Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВЫ АТТЕСТАЦИИ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
4	2	72	8	22	0		42	0	З
Итого	2	72	8	22	0	12	42	0	

Москва, 2020

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Основы аттестации защищаемых помещений» содержит описание целей освоения дисциплины, ее место в структуре ООП, ВО, формируемые в результате освоения дисциплины компетенции студента, структуру и содержание дисциплины, используемые во время освоения дисциплины образовательные технологии, оценочные средства для контроля успеваемости, учебно-методическое, информационное и материально-техническое обеспечение дисциплины.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Основы аттестации защищаемых помещений» обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ аттестации защищаемых помещений по требованиям безопасности информации.

Задачами дисциплины являются:

- дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области технической защиты информации (ТЗИ); физических основ реализации угроз безопасности информации защищаемых помещений (ВП) и порядка их выявления; практической отработки методик проведения специальных исследований ВП в соответствии с методологией исследований защищенности помещений на соответствие требованиям по безопасности информации; организации и порядка проведения аттестации ВП и отработки технических документов по результатам аттестационных испытаний.

В результате обучения студенты должны ознакомиться с:

концептуальными основами защиты информации в Российской Федерации и с содержанием документов, составляющих правовую основу ТЗИ;

системой организационно-распорядительных, нормативных и информационных документов ФСТЭК России и Ростехрегулирования, определяющих организацию, правила и порядок осуществления деятельности в области ТЗИ;

организацией лицензирования деятельности в области защиты информации, функциями участников системы лицензирования ФСТЭК России;

организацией сертификации средств защиты информации в системе сертификации ФСТЭК России №РОСС RU.0001.01.БИ00, функциями участников системы сертификации;

организацией контроля выполнения лицензионных требований и условий предприятиями-лицензиатами ФСТЭК России;

должны знать:

потенциальные угрозы безопасности информации, реализуемые на объектах информатизации и в автоматизированных (информационных) системах;

организационно-технические основы реализации угроз конфиденциальности, доступности и целостности информации ограниченного доступа;

физические основы возникновения технических каналов утечки информации при ее обработке на технических средствах;

организационно-технические основы реализации несанкционированного доступа к информации, циркулирующей в ВП;

требования и рекомендации организационно-распорядительных и нормативных документов по обеспечению безопасности информации ограниченного доступа, а также

требования к форме и содержанию технических документов, разрабатываемых по результатам аттестации ВП;

инструментальные, инструментально-расчетные и расчетные методы и процедуры выявления угроз безопасности информации для ВП;

порядок организации защиты информации на предприятии, номенклатуру и требования к содержанию организационно-распорядительных документов внутреннего пользования предприятия;

номенклатуру и возможности технических, программно-технических и программ.

должны уметь:

проводить специальные исследования ВП и аттестационные испытания ВП по требованиям безопасности информации (БИ);

применять технические, программно-технические и программные средства контроля защищённости информации и средства оценки эффективности применяемых для ВП средств защиты информации;

разрабатывать технические документы по результатам аттестационных испытаний ВП;

должны владеть навыками:

выявления потенциальных угроз безопасности информации для ВП;

применения расчётных, инструментально-расчетных и расчетных методов оценки защищённости информации, циркулирующей в ВП;

разработки технических документов по результатам аттестационных испытаний ВП по требованиям БИ.

Дисциплина «Основы аттестации защищаемых помещений» является неотъемлемой составной частью профессиональной подготовки магистров по образовательной программе подготовки «Обеспечение безопасности значимых объектов критической информационной инфраструктуры». Вместе с другими дисциплин специального цикла изучение данной дисциплины призвано вырабатывать такие качества, как:

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Основы аттестации защищаемых помещений» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками таких дисциплин, как «Физические основы технических каналов утечки информации», «Измерительная аппаратура анализа защищенности объектов», «Методы и средства контроля эффективности защиты информации от несанкционированного доступа», «Основы технической защиты конфиденциальной информации».

Знания, полученные при изучении дисциплины «Основы аттестации защищаемых помещений» являются базовыми, для дисциплин, входящих в вариативную часть профессионального цикла учебного плана подготовки магистров по направлению подготовки

10.04.01 «Информационная безопасность» по образовательной программе подготовки «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-3 [1] – Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	З-ОПК-3 [1] – Знать: основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью У-ОПК-3 [1] – Уметь: проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации В-ОПК-3 [1] – Владеть: навыками разработки политик безопасности различных уровней и работы с нормативными правовыми актами в области информационной безопасности

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-2.3 [1] - Способен устанавливать требования к обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов	З-ПК-2.3[1] - Знать: Отечественные стандарты в области информатизации и обеспечения информационной безопасности АСУ, информационных и телекоммуникационных систем общего и специального назначения; Основные

		КИИ *Основание:* Профессиональный стандарт: 06.033, 06.034	принципы обеспечения безопасности КИИ; Основные положения ядерной безопасности; Причины возникновения инцидентов ядерной безопасности; Основные виды угроз для АСУ ТП на АЭС; Сущность основных физических процессов и информационных угроз в АСУ ТП в ядерном реакторе, их взаимосвязь; Требования по обеспечению безопасности значимых объектов КИИ.; У-ПК-2.3[1] - Уметь: Планировать, разрабатывать, совершенствовать и осуществлять внедрение мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Выявлять основные информационные угрозы в АСУ ТП ядерного реактора; Проводить оценку необходимости применения средств ядерной защиты реакторов. ; В-ПК-2.3[1] - Владеть: Навыками внедрения мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Навыками внедрения мероприятий по реализации комплекса

			мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности значимых объектов КИИ; Навыком обоснованного выбора средств защиты информации и средств ядерной защиты реакторов с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ; Навыком общего/детального анализа структуры системы безопасности значимого объекта КИИ.
научно- исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем

			защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	З-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки

безопасности информации	инфраструктуры		за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов

			аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения

			аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	4 Семестр						
1	Раздел 1. Общие положения законодательной и нормативно- правовой базы в области защиты информации. Выявление угроз безопасности информации, обусловленных техническими каналами утечки информации	1-8			25	КИ-8	З-ОПК-3, У-ОПК-3, З-ПК-2.3, У-ПК-2.3, З-ПК-4, У-ПК-4
2	Раздел 2. Порядок аттестации защищаемых помещений по требованиям безопасности информации. Содержание этапов аттестационных испытаний ЗП	9-15			25	КИ-15	З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-

							ПК-4
	Итого за 4 Семестр		8/22/0		50		
	Контрольные мероприятия за 4 Семестр				50	З	З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-4

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	4 Семестр	8	22	0
1-8	**Раздел 1. Общие положения законодательной и нормативно- правовой базы в области защиты информации. Выявление угроз безопасности**	4	12	

	информации, обусловленных техническими каналами утечки информации			
1 - 2	**Тема 1. Организационно-правовые основы технической защиты информации Лицензирование деятельности по защите информации, сертификация средств защиты информации** Основные понятия в области ТЗИ. Концепция национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих. Сертификация средств защиты информации по требованиям безопасности информации. Система сертификации средств защиты информации по требования безопасности информации № РОСС RU.0001.01.БИ00. Порядок аккредитации участников системы сертификации. Основные направления деятельности органов по аттестации объектов информатизации по требованиям безопасности информации. Функции органов по аттестации ОИ по требованиям безопасности информации. Общий порядок аттестации ОИ по требованиям безопасности информации.	Всего аудиторных часов		
		1	2	
		Онлайн		
3 - 4	**Тема 2. Технические каналы утечки информации** Физические основы возникновения технических каналов утечки информации. Классификация технических каналов утечки информации в технических средствах. Характеристики технических каналов утечки информации. Технические каналы утечки информации объектов информатизации. Система документов, определяющих требования, нормы, рекомендации по защите информации от утечки по техническим каналам.	Всего аудиторных часов		
		1	4	
		Онлайн		
5 - 6	**Тема 3. Порядок выявления угроз безопасности информации ограниченного доступа, обусловленных реализацией технических каналов утечки информации** Специальные исследования защищаемых помещений. Требования к контрольно-измерительному и специальному оборудованию рабочего места, предназначенного для проведения специальных исследований защищаемых помещений. Общий порядок проведения специальных исследований. Тестовые сигналы. Общие технические требования к характеристикам тестовых сигналов. Номенклатура и требования к содержанию технических документов, подготавливаемых по результатам специальных исследований технических средств и защищаемых помещений. Протокол специальных исследований. Предписание на эксплуатацию технического средства. Основные требования и рекомендации по технической защите информации, составляющей государственную	Всего аудиторных часов		
		1	4	
		Онлайн		

	тайну. Основные требования и рекомендации по технической защите информации ограниченного доступа, содержащей сведения, не составляющие государственную тайну.			
7 - 8	**Тема 4. Средства контроля эффективности защиты информации. Технические, программно-технические средства защиты информации.** Средства контроля защищенности информации от утечки по техническим каналам. Средства контроля защищенности информации от утечки по каналу побочных электромагнитных излучений и наводок. Средства контроля защищенности информации от утечки за счет модуляции информативным сигналом преднамеренно создаваемых (непреднамеренно возникающих за счет работы технических систем и средств) высокочастотных колебаний или полей. Средства контроля защищенности информации, обрабатываемой с использованием автоматизированных систем различного уровня и назначения. Установка, монтаж, настройка (наладка) средств защиты информации от утечки по техническим каналам.	Всего аудиторных часов 1 Онлайн	2	
9-15	**Раздел 2. Порядок аттестации защищаемых помещений по требованиям безопасности информации. Содержание этапов аттестационных испытаний ЗП**	4	10	
9 - 12	**Тема 5. Основные этапы проведения аттестации ЗП по требованиям безопасности информации.** Перечень и содержание организационно-распорядительных и технических документов на выделенное помещение, подготавливаемых заявителем. Акт категорирования объекта информатизации. Акт классификации объекта информатизации. Технический паспорт объекта информатизации. Распоряжения, приказы, инструкции, регламентирующие организацию функционирования и защиту информации на объекте информатизации Определение (расчет) трудозатрат на проведение аттестации защищаемого помещения. Этап контроля (оценки) полноты и качества разработки заявителем организационно-распорядительных и технических документов на ЗП. Проверка соответствия исходных данных на ЗП. Проверка правильности категорирования и классификации объекта информатизации. Проверка содержания технического паспорта объекта информатизации на предмет полноты учета технических (программных, программно-технических) и организационных предпосылок для реализации угроз безопасности информации. Этап подготовки к проведению аттестационных испытаний. Определение номенклатуры задач, решаемых для ЗП, вида, объема и степени циркулирующей информации. Определение состава технических средств, установленного в ЗП. Определение необходимого комплекса технических средств, общего и специального	Всего аудиторных часов 2 Онлайн	6	

	(прикладного) программного обеспечения, применяемого для обработки информации ограниченного доступа. Определение условий расположения (размещения) ЗП относительно контролируемой зоны. Определение состава и степени участия персонала в обработке информации ограниченного доступа. Определение уровня квалификации персонала, допущенного к эксплуатации ЗП. Программа и методики аттестационных испытаний ЗП. Этап аттестационных испытаний. Методы проведения аттестационных испытаний. Инструментально-расчетные и расчетные методы оценки защищенности информации ограниченного доступа. Разработка рекомендаций по защите информации, обрабатываемой в ЗП. Оценка эффективности средств защиты информации. Этап разработки документов по результатам объектовых аттестационных испытаний. Основные требования к содержанию документов, разрабатываемых по результатам аттестационных испытаний.			
13 - 15	**Тема 6. Организация контроля защищенности информации ограниченного доступа на этапе эксплуатации защищаемого помещения** Планирование работ по контролю состояния защиты информации в защищаемом помещении. Организация и порядок про ведения периодического контроля выполнения норм, требований и рекомендаций, определенных техническими документами на ЗП. Разработка предложений по устранению выявленных по результатам периодического контроля недостатков. Номенклатура, форма и требования к содержанию документов, разрабатываемых по результатам периодического контроля выполнения норм, требований и рекомендаций по защите информации в выделенном помещении. Заключение.	Всего аудиторных часов		
		2	4	
		Онлайн		

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	Темы занятий / Содержание
	4 Семестр
1 - 2	**Тема 1. Организационно-правовые основы технической защиты информации Лицензирование деятельности по защите информации, сертификация средств защиты информации** Основные понятия в области ТЗИ.
3 - 4	**Тема 2. Технические каналы утечки информации** Физические основы возникновения технических каналов утечки информации.
5 - 6	**Тема 3. Порядок выявления угроз безопасности информации ограниченного доступа, обусловленных реализацией технических каналов утечки информации** Специальные исследования защищаемых помещений.
7 - 8	**Тема 4. Средства контроля эффективности защиты информации. Технические, программно-технические средства защиты информации.** Средства контроля защищенности информации от утечки по техническим каналам.
9 - 12	**Тема 5. Основные этапы проведения аттестации ЗП по требованиям безопасности информации.** Перечень и содержание организационно-распорядительных и технических документов на выделенное помещение, подготавливаемых заявителем.
13 - 15	**Тема 6. Организация контроля защищенности информации ограниченного доступа на этапе эксплуатации защищаемого помещения** Планирование работ по контролю состояния защиты информации в защищаемом помещении.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий.

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации защищаемых помещений по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Практические занятия по аттестации защищаемых помещений по требованиям безопасности информации, обнаружению ТКУИ и отработке методического

аппарата технического контроля проводятся по циклам на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ. Результаты используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ОПК-3	З-ОПК-3	З, КИ-8, КИ-15
	У-ОПК-3	З, КИ-8, КИ-15
	В-ОПК-3	З, КИ-15
ПК-2.3	З-ПК-2.3	З, КИ-8, КИ-15
	У-ПК-2.3	З, КИ-8, КИ-15
	В-ПК-2.3	З, КИ-15
ПК-3	З-ПК-3	З, КИ-15
	У-ПК-3	З, КИ-15
	В-ПК-3	З, КИ-15
ПК-4	З-ПК-4	З, КИ-8, КИ-15
	У-ПК-4	З, КИ-8, КИ-15
	В-ПК-4	З, КИ-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать

			теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Д84 Оценка защищенности речевой информации Ч.1 Выявление акустических и вибрационных каналов утечки речевой информации, Москва: НИЯУ МИФИ, 2015

2. ЭИ Д84 Оценка защищенности речевой информации Ч.2 Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

3. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале акустоэлектромагнитного преобразования, Москва: НИЯУ МИФИ, 2018

4. ЭИ Д84 Оценка защищенности речевой информации Ч.4 Проведение инструментального контроля в канале высокочастотного навязывания, Москва: НИЯУ МИФИ, 2018

5. ЭИ Д84 Оценка защищенности речевой информации Ч.5 Проведение инструментального контроля в канале высокочастотного облучения, Москва: НИЯУ МИФИ, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

2. 004 А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

3. ЭИ К65 Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : лабораторный практикум, Москва: НИЯУ МИФИ, 2013

4. 004 К65 Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

5. 004 К65 Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

6. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале высокочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Вузовские электронно-библиотечные системы учебной литературы ()

2. База научно-технической информации (например, ВИНИТИ РАН) ()

3. www.fstec.ru; www.gost.ru; www.fsb.ru. ()

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. «Защита речевой информации от утечки за счет недостаточной звуко- и виброизоляции помещений (АВАК)»

2. «Защита информации от утечки по техническим каналам (ПЭМИН)»

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы, место курса в различных областях науки и техники, в том числе в области информационной безопасности.

Аттестация по разделам:

КР8, КР14 - максим.балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех практических заданий раздела.

При не аттестации хотя бы по одному из разделов, студент не допускается к зачету.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации защищаемых помещений по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений.

Практические занятия по аттестации защищаемых помещений по требованиям безопасности информации, обнаружению ТКУИ и отработке методического аппарата технического контроля проводятся по циклам на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы, место курса в различных областях науки и техники, в том числе в области информационной безопасности.

Аттестация по разделам:

КР8, КР14 - максим. балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При неаттестации хотя бы по одному из разделов, студент не допускается к зачету.

1. Чтение лекций.

Первая лекция должна быть введением к дисциплине (разделу дисциплины, читаемому

в начинающемся семестре). Она должна содержать общий обзор содержания дисциплины. В ней следует отметить методические инновации в решении задач, рассматриваемых в дисциплине, дать перечень рекомендованной литературы и вновь появившихся литературных источников, обратив внимание студентов на обязательную и дополнительную литературу.

Изложению текущего лекционного материала должна предшествовать вводная часть, содержащая краткий перечень вопросов, рассмотренных на предыдущих лекциях. На этом этапе полезно задать несколько вопросов аудитории, осуществить выборочный контроль знания студентов.

При изложении лекционного материала следует поощрять вопросы непосредственно в процессе изложения, внимательно относясь к вопросам студентов и при необходимости давая дополнительные, более подробные пояснения.

При чтении лекций преимущественное внимание следует уделять качественным вопросам, опуская простые математические выкладки, либо рекомендуя выполнить их самим студентам, либо отсылая студентов к литературным источникам и методическим пособиям.

В процессе лекционного курса необходимо возможно чаще возвращаться к основным вопросам дисциплины, проводя выборочный экспресс-контроль знаний студентов.

Принятая преподавателем система обозначений должна чётко разъясняться в процессе её введения и использоваться в конспектах лекций

В лекциях, предшествующих практическим занятиям, следует кратко излагать содержание и основные задачи практического занятия, дать рекомендации студентам для подготовки к нему.

На последней лекции важно найти время для обзора основных положений, рассмотренных в дисциплине, перечню и формулировке вопросов, выносимых на экзамен или зачёт.

2. Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Дураковский Анатолий Петрович, к.т.н., доцент

Рецензент(ы):

Горбатов В.С.