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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Рабочая программа дисциплины
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.26**
Трудоемкость в зачетных единицах:	**6 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**6 семестр - 20 часов;**
Практические занятия	**6 семестр - 24 часа;**
Лабораторные работы	**6 семестр - 12 часов;**
Консультации	**6 семестр - 2 часа;**
Самостоятельная работа	**6 семестр - 157,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Лабораторная работа** **Творческая задача**	
Промежуточная аттестация:	
Экзамен	**6 семестр - 0,5 часа;**

Москва 2021

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Рыжиков С.С. Идентификатор: R6eeae99e-RyzhikovSS-b1299f04	С.С. Рыжиков
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Освоение общекультурных и профессиональных компетенций, заключающихся в формировании общей готовности студентов к выполнению отдельных мероприятий информационной безопасности применением технических средств защиты информации, а также способности реализовывать техническую защиту информации в интересах обеспечения безопасности хозяйствующего субъекта на основе системного подхода

Задачи дисциплины

- Получение студентами знаний и практических навыков в области комплексной защиты объектов информатизации на основе изучения организационных и технических мер защиты информации, технических средств защиты информации, показателей эффективности защиты и методов их оценки, а также основных руководящих, методических и нормативных документов по инженерно-технической защите информации.

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

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ОПК-4.4 способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ИД-1$_{ОПК-4.4}$ Выполняет обнаружение и идентификацию инцидентов в процессе эксплуатации автоматизированной системы	знать: - перечень, основное содержание и сущность методических и нормативных документов по защите информации. уметь: - оценивать эффективность технических средств защиты информации.
ОПК-4.4 способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ИД-2$_{ОПК-4.4}$ Оценивает защищенность автоматизированных систем с помощью типовых программных средств	знать: - назначение, общую характеристику и принципы работы технических средств защиты информации. уметь: - определять рациональные организационно-режимные меры и технические средства защиты на объектах.
ОПК-4.4 способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ИД-3$_{ОПК-4.4}$ Выполняет инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах	знать: - назначение и порядок проведения инструментального контроля эффективности защиты информации. уметь: - контролировать эффективность мер инженерно-технической защиты информации.
ОПК-11 способен проводить эксперименты по заданной методике и обработку их результатов	ИД-1$_{ОПК-11}$ Проводит эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	знать: - классификацию, общую характеристику и порядок применения технических средств защиты информации, показателей эффективности защиты и методы их

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		оценки. уметь: - разрабатывать технические решения по защите объектов информатизации на основе использования технических средств защиты информации.
ОПК-11 способен проводить эксперименты по заданной методике и обработку их результатов	ИД-2$_{ОПК-11}$ Принимает участие в проведении экспериментальных исследований системы защиты информации	знать: - содержание принципов и основ проведения технического контроля защищенности объектов информатизации. уметь: - организовывать проведение и сопровождение аттестации объекта защиты на соответствие требованиям нормативных документов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Способы и технические средства защиты конфиденциальной информации	50	6	4	4	6	-	-	-	-	-	36	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Способы и технические средства защиты конфиденциальной информации" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Способы и технические средства защиты конфиденциальной информации" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Способы и технические средства защиты конфиденциальной информации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Способы и технические средства защиты конфиденциальной информации" ***Изучение материалов литературных***
1.1	Введение	16		1	1	2	-	-	-	-	-	12	-	
1.2	Тема 1	16		1	1	2	-	-	-	-	-	12	-	
1.3	Тема 2	18		2	2	2	-	-	-	-	-	12	-	

														источников: [4], 8-23 [5], 9-25
2	Защита информации техническими средствами в организации	82		12	6	12	-	-	-	-	-	52	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Защита информации техническими средствами в организации"
2.1	Тема 3	13		2	1	2	-	-	-	-	-	8	-	***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Защита информации техническими средствами в организации" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Защита информации техническими средствами в организации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты:
2.2	Тема 4	13		2	1	2	-	-	-	-	-	8	-	
2.3	Тема 5	13		2	1	2	-	-	-	-	-	8	-	
2.4	Тема 6	13		2	1	2	-	-	-	-	-	8	-	
2.5	Тема 7	15		2	1	2	-	-	-	-	-	10	-	
2.6	Тема 8	15		2	1	2	-	-	-	-	-	10	-	

														Подготовка к практическим занятиям: Изучение материала по разделу "Защита информации техническими средствами в организации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Защита информации техническими средствами в организации" ***Изучение материалов литературных источников:*** [3], 10-23
3	Принципы оценки эффективности системы инженерно-технической защиты информации	48		4	2	6	-	-	-	-	-	36	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Принципы оценки эффективности системы инженерно-технической защиты информации"
3.1	Тема 9	23		2	1	2	-	-	-	-	-	18	-	***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Принципы оценки эффективности системы инженерно-технической защиты информации" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Принципы оценки эффективности системы инженерно-технической защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и
3.2	Тема 10	25		2	1	4	-	-	-	-	-	18	-	

														разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***<u>Подготовка доклада, выступления:</u>*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***<u>Подготовка к контрольной работе:</u>*** Изучение материалов по разделу Принципы оценки эффективности системы инженерно-технической защиты информации и подготовка к контрольной работе ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Принципы оценки эффективности системы инженерно-технической защиты информации" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Принципы оценки эффективности системы инженерно-технической защиты информации" ***<u>Изучение материалов литературных источников:</u>*** [1], 179-186 [2], 60-88
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**216.0**		**20**	**12**	**24**	**-**	**2**	**-**	**-**	**0.5**	**124**	**33.5**	
	Итого за семестр	**216.0**		**20**	**12**	**24**	**2**		**-**		**0.5**	**157.5**		

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

3.2 Краткое содержание разделов

1. Способы и технические средства защиты конфиденциальной информации

1.1. Введение

Предмет, цели, задачи, содержание и структура дисциплины «Защита информации от утечки по техническим каналам». Базовые знания, необходимые для изучения курса. Виды и формы отчетности. Связь курса с другими дисциплинами. Структура курса Рекомендуемые учебные пособия основной и дополнительной литературы по дисциплине..

1.2. Тема 1

Общие положения защиты информации техническими средствами. Задачи и требования к способам и средствам защиты конфиденциальной информации техническими средствами. Классификация способов и технических средств защиты информации. Физическая защита информации и ее методы. Методы скрытия информации. Зависимость качества информации от соотношения сигнал/шум. Методы энергетического скрытия сигналов..

1.3. Тема 2

Способы и технические средства инженерной защиты объектов информатизации. Структура системы физической защиты информации. Классификация средств подсистем предупреждения, обнаружения, ликвидации угроз и управления. Естественные и искусственные преграды инженерной защиты. Показатели эффективности инженерной защиты. Способы управления системами физической защиты. Основные средства инженерной защиты информации (заборы, окна, двери, ограждения зданий и помещений, металлические шкафы, сейфы и хранилища) и показатели их защищенности от злоумышленника..

2. Защита информации техническими средствами в организации

2.1. Тема 3

Характеристика основ организации защиты объектов информатизации в организации. Общие требования, предъявляемые к защите информации от технических средств разведки в организации. Классификация видов документов нормативно-правовой базы по защите информации. Руководящие и нормативные документы по организации инженерно-технической защиты, их состав, сущность и основная направленность на уровне государства, ведомства и организации. Состав основных документов нормативно-методической базы, обеспечивающей организацию инженерно-технической защиты информации на предприятии. Краткое содержание положений основных руководящих и нормативных документов государственного и межведомственного уровней. Краткое содержание нормативно-методических документов регламентирующих организацию инженерно-технической защиты информации на предприятии, порядок их разработки и использования..

2.2. Тема 4

Мероприятия технической защиты объектов информации. Основные направления организации защиты объектов информации в организациях. Состав и сущность организационно-технических и технических мер по защите информации в организации. Виды контроля эффективности инженерно-технической защиты информации. Особенности контроля эффективности защиты информации технологических процессов. Меры технического контроля эффективности защиты информации. Характеристика содержания основных организационно-технических мероприятий, определения контролируемых зон и оптимального количества технических средств (ОТСС и ВТСС). Содержание основных технических мероприятий инженерно-технической защиты информации основанных на

использовании способов защиты объекта путем скрытия его демаскирующего признака или технической дезинформации путем искажения технических демаскирующих признаков. Содержание и порядок использования мероприятий по контролю эффективности защиты информации..

2.3. Тема 5

Способы и средства защиты каналов утечки информации. Пассивные и активные методы и способы защиты каналов утечки информации. Методы и способы защиты информации обрабатываемой в ТСПИ. Средства ослабления ПЭМИ ТСПИ и их наводок. Акустическая защита защищаемого помещения. Защита пассивными средствами защищаемых помещений. Аппаратура и способы активной защиты помещений от утечки речевой информации. Способы предотвращения несанкционированной записи речевой информации на диктофон..

2.4. Тема 6

Способы и технические средства обнаружения (поиска) каналов утечки информации. Способы и средства предотвращения утечки информации с помощью закладных устройств. Классификация технических средств обнаружения (поиска) каналов утечки информации. Технические средства физического поиска каналов утечки информации. Технические средства инструментального (технического) контроля каналов утечки информации. Способы и средства визуального осмотра помещений. Способы и средства обнаружения (поиска) каналов утечки информации за счет ПЭМИН. и порядок применения. Принципы работы нелинейных локаторов. Типы и характеристики отечественных и зарубежных локаторов. Физические принципы работы и способы применения обнаружителей пустот, для выявления закладных устройств..

2.5. Тема 7

Специальные проверки. Порядок проведения специальной проверки технических средств. Специальные обследования. Подготовка к проведению специальных обследований. Оценка условий, в которых решается задача выявления технических каналов утечки информации. Порядок и последовательность решения проблемы поисковой операции. Выполнение поисковых мероприятий, радиообнаружение. Проверка проводных коммуникаций. Подготовка отчетных материалов. Специальные исследования. Общие положения, термины и определения в области специальных исследований. Порядок постановки задачи на выполнение специальных исследований по выявлению и измерению опасных сигналов в каналах возможной утечки информации. Специальные исследования в области защиты речевой информации. Специальные исследования в области акустоэлектрических преобразователей. Специальные исследования в области защиты цифровой информации. Специальные исследования побочных электромагнитных излучений и наводок..

2.6. Тема 8

Способы и средства предотвращения утечки информации по материально-вещественному каналу. Способы предотвращения утечки информации по материально-вещественному каналу. Технические средства защиты и экстренного уничтожения информации на бумажных носителях. Технические средства защиты и экстренного уничтожения информации на машинных носителях..

3. Принципы оценки эффективности системы инженерно-технической защиты информации

3.1. Тема 9

Моделирование защиты информации. Методы организации системы защиты информации на предприятии. Виды моделей системы защиты информации и показатели эффективности. Рекомендации по выбору рациональных вариантов защиты информации и соответствующих средств. Формы представления результатов моделирования..

3.2. Тема 10

Методические рекомендации по разработке мер защиты информации техническими средствами и контроль их эффективности. Типовые рекомендации по выбору мер инженерно-технической защиты информации. Способы оценки значений показателей моделей. Технический контроль эффективности принимаемых мер защиты. Основные средства технического контроля..

3.3. Темы практических занятий

1. 1. Порядок разработки и использования методических документов по технической защите информации. Характеристика содержания основных технических мероприятий, определения контролируемых зон и оптимального количества технических средств - ОТСС и ВТСС;
2. 2. Характеристика содержания основных технических мероприятий инженерно-технической защиты информации основанных на использовании технических средств защиты объекта скрытием его демаскирующего признака. Характеристика содержания основных технических мероприятий основанных на использовании способов защиты технической дезинформации и искажения технических демаскирующих признаков. Характеристика основ технического контроля эффективности мер инженерно-технической защиты информации;
3. 3. Классификация методов и технических средств защиты информации. Назначение, состав и характеристика способов и средств инженерной защиты. Назначение, состав и характеристика способов и технических средств обнаружения (поиска) каналов утечки информации. Назначение, принципы работы и порядок использования технических средств визуального поиска закладных устройств и за счет выявления побочного электромагнитного излучения;
4. 4. Назначение, принципы работы и порядок использования технических средств обнаружения радиоизлучающих средств негласного съема информации. Назначение, принципы работы и порядок использования технических средств обнаружения неизлучающих средств негласного съема информации. Назначение, принципы работы и порядок использования технических средств защиты информации обрабатываемой ТСПИ;
5. 5. Способы и средства защиты информации, обрабатываемой в телефонных аппаратах, циркулирующей в двухпроводных линиях и каналах связи. Назначение, принципы работы и порядок использования технических средств защиты акустической информации в защищаемых помещениях. Назначение, классификация и характеристика основных технических средств используемых для предотвращения утечки информации по материально-вещественному каналу;
6. 6. Организация и порядок выполнения мероприятий по выявлению каналов утечки информации на основе проведения специальных исследований в области акустоэлектрических преобразований. Состав и основное содержание требований положений основных руководящих, нормативных и методических документов государственного и межведомственного уровней по организации защиты информации на основе использования технических средств защиты информации. Состав и основное содержание требований положений основных руководящих и методических документов регламентирующих порядок и организацию применения технических средств защиты информации в организации;

7. 7. Организация и порядок выполнения мероприятий по выявлению каналов утечки информации на основе проведения специальных исследований в области защиты цифровой информации. Организация и порядок выполнения мероприятий по выявлению каналов утечки информации на основе проведения специальных исследований в области ВЧ-навязывания, ВЧ-облучения и защиты волоконно-оптических линий передачи;
8. 8. Формирование основных документов создаваемых при подготовке и проведении аттестации объекта защиты на соответствие его требованиям безопасности информации и разработке итогового документа «Аттестата соответствия». Методические рекомендации по моделированию угроз и технических каналов утечки информации. Практическая разработка предложений по выбору и размещению технических средств охраны;
9. 9. Практическая разработка типовых вариантов решений по предотвращению утечки информации за счет побочных электромагнитных излучений и наводок;
10. 10. Практическое занятие по оценке вариантов предложенных решений по предотвращению утечки информации за счет побочных электромагнитных излучений и наводок;
11. 11. Практическая разработка предложений по защите информации в кабинете руководителя;
12. 12. Практическое занятие по оценке вариантов предложенных решений по защите информации в кабинете руководителя.

3.4. Темы лабораторных работ

1. Лабораторная работа № 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля;
2. Лабораторная работа № 6. Методы защиты конфиденциальной информации, обрабатываемой в ПЭВМ, от утечки по каналу побочных излучений;
3. Лабораторная работа № 2. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому каналу;
4. Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу;
5. Лабораторная работа № 4. Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ»;
6. Лабораторная работа № 5. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях.

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Способы и технические средства защиты конфиденциальной информации"
2. Обсуждение материалов по кейсам раздела "Защита информации техническими средствами в организации"
3. Обсуждение материалов по кейсам раздела "Принципы оценки эффективности системы инженерно-технической защиты информации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Способы и технические средства защиты конфиденциальной информации"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Защита информации техническими средствами в организации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Принципы оценки эффективности системы инженерно-технической защиты информации"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)			Оценочное средство (тип и наименование)
		1	2	3	
Знать:					
перечень, основное содержание и сущность методических и нормативных документов по защите информации	ИД-1$_{ОПК-4.4}$		+		Лабораторная работа/Лабораторная работа № 5. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. Лабораторная работа № 6. Методы защиты конфиденциальной информации, обрабатываемой в ПЭВМ, от утечки по каналу побочных излучений
назначение, общую характеристику и принципы работы технических средств защиты информации	ИД-2$_{ОПК-4.4}$			+	Творческая задача/Защита предложенных вариантов решений по защите информации в кабинете руководителя
назначение и порядок проведения инструментального контроля эффективности защиты информации	ИД-3$_{ОПК-4.4}$		+		Лабораторная работа/Лабораторная работа № 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля. Лабораторная работа № 4. Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ»
классификацию, общую характеристику и порядок применения технических средств защиты информации, показателей эффективности защиты и методы их оценки	ИД-1$_{ОПК-11}$	+			Лабораторная работа/Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу. Лабораторная работа № 2. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому каналу
содержание принципов и основ проведения технического контроля защищенности объектов информатизации	ИД-2$_{ОПК-11}$		+		Лабораторная работа/Лабораторная работа № 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля. Лабораторная работа № 4. Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса

					обнаружения радиоизлучающих средств «Крона НМ»
Уметь:					
оценивать эффективность технических средств защиты информации	ИД-1$_{ОПК-4.4}$			+	Творческая задача/Защита предложенных вариантов решений по защите информации в кабинете руководителя
определять рациональные организационно-режимные меры и технические средства защиты на объектах	ИД-2$_{ОПК-4.4}$	+			Лабораторная работа/Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу. Лабораторная работа № 2. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому каналу
контролировать эффективность мер инженерно-технической защиты информации	ИД-3$_{ОПК-4.4}$		+		Лабораторная работа/Лабораторная работа № 5. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. Лабораторная работа № 6. Методы защиты конфиденциальной информации, обрабатываемой в ПЭВМ, от утечки по каналу побочных излучений
разрабатывать технические решения по защите объектов информатизации на основе использования технических средств защиты информации	ИД-1$_{ОПК-11}$	+			Лабораторная работа/Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу. Лабораторная работа № 2. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому каналу
организовывать проведение и сопровождение аттестации объекта защиты на соответствие требованиям нормативных документов	ИД-2$_{ОПК-11}$		+		Лабораторная работа/Лабораторная работа № 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля. Лабораторная работа № 4. Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ»

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

4.1. Текущий контроль успеваемости

6 семестр

Форма реализации: Выполнение задания

1. Защита предложенных вариантов решений по защите информации в кабинете руководителя (Творческая задача)

Форма реализации: Защита задания

1. Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу. Лабораторная работа № 2. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому каналу (Лабораторная работа)
2. Лабораторная работа № 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля. Лабораторная работа № 4. Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ» (Лабораторная работа)
3. Лабораторная работа № 5. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. Лабораторная работа № 6. Методы защиты конфиденциальной информации, обрабатываемой в ПЭВМ, от утечки по каналу побочных излучений (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №6)

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих (проводимого по билетам).

В диплом выставляется оценка за 6 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Зайцев, А. П. Технические средства и методы защиты информации : учебник для вузов по группе специальностей "Информационная безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов . – 7-е изд . – М. : Горячая Линия-Телеком, 2012 . – 442 с. - ISBN 978-5-9912-0233-6 .;
2. Халяпин, Д. Б. Инженерно-техническая защита информации. Лабораторный практикум. Ч.1 : учебное пособие для института безопасности бизнеса МЭИ (ТУ) / Д. Б. Халяпин, А. Ю. Невский ; Ред. Л. М. Кунбутаев ; Ин-т безопасности бизнеса МЭИ (ТУ) . – М. : Издательский дом МЭИ, 2009 . – 88 с. - ISBN 978-5-383-00359-6 .

http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=402;
3. Торокин, А. А. Инженерно-техническая защита информации : учебное пособие для вузов по специальностям в области информационной безопасности / А. А. Торокин . – М. : Гелиос АРВ, 2005 . – 960 с. - ISBN 5-85438-140-0 .;
4. Халяпин, Д. Б. Защита информации. Вас подслушивают? Защищайтесь! / Д. Б. Халяпин . – М. : Баярд, 2004 . – 432 с. - ISBN 5-948960-17-X .;
5. А. А. Титов- "Инженерно-техническая защита информации", Издательство: "Томский государственный университет систем управления и радиоэлектроники", Томск, 2010 - (195 с.)
https://biblioclub.ru/index.php?page=book&id=208567.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

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

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор,

		экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Учебные аудитории для проведения практических занятий, КР и КП	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения лабораторных занятий	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам

(название дисциплины)

6 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу. Лабораторная работа № 2. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому каналу (Лабораторная работа)

КМ-2 Лабораторная работа № 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля. Лабораторная работа № 4. Организация и проведение радиомониторинга с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ» (Лабораторная работа)

КМ-3 Лабораторная работа № 5. Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. Лабораторная работа № 6. Методы защиты конфиденциальной информации, обрабатываемой в ПЭВМ, от утечки по каналу побочных излучений (Лабораторная работа)

КМ-4 Защита предложенных вариантов решений по защите информации в кабинете руководителя (Творческая задача)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Способы и технические средства защиты конфиденциальной информации					
1.1	Введение		+			
1.2	Тема 1		+			
1.3	Тема 2		+			
2	Защита информации техническими средствами в организации					
2.1	Тема 3			+	+	
2.2	Тема 4			+	+	
2.3	Тема 5			+	+	
2.4	Тема 6			+	+	

2.5	Тема 7		+	+	
2.6	Тема 8		+	+	
3	Принципы оценки эффективности системы инженерно-технической защиты информации				
3.1	Тема 9				+
3.2	Тема 10				+
	Вес КМ, %:	25	25	25	25