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 ТЕХНИЧЕСКИХ СРЕДСТВ ОБРАБОТКИ ИНФОРМАЦИИ

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**
3, 4	2	72	8	0	24		40	0	З
Итого	2	72	8	0	24	12	40	0	

Москва, 2020

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Основы аттестации технических средств обработки информации» 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 технических средств обработки информации» обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области аттестации технических средств обработки информации и автоматизированных (информационных) систем (АС) 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 на ОИ и порядка их выявления; практической отработки методик проведения специальных исследований ОТСС и ВТСС в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации; организации и порядка проведения аттестации ОИ 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, обрабатываемой в АС;

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 АС;

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

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 ОТСС, ВТСС и аттестационные испытания АС по требованиям безопасности информации (БИ);

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

разрабатывать технические документы по результатам аттестационных испытаний АС;

должны владеть навыками:

выявления потенциальных угроз безопасности информации, обрабатываемой в АС;

применения расчётных, инструментально-расчетных и расчетных методов оценки защищённости информации, обрабатываемой в АС;

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

Дисциплина «Основы аттестации технических средств обработки информации» является неотъемлемой составной частью профессиональной подготовки магистров по образовательной программе подготовки «Обеспечение безопасности информации ключевых систем 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 технических средств обработки информации» 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 смежных дисциплин «Электротехника», «Метрология и электрорадиоизмерения», «Основы радиотехники», «Распространение радиоволн», «Системы связи», «Программно-аппаратные средства обеспечения информационной безопасности», «Антенно-фидерные устройства», «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 технических средств обработки информации» 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	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-2.3 [1] - Способен устанавливать требования к обеспечению безопасности	З-ПК-2.3[1] - Знать: Отечественные стандарты в области информатизации и обеспечения информационной

объектов на стадиях разработки, эксплуатации и модернизации		значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ *Основание:* Профессиональный стандарт: 06.033, 06.034	безопасности АСУ, информационных и телекоммуникационных систем общего и специального назначения; Основные 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	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	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	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

научных исследований отчетов, статей, докладов на научных конференциях	инфраструктуры	*Основание:* Профессиональный стандарт: 06.030	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	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы,	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный	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

испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	стандарт: 06.032, 06.034	информации в компьютерных системах; методы и методики контроля защищенности информации от утечки 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
	3 Семестр						
1	Выявление угроз безопасности информации, обрабатываемой техническими средствами обработки информации (ТСОИ), обусловленных техническими каналами утечки информации	1-8	4/0/12		25	КИ-8	З-ОПК-3, У-ОПК-3, З-ПК-2.3, У-ПК-2.3, З-ПК-4, У-ПК-4
2	Порядок аттестации ТСОИ по требованиям безопасности информации. Содержание этапов аттестационных испытаний ТСОИ	9-15	4/0/12		25	КИ-16	В-ПК-2.3, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-4, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-2.3, У-

							ПК-2.3
	Итого за 3 Семестр		8/0/24		50		
	Контрольные мероприятия за 3 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.**
	3 Семестр	8	0	24
1-8	**Выявление угроз безопасности информации, обрабатываемой техническими средствами обработки**	4	0	12

	информации (ТСОИ), обусловленных техническими каналами утечки информации			
1 - 3	**Тема 1. Порядок выявления угроз безопасности информации ограниченного доступа, обусловленных реализацией технических каналов утечки информации** Специальные исследования основных и вспомогательных технических средств, и систем. Требования к контрольно-измерительному и специальному оборудованию рабочего места, предназначенного для проведения специальных исследований технических средств и систем. Общий порядок проведения лабораторных 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 систем. Протокол специальных исследований. Предписание на эксплуатацию технического средства. Основные требования и рекомендации по технической защите информации, составляющей государственную тайну. Основные требования и рекомендации по технической защите информации ограниченного доступа, содержащей сведения, не составляющие государственную тайну.	Всего аудиторных часов		
		1		4
		Онлайн		
4 - 5	**Тема 2. Порядок выявления угроз безопасности информации ограниченного доступа, обусловленных несанкционированным доступом к информации и реализацией специальных воздействий на нее** Особенности проведения комплексного исследования объектов информатизации автоматизированных (информационных) систем на наличие угроз безопасности информации. Оценка опасности угроз. Классификация объектов информатизации, информационных ресурсов. Категорирование объектов информатизации, информационных ресурсов. Рекомендации по классификации и категорированию. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Построение и функционирование системы защиты информации типовых объектов информатизации на различных стадиях их жизненного цикла. Основные предпосылки реализации угроз безопасности информации ограниченного доступа, обрабатываемой с использованием автоматизированных систем различного уровня и назначения, обусловленных несанкционированным доступом (НСД) к ней и специальными воздействиями на нее. Классификация угроз безопасности информации по результатам реализации НСД и специальных воздействий	Всего аудиторных часов		
		1		4
		Онлайн		

	на нее. Принципы выявления угроз НСД к информации и специальных воздействий на нее в системах обработки информации. Система документов, определяющих требования, нормы, рекомендации по защите информации ограниченного доступа от НСД и специальных воздействий на информацию. Защита автоматизированных систем от несанкционированного доступа к обрабатываемой информации. Классификация автоматизированных систем и требования по защите информации. Оценка защищенности автоматизированных систем от НСД к обрабатываемой информации. Методики оценки защищенности подсистемы управления доступом в автоматизированных системах (АС), подсистемы регистрации и учета в АС, криптографической подсистемы защиты информации, обрабатываемой в АС, подсистемы обеспечения целостности информации, обрабатываемой в АС. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ. Деструктивные функции вредоносных программ и способы их реализации. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии АС, обрабатывающей информацию ограниченного доступа, с информационными сетями общего пользования.			
6 - 8	**Тема 3. 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. Средства защиты информации от несанкционированного доступа. Средства контроля разграничения доступа к информационным ресурсам в автоматизированной (информационной) системе. Средства контроля затирания остаточной информации на машинных носителях информации. Средства контроля и фиксации состояния программного комплекса автоматизированной	Всего аудиторных часов 2 Онлайн		4

	(информационной) системы. Установка, монтаж, настройка (наладка) средств защиты информации от утечки по техническим каналам, средств защиты информации от НСД.			
9-15	**Порядок аттестации ТСОИ по требованиям безопасности информации. Содержание этапов аттестационных испытаний ТСОИ**	4	0	12
9 - 13	**Тема 4. Основные этапы проведения аттестации ТСОИ по требованиям безопасности информации.** Перечень и содержание организационно-распорядительных и технических документов на объект информатизации, 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 объекта информатизации. Этап контроля (оценки) полноты и качества разработки заявителем организационно-распорядительных и технических документов на объект информатизации. Проверка соответствия исходных данных на объект информатизации фактическим. 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 с использованием объекта информатизации, вида, объема и степени секретности информационных ресурсов, подлежащих обработке. Определение состава технических средств (в том числе носителей информации), с помощью которых производится обработка информации ограниченного доступа. Определение необходимого комплекса технических средств, общего и специального (прикладного) программного обеспечения, применяемого для обработки информации ограниченного доступа. Определение условий расположения (размещения) объекта информатизации относительно контролируемой зоны. Определение состава и степени участия персонала в обработке информации ограниченного доступа. Определение уровня квалификации персонала, допущенного к эксплуатации объекта информатизации. Программа и методики аттестационных испытаний объекта информатизации. Этап объектовых аттестационных испытаний. Методы проведения объектовых аттестационных испытаний.	Всего аудиторных часов 2 Онлайн		6

	Инструментально-расчетные и расчетные методы оценки защищенности информации ограниченного доступа. Разработка рекомендаций по защите информации, обрабатываемой на объекте информатизации. Оценка эффективности средств защиты информации. Этап разработки документов по результатам объектовых аттестационных испытаний. Основные требования к содержанию документов, разрабатываемых по результатам аттестационных испытаний.			
14 - 15	**Тема 5. Организация контроля защищенности информации ограниченного доступа на этапе эксплуатации ТСОИ** Планирование работ по контролю состояния защиты информации на объекте информатизации. Организация и порядок про ведения периодического контроля выполнения норм, требований и рекомендаций, определенных техническими документами на объект информатизации. 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 на объекте информатизации. Заключение.	Всего аудиторных часов		
		2		6
		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 ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	3 Семестр
1 - 3	**Лабораторная работа № 1** Измерение спектральных характеристик тестовых сигналов ПЭМИН. Расчет показателей защищенности (R2, r1 и r1'). Оформление протоколов стендовых специальных исследований и предписания на эксплуатацию СВТ.

4 - 5	**Лабораторная работа № 2** Инструментальный контроль защищенности ОТСС, обрабатывающих цифровую информацию, представленную в виде электрических сигналов в эфире. Выбор размещения (уточнение) точек контроля показателя защищенности в эфире. Организация тестовых режимов работы при оценке эффективности активных средств защиты.
6 - 8	**Лабораторная работа № 3** Инструментальный контроль защищенности ОТСС, обрабатывающих цифровую информацию, представленную в виде электрических сигналов в линиях. Выбор размещения (уточнение) точек контроля показателя защищенности в линиях. Организация тестовых режимов работы при оценке эффективности активных средств защиты.
9 - 10	**Лабораторная работа № 4** Измерение реального затухания тестовых сигналов и шумовых сигналов средств защиты информации на объекте информатизации до выбранных точек возможного ведения разведки.
11 - 13	**Лабораторная работа № 5** Инструментальный контроль защищенности речевой информации от утечки по каналу низкочастотного акустоэлектрического преобразования (НЧ АЭП)
14 - 15	**Лабораторная работа № 6** Инструментальный контроль защищенности речевой информации от утечки по каналу высокочастотного акустоэлектрического преобразования (ВЧ АЭП)

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 ТСОИ 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 ТСОИ по требованиям безопасности информации, обнаружению ТКУИ и отработке методического аппарата технического контроля

проводятся по циклам на автоматизированных рабочих местах в специализированной лаборатории и в безэховой экранированной камере. 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-16
	У-ОПК-3	З, КИ-8, КИ-16
	В-ОПК-3	З, КИ-16
ПК-2.3	З-ПК-2.3	З, КИ-8, КИ-16
	У-ПК-2.3	З, КИ-8, КИ-16
	В-ПК-2.3	З, КИ-16
ПК-3	З-ПК-3	З, КИ-16
	У-ПК-3	З, КИ-16
	В-ПК-3	З, КИ-16
ПК-4	З-ПК-4	З, КИ-8, КИ-16
	У-ПК-4	З, КИ-8, КИ-16
	В-ПК-4	З, КИ-16

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.3 Проведение инструментального контроля в канале высокочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

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

6. 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 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

3. 004 П30 Основы практической защиты информации : учебное пособие, Москва: Akademia, 2013

4. 004 В24 Введение в информационную безопасность : учебное пособие для вузов, А. А. Малюк [и др.], Москва: Горячая линия - Телеком, 2013

5. 004 Б90 Защита от утечки информации по техническим каналам : учеб. пособие, Г. А. Бузов, С. В. Калинин, А. В. Кондратьев, М.: Горячая линия - Телеком, 2005

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 информации от утечки по техническим каналам (ПЭМИН)» ()

2. Безэховая экранированная камера (БЭК) ()

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

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.