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

МЕТОДЫ ВЫЯВЛЕНИЯ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В РАДИОЭЛЕКТРОННОЙ АППАРАТУРЕ

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	3	108	8	24	0		40	0	Э
Итого	3	108	8	24	0	12	40	0	

АННОТАЦИЯ

Задачами дисциплины являются:

дать основы первичного анализа состава радиоэлектронной аппаратуры с выделением критичных и подозрительных элементов, блоков, узлов; познакомить с существующими методами более детального анализа и проверки аутентичности электронных компонентов, блоков и узлов для развития навыков рационального выбора состава и последовательности применения этих методов, которые нарабатываются в ходе практических занятий; обоснованного разделения подозрительных электронных компонентов на аутентичные, контрафактные, а также искусственно внесенные в конструкцию для получения несанкционированного доступа к информации и/или реализации недекларированных возможностей. В основе теоретической базы лежат как отечественные нормативные документы (национальные стандарты, рекомендации), так и зарубежные стандарты, разработанные международными исследовательскими группами.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Методы выявления недекларированных возможностей в радиоэлектронной аппаратуре» является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области выбора и применения методов выявления демаскирующих признаков неаутентичных электронных компонентов, блоков, модулей в составе радиоэлектронной аппаратуры.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Методы выявления недекларированных возможностей в радиоэлектронной аппаратуре» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» (блок Б1.ДВ.2).

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками смежных дисциплин «Теоретические основы защиты информации в ключевых системах информационной инфраструктуры», «Организационно-правовые механизмы обеспечения информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Основы аттестации объектов информатизации».

Знания, полученные при изучении дисциплины «Методы выявления недекларированных возможностей в радиоэлектронной аппаратуре» 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-1 [1] – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	В-ОПК-1 [1] – Владеть: навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности У-ОПК-1 [1] – Уметь: проектировать информационные системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности. З-ОПК-1 [1] – Знать: основы стандартов в области обеспечения информационной безопасности; элементы компьютерного моделирования сложных систем, проектирования информационных, автоматизированных и автоматических систем
ОПК-2 [1] – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	З-ОПК-2 [1] – Знать: методы проектирования технологий обеспечения информационной безопасности; принципы построения и функционирования современных информационных систем; требования к системам комплексной защиты информации У-ОПК-2 [1] – Уметь: обосновывать применяемые методы решения задач защиты информации, проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов, разрабатывать модели угроз и нарушителей информационной безопасности В-ОПК-2 [1] – Владеть: навыками проектирования систем 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,	Средства и технологии обеспечения безопасности значимых объектов критической информационной	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ иди информационно-	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации

эксплуатации и модернизации	инфраструктуры	аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа. ; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства

			современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее. ; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее;

			основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.
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.

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	Первый раздел	1-8	4/12/0		25	КИ-8	З-ОПК-1, У-ОПК-1, З-ОПК-2, У-ОПК-2, З-ПК-2, У-ПК-2, З-ПК-3, У-ПК-3
2	Второй раздел	9-16	4/12/0		25	КИ-16	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-

							ОПК-2, У-ОПК-2, В-ОПК-2, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 3 Семестр		8/24/0		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ПК-2, У-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3

* – 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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	3 Семестр	8	24	0
1-8	**Первый раздел**	4	12	0
1 - 2	**Тема 1. Общие вопросы по недекларированным возможностям, электронной компонентной базе, важные особенности и характеристики изделий электроники, применяемые для испытаний** Понятия: электроника, полупроводники, диэлектрики, металлы, электронная компонентная база, планарная технология изготовления микроэлектроники, диод, транзистор, микросхема интегральная, электронный модуль, радиоэлектронная аппаратура, гибридная микросхема, многокристальный модуль, корпус изделия ЭКБ, аналоговая и цифровая электроника	Всего аудиторных часов 1 Онлайн 0	2 0	0 0
3 - 4	**Тема 2. Основные общие правовые и практические вопросы, связанные с разработкой, применением и сертификацией ЭКБ** Понятия: головные научно-исследовательские организации в области разработки и применения ЭКБ, категории качества ЭКБ, порядок сертификации ЭКБ различных категорий качества, военное представительство, представитель заказчика, маркировка ЭКБ, особые знаки в маркировке, технические условия и datasheet, сопроводительная документация, источники доверенной информации признаков аутентичности ЭКБ	Всего аудиторных часов 1 Онлайн 0	2 0	0 0
5 - 6	**Тема 3. Угроза контрафакта в целом, мировые тенденции роста доли поддельных изделий. Угрозы объектам критической информационной инфраструктуры от применения контрафактных изделий ЭКБ включая известные** Понятия: контрафакт, признаки контрафакта, доля контрафакта в мировом рынке ЭКБ, известные случаи отказа американской военной и космической техники из-за контрафактных ЭКБ, источники поддельных ЭКБ, примеры выявленных контрафактных изделий, нормативные документы по контрафакту ЭКБ, классификация методов выявления поддельных и подозрительных изделий, обратное проектирование	Всего аудиторных часов 1 Онлайн 0	4 0	0 0
7 - 8	**Тема 4. Недекларированные возможности ЭКБ** Понятия: недекларированные возможности,	Всего аудиторных часов		

	недокументированные возможности, несанкционированный доступ, саботаж, информативный сигнал, побочные электромагнитные излучения и наводки, основные технические средства и системы, вспомогательные технические средства и системы, электронное устройство негласного получения информации, классификация НДВ по реализации и по функциональному назначению, примеры таких устройств на основе литературных данных	1	4	0
		Онлайн		
		0	0	0
9-16	**Второй раздел**	4	12	0
9 - 11	**Тема 5. Методы исследования ЭКБ для выявления признаков контрафакта по ГОСТ. Основные требования, характеристики установок реализации, последовательность проведения** Понятия: демаскирующие признаки, признаки контрафакта, первичная документация, маркировка, корпус, визуальный контроль, перемаркировка, замена верхнего покрытия корпуса, перешлифовка, проверка с применением растворителей, сканирующий электронный микроскоп, сканирующий акустический микроскоп, рентгеновский аппарат, рентгенологическое исследование, проверка с применением рентгеновской спектроскопии, электрические испытания 1, 2, 3, 4 уровней, декапсуляция, физический анализ	Всего аудиторных часов		
		2	4	0
		Онлайн		
		0	0	0
12 - 16	**Тема 6. Методы испытаний ЭКБ для выявления признаков контрафакта в соответствии с международными стандартами** Понятия: SAE, AS6171, уровни доверия, целевая достоверность аутентичности, уровень выявления испытательной лабораторией признаков контрафакта, подтвержденная достоверность аутентичности. Демаскирующие признаки: корпуса и маркировки, материала выводов, поверхности корпуса, кристалла, несоответствия электрическим нормам или функциональному контролю. Типы контрафакта в том числе специально модифицированное изделие с внесением НДВ с целью реализации НСД и саботажа. Методы выявления контрафакта: общие требования к визуально-оптическому осмотру, общий осмотр партии изделий, детальный осмотр, проверка перемаркировки, проверка обновления поверхности, измерение размеров образца, исследование текстуры поверхности. Не визуально-оптические методы выявления признаков контрафакта.	Всего аудиторных часов		
		2	8	0
		Онлайн		
		0	0	0

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**
	3 Семестр
1 - 2	**Семинар №1:** Первичный анализ состава тренировочного изделия РЭА – идентификация элементов РЭА на основе маркировки корпусов и информационного поиска официальной документации на изделия ЭКБ. Анализ состава и выделение критичных и потенциально интересных для детального анализа элементов
3 - 4	**Семинар №2:** Проверка и обновление базовых знаний в области электроники, схемотехники, принципах конструирования аппаратуры. Разбор тренировочного изделия РЭА
5 - 6	**Семинар №3:** Контроль состава изделия РЭА и составление описи входящих в его состав элементов. Практическое занятие с тренировочным изделием РЭА
7	**Семинар №4:** Подготовка документов для проведения испытаний на выявление признаков контрафакта в ЭКБ: программы-методики испытаний, проекта протокола
8	**Практическое занятие:** Проверка знаний половины семестра. Проведение Контрольной работы №1
9 - 10	**Семинар №5:** Контроль наличия или отсутствия в составе РЭА критичных элементов, которые могут реализовать угрозу НСД или саботажа. Анализ состава РЭА с точки зрения выявления потенциальных НДВ.
11 - 12	**Семинар №6:** Проведение аутентификации ЭКБ изделия РЭА методами ГОСТ
13 - 14	**Семинар №7:** Проведение аутентификации ЭКБ изделия РЭА методами международных стандартов SAE
15	**Семинар №8:** Оценка подтвержденной достоверности аутентичности ЭКБ, по результатам испытаний комплексом методов.
16	**Практическое занятие:** Проверка знаний половины семестра. Проведение Контрольной работы №2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач. 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 выявления недекларированных возможностей в радиоэлектронной аппаратуре. 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 и семинары выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл семинаров по отработке методов выявления недекларированных возможностей и признаков контрафакта, проводится в специализированных испытательных лабораториях с предварительной настройкой необходимого оборудования. Для проведения цикла семинаров выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении семинаров необходимо отрабатывать задания, в том числе с обсуждением домашнего задания.

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 семинарах.

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-1	З-ОПК-1	Э, КИ-8, КИ-16
	У-ОПК-1	Э, КИ-8, КИ-16
	В-ОПК-1	Э, КИ-16
ОПК-2	З-ОПК-2	Э, КИ-8, КИ-16
	У-ОПК-2	Э, КИ-8, КИ-16
	В-ОПК-2	Э, КИ-16
ПК-2	З-ПК-2	Э, КИ-8, КИ-16
	У-ПК-2	Э, КИ-8, КИ-16

	В-ПК-2	КИ-16
ПК-3	З-ПК-3	Э, КИ-8, КИ-16
	У-ПК-3	Э, КИ-8, КИ-16
	В-ПК-3	Э, 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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

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

2. ЭИ П 30 Защита персональных данных в информационных системах. Практикум : учебное пособие, Санкт-Петербург: Лань, 2021

3. ЭИ П 84 Информационная безопасность и защита информации : учебное пособие, Санкт-Петербург: Лань, 2021

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

5. ЭИ Л 14 Сертификация информационных систем : учебное пособие, Санкт-Петербург: Лань, 2020

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 О-75 Основы управления информационной безопасностью Кн.1, Москва: Горячая линия - Телеком, 2018

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

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 - Комплексная защита объектов информатизации, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования

образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР16 - 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 не аттестации хотя бы по одному из разделов, студент не допускается к зачету.

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 - Комплексная защита объектов информатизации, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КЛР8, КЛР16 - 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 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 выявления недекларированных возможностей в радиоэлектронной аппаратуре. 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 и семинары выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл семинаров по отработке методов выявления недекларированных возможностей и признаков контрафакта, проводится в специализированных испытательных лабораториях с предварительной настройкой необходимого оборудования. Для проведения цикла семинаров выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении семинаров необходимо отрабатывать задания, в том числе с обсуждением домашнего задания.

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 семинарах.

Особенности изучения разделов дисциплины

Учебная дисциплина «Методы выявления недекларированных возможностей в радиоэлектронной аппаратуре» может быть охарактеризована как прикладная дисциплина технической направленности, является достаточно сложной, поскольку требует хорошей физико-математической подготовки. Необходимо глубокое знание смежных дисциплин специализации.

В процессе изучения данной программы 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).

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

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):

Кессаринский Леонид Николаевич, к.т.н.

Рецензент(ы):

Дураковский А.П.