

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная


Рабочая программа дисциплины
АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ
БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Часть, формируемая участниками образовательных отношений
№ дисциплины по учебному плану:	Б1.Ч.05.03.01
Трудоемкость в зачетных единицах:	3 семестр - 4;
Часов (всего) по учебному плану:	144 часа
Лекции	3 семестр - 32 часа;
Практические занятия	3 семестр - 32 часа;
Лабораторные работы	3 семестр - 16 часов;
Консультации	проводится в рамках часов аудиторных занятий
Самостоятельная работа	3 семестр - 63,7 часа;
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	проводится в рамках часов аудиторных занятий
включая: Контрольная работа Отчет	
Промежуточная аттестация:	
Зачет с оценкой	3 семестр - 0,3 часа;

Москва 2023

ПРОГРАММУ СОСТАВИЛ:


Преподаватель

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Рыжиков С.С.
	Идентификатор	R6eeae99e-RyzhikovSS-b1299f04

С.С. Рыжиков


СОГЛАСОВАНО:

Руководитель
образовательной программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

А.С. Минзов

Заведующий выпускающей
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

А.Ю. Невский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование у обучаемых знаний методов и технологий аттестации объектов информатизации требованиям нормативных документов ФСТЭК

Задачи дисциплины

- Знать понятие «аттестация объектов информатизации» как комплекс организационно-технических мероприятий;
- Уметь определять соответствие объекта требованиям по защите информации от несанкционированного доступа;
- Уметь проводить комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ПК-1 Способен организовывать работу по управлению функционированием СОИБ организации в соответствии с современными трендами информационной безопасности, на основе документального и инструментального анализа текущего состояния защищенности информационной инфраструктуры	ИД-2ПК-1 Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем	знать: - перечень работ, выполняемых при проведении аттестационных испытаний, и порядок их проведения в ходе сертификации средств защиты информации. уметь: - проводить аттестационные испытания защищаемого объекта информатизации в реальных условиях эксплуатации; - разрабатывать (участвовать в разработке) модели угроз безопасности современного объекта, в том числе с АСУ (АСУТП).
ПК-2 Способен применять математические методы и инновационные технологии при построении процедур оценки и управления рисками информационной безопасности	ИД-2ПК-2 Проводит оценку эффективности системы защиты информации автоматизированных систем	знать: - положение по аттестации объектов информатизации по требованиям безопасности информации; - алгоритм разработки программы и методик аттестационных испытаний объектов информатизации как комплекса организационно-технических мероприятий. уметь: - разрабатывать содержание отчетов и технической документации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП), направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

Базируется на уровне высшего образования (бакалавриат, специалитет).

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа							СР			
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
КПР	ГК	ИККП	ТК											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации	60	3	16	8	16	-	-	-	-	-	20	-	<p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации"</p> <p><u>Подготовка к лабораторной работе:</u> Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации" материалу.</p> <p><u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать</p>
1.1	Тема 1	7		2	1	2	-	-	-	-	-	2	-	
1.2	Тема 2	7		2	1	2	-	-	-	-	-	2	-	
1.3	Тема 3	9		2	1	2	-	-	-	-	-	4	-	
1.4	Тема 4	9		2	1	2	-	-	-	-	-	4	-	
1.5	Тема 5	14		4	2	4	-	-	-	-	-	4	-	
1.6	Тема 6	14		4	2	4	-	-	-	-	-	4	-	

													<p>примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><u>Подготовка доклада, выступления:</u> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты:</p> <p><u>Подготовка к контрольной работе:</u> Изучение материалов по разделу Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации и подготовка к контрольной работе</p> <p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации" подготовка к выполнению заданий на практических занятиях</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации"</p> <p><u>Изучение материалов литературных источников:</u> [1], 5-56</p>
2	Комплексная проверка (аттестационные испытания) защищаемого объекта	66		16	8	16	-	-	-	-	26	-	<p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях</p>

	информатизации в реальных условиях эксплуатации												эксплуатации" <u>Подготовка к лабораторной работе:</u> Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации" материалу. <u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы <u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <u>Подготовка доклада, выступления:</u> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: <u>Подготовка к контрольной работе:</u> Изучение материалов по разделу Комплексная проверка (аттестационные
2.1	Тема 7	16	4	2	4	-	-	-	-	-	6	-	
2.2	Тема 8	16	4	2	4	-	-	-	-	-	6	-	
2.3	Тема 9	16	4	2	4	-	-	-	-	-	6	-	
2.4	Тема 10	18	4	2	4	-	-	-	-	-	8	-	

													испытания) защищаемого объекта информатизации в реальных условиях эксплуатации и подготовка к контрольной работе <u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации" подготовка к выполнению заданий на практических занятиях <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации" <u>Изучение материалов литературных источников:</u> [1], 600-780 [2], 1-200 [3], 5-108
	Зачет с оценкой	18.0	-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	144.0	32	16	32	-	-	-	-	0.3	46	17.7	
	Итого за семестр	144.0	32	16	32	-	-	-	-	0.3	63.7		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПр – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации

1.1. Тема 1

Понятие «аттестация объектов информатизации» как комплекс организационно-технических мероприятий, в результате которых посредством специального документа (Аттестата соответствия) подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией (ФСТЭК) России..

1.2. Тема 2

Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации..

1.3. Тема 3

Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации. Правовой статус аттестата соответствия. Подача апелляции..

1.4. Тема 4

Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации..

1.5. Тема 5

Проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств; проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации. Анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации..

1.6. Тема 6

Организационно-правовые основы лицензирования деятельности по защите информации. Основные понятия в области лицензирования и их определения. Нормативные правовые акты, регламентирующие лицензирование деятельности в области защиты информации. Виды деятельности в области защиты информации, подлежащие лицензированию. Участники лицензионных отношений в области защиты информации. Порядок получения лицензий на деятельность в области защиты информации. Оснащение лаборатории по проведению специальных исследований объектов информатизации. Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации..

2. Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации

2.1. Тема 7

Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации, включающая: анализ исходных данных по аттестуемому объекту информатизации; предварительное ознакомление с аттестуемым объектом информатизации; проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации..

2.2. Тема 8

Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации, включающая: проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств..

2.3. Тема 9

Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации, включающая: проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации..

2.4. Тема 10

Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации, включающая: проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации; анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации..

3.3. Темы практических занятий

1. 7. Проведение контроля защищенности объекта информатизации в процессе эксплуатации с целью подтверждения заявленных характеристик;
2. 3. Формирование «пакета документов Заказчика» - перечень и структура документов, разрабатываемых на объекте информатизации перед началом аттестационных работ;
3. 5. Анализ исходных данных по аттестуемому объекту информатизации, проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативным документам;
4. 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации;
5. 6. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
6. 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации;
7. 8. Анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации;
8. 4. Формирование программы аттестационных испытаний и ознакомление с методиками, применяемыми для оценки защищенности объекта информатизации.

3.4. Темы лабораторных работ

1. Лабораторная работа №4. ПАК «Навигатор». Оценка защищенности информации от утечки по цепям электропитания, заземления, совместно расположенным линиям ВТСС и инженерным коммуникациям с учетом средств активной защиты;
2. Лабораторная работа №1. ПАК «Навигатор». Поиск информативного сигнала и определение его параметров. Измерения информативных сигналов, излучаемых СВТ. Расчеты величины зон r_1 , r_1' и R_2 возможного перехвата информации. Особенности проведения СИ TFT монитора;
3. Лабораторная работа №2. ПАК «Навигатор». Проведение объектовых специальных исследований. Оценка защищенности информации от утечки по цепям электропитания, заземления, совместно расположенным линиям ВТСС и инженерным коммуникациям;
4. Лабораторная работа №3. ПАК «Навигатор». Оценка защищенности информации от утечки по каналу ПЭМИ с учетом средств активной защиты;
5. Лабораторная работа №6. Оценка защищенности ЗП от утечки по акустическому каналу. Регулировка САЗ речевой информации и оценка их эффективности;
6. Лабораторная работа №7. Оценка защищенности ЗП от утечки по виброакустическому каналу. Проведение измерений на элементах ограждающих конструкций и инженерных коммуникаций. Регулировка САЗ речевой информации и оценка их эффективности;
7. Лабораторная работа №8. Пак «Навигатор». Оценка защищенности информации на объекте информатизации. Оценка эффективности САЗ;
8. Лабораторная работа №5. Контроль защищенности от НСД. Средство создания модели системы разграничения доступа «Ревизор 1 ХР». Программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 ХР». Программа фиксации и контроля исходного состояния программного комплекса «Фикс 2.0.1»; Программа поиска и гарантированного уничтожения информации на дисках «Terrier».

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации"
2. Обсуждение материалов по кейсам раздела "Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)		Оценочное средство (тип и наименование)
		1	2	
Знать:				
перечень работ, выполняемых при проведении аттестационных испытаниях, и порядок их проведения в ходе сертификации средств защиты информации	ИД-2ПК-1	+		Контрольная работа/Контрольная работа № 1; Защита лабораторной работы № 1; Защита лабораторной работы № 2; Защита лабораторной работы № 3 Отчет/Контрольная работа № 2; Защита лабораторной работы № 4; Защита лабораторной работы № 5
алгоритм разработки программы и методик аттестационных испытаний объектов информатизации как комплекса организационно-технических мероприятий	ИД-2ПК-2	+		Контрольная работа/Контрольная работа № 3; Защита лабораторной работы № 6
положение по аттестации объектов информатизации по требованиям безопасности информации	ИД-2ПК-2		+	Отчет/Защита лабораторной работы № 7; Защита лабораторной работы № 8
Уметь:				
разрабатывать (участвовать в разработке) модели угроз безопасности современного объекта, в том числе с АСУ (АСУТП)	ИД-2ПК-1	+		Контрольная работа/Контрольная работа № 3; Защита лабораторной работы № 6
проводить аттестационные испытания защищаемого объекта информатизации в реальных условиях эксплуатации	ИД-2ПК-1	+		Контрольная работа/Контрольная работа № 1; Защита лабораторной работы № 1; Защита лабораторной работы № 2; Защита лабораторной работы № 3 Отчет/Контрольная работа № 2; Защита лабораторной работы № 4; Защита лабораторной работы № 5
разрабатывать содержание отчетов и технической	ИД-2ПК-2		+	Отчет/Защита лабораторной работы № 7; Защита

документации				лабораторной работы № 8
--------------	--	--	--	-------------------------

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

3 семестр

Форма реализации: Защита задания

1. Защита лабораторной работы № 7; Защита лабораторной работы № 8 (Отчет)
2. Контрольная работа № 2; Защита лабораторной работы № 4; Защита лабораторной работы № 5 (Отчет)

Форма реализации: Письменная работа

1. Контрольная работа № 1; Защита лабораторной работы № 1; Защита лабораторной работы № 2; Защита лабораторной работы № 3 (Контрольная работа)
2. Контрольная работа № 3; Защита лабораторной работы № 6 (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №3)

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 3 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие : пер. с англ. / Б. А. Фороузан . – М. : Интернет-Ун-т информ. технологий : БИНОМ. Лаборатория знаний, 2010 . – 784 с. – (Основы информационных технологий) . - ISBN 978-5-9963-0242-0 .;
2. Конституция Российской Федерации: Комментарий Конституционного суда РФ, официальный текст, принятие и вступление в силу поправок / Упр. юстиции Моск. области ; Ред. Ю. Н. Власов . – 3-е изд., доп. и перераб . – М. : Юрайт, 2000 . – 200 с. - ISBN 5-85294-042-0 .;
3. Ворона В. А., Тихонов В. А.- "Инженерно-техническая и пожарная защита объектов. (Серия «Обеспечение безопасности объектов»; Выпуск 4.)", Издательство: "Горячая линия-Телеком", Москва, 2012 - (512 с.)
http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5139.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Видеоконференции (Майнд, Сберджаз, ВК и др).

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. Научная электронная библиотека - <https://elibrary.ru/>
3. База данных Web of Science - <http://webofscience.com/>
4. База данных Scopus - <http://www.scopus.com>
5. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
6. Портал открытых данных Российской Федерации - <https://data.gov.ru>
7. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
8. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
9. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
10. База открытых данных Росфинмониторинга - <http://www.fedsfm.ru/opendata>
11. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
12. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
13. Официальный сайт Федерального агентства по техническому регулированию и метрологии - <http://protect.gost.ru/>
14. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
	М-504, Учебная лаборатория "Технические средства защиты информации"	парта, стул, экран, доска маркерная, лабораторный стенд, компьютер персональный, кондиционер
Учебные аудитории для проведения лабораторных занятий	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
	М-504, Учебная лаборатория "Технические средства защиты информации"	парта, стул, экран, доска маркерная, лабораторный стенд, компьютер персональный, кондиционер

Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Аттестация объектов информатизации по требованиям безопасности информации

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Контрольная работа № 1; Защита лабораторной работы № 1; Защита лабораторной работы № 2; Защита лабораторной работы № 3 (Контрольная работа)
- КМ-2 Контрольная работа № 2; Защита лабораторной работы № 4; Защита лабораторной работы № 5 (Отчет)
- КМ-3 Контрольная работа № 3; Защита лабораторной работы № 6 (Контрольная работа)
- КМ-4 Защита лабораторной работы № 7; Защита лабораторной работы № 8 (Отчет)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации					
1.1	Тема 1		+	+	+	
1.2	Тема 2		+	+	+	
1.3	Тема 3		+	+	+	
1.4	Тема 4		+	+	+	
1.5	Тема 5		+	+	+	
1.6	Тема 6		+	+	+	
2	Комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации					
2.1	Тема 7					+
2.2	Тема 8					+
2.3	Тема 9					+
2.4	Тема 10					+
Вес КМ, %:			20	20	20	40

