какие методы используются для оценки эффективности средств защиты информации?
29. Какие параметры тестируются при проверке систем контроля доступа и шифрования данных?
30. Как анализируется устойчивость ОИ к атакам с использованием методик MITRE ATT&CK?
Тема: 7. Документационное сопровождение аттестации
31. Как оформляется протокол аттестационных испытаний? Какие разделы обязательны?
32. Какие данные включает «Аттестат соответствия»? Какие сроки его действия?
33. Как происходит регистрация и выдача аттестата? Какие органы уполномочены на это?
34. Какие ошибки чаще всего допускаются при оформлении документов аттестации (например, недостаток данных, несоответствие ГОСТ)?
35. Какие метрики используются для оценки качества аттестации ОИ?
Тема: 8. Специфика аттестации КВО
36. Какие особенности аттестации ОИ, относящихся к КВО (например, АСУ ТП, системы связи)?
37. Как учитываются специфика объектов КВО при разработке программы аттестации?
38. Какие дополнительные меры ИБ реализуются на ОИ КВО по сравнению с обычными системами?
39. Как категорирование КВО влияет на требования к аттестации ОИ?
40. Какие угрозы наиболее критичны для ОИ КВО (например, APT, физический доступ, утечка через побочные каналы)?
Тема: 9. Контроль и надзор за аттестацией
41. Как организован государственный контроль за проведением аттестации ОИ (например, проверки ФСТЭК)?
42. Какие виды инспекционного контроля проводятся за эксплуатацией аттестованных ОИ?
43. Как обрабатываются апелляции на результаты аттестации? Какие этапы рассмотрения?
44. Какие последствия могут быть при выявлении нарушений в ходе инспекционного контроля?
45. Как связаны аттестация ОИ и требования к защите государственной тайны?
Тема: 10. Современные вызовы и перспективы
46. Какие проблемы возникают при аттестации гибридных систем (локальные + облачные)?
47. Как искусственный интеллект и машинное обучение используются для автоматизации аттестации ОИ?
48. Как квантовые технологии влияют на будущее аттестации систем КВО?
49. Какие угрозы связаны с зависимостью от иностранных ИТ-технологий в аттестуемых системах?
50. Какие тренды будут определять развитие аттестации ОИ в ближайшие 5 лет (например, Zero Trust, защита IIoT)?
Тема: 11. Практические аспекты и кейсы
51. Какие этапы включает подготовка к аттестации системы управления водоснабжением города?
52. Как организовать симуляцию атаки (red team/blue team) для проверки защищенности ОИ КВО?
53. Какие ошибки чаще всего приводят к отказу в аттестации?
54. Какие меры реагирования требуются для исправления выявленных замечаний после аттестации?
55. Как подготовить отчет по результатам аттестации (структура, содержание, передача в ФСТЭК)?
Тема: 12. Сравнение с международным опытом
56. Какие отличия в подходах к аттестации ОИ в России и за рубежом (например, NIST, Common Criteria)?
57. Какие стандарты и фреймворки используются за рубежом для оценки защищенности критических систем (например, NIST IR, ISO/IEC 27001)?

58. Какие уроки из зарубежных инцидентов (например, Colonial Pipeline, SolarWinds) применимы к аттестации ОИ в РФ?
59. Как международное сотрудничество (INTERPOL, ENISA) влияет на обмен практиками аттестации?
60. Какие ограничения у российских подходов к аттестации по сравнению с зарубежными?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Основы аттестации 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	Тумбинская М. В., Петровский М. В.	Комплексное обеспечение информационной безопасности на предприятии: учебник для вузов	Санкт-Петербург: Лань, 2025
Л1.2	Гвоздева Т. В., Баллод Б. А.	Проектирование информационных систем. Стандартизация, техническое документирование информационных систем	Санкт-Петербург: Лань, 2021

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

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.	

4-48	Специализированная многофункциональная учебная лаборатория № 4-48 для проведения лабораторных и практических занятий	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 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.	

Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Основы аттестации 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.