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 компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Базовая**
№ дисциплины по учебному плану:	**Б1.Б.23**
Трудоемкость в зачетных единицах:	**5 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**5 семестр - 32 часа;**
Практические занятия	**5 семестр - 32 часа;**
Лабораторные работы	**5 семестр - 16 часов;**
Консультации	**5 семестр - 2 часа;**
Самостоятельная работа	**5 семестр - 133,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет**	
Промежуточная аттестация:	
Экзамен	**5 семестр - 0,5 часа;**

Москва 2018

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 мероприятий информационной безопасности по применению методов, способов и средств технической защиты информации.

Задачи дисциплины

- изучение теоретических основ технической защиты информации, а также технических каналов утечки информации;
- формирование готовности и способности обеспечить выявление угроз безопасности информации на объектах информатизации;
- приобретение навыков системного подхода к применению методов, способов и средств технической защиты информации и моделированию систем технической защиты 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**
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		знать: - возможности, классификацию и технические характеристики технических каналов утечки информации; - классификацию и степень актуальности угроз безопасности информации; - перечень и характеристику основных демаскирующие признаков объектов защиты и носителей информации; - особенности информации, как предмета технической защиты, классификацию и общую характеристику основных источников и носителей защищаемой информации.
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		уметь: - выявлять технические каналы утечки информации на конкретных объектах и оценивать их возможности; - выявлять и оценивать актуальность угроз безопасности информации на конкретных объектах.
ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности		знать: - методы оценки уровня угрозы на объектах защиты информации; - методы, способы и средства выявления технических каналов утечки информации.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
информации		
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов		знать: - нормативные и методические документы, необходимые для оформления технической документации. уметь: - оформлять техническую документацию.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации		знать: - способы проведения экспериментальных исследований. уметь: - проводить экспериментальные исследования системы защиты информации.
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		знать: - принципы, способы и средства добывания информации; - общие теоретические основы технической защиты информации в обеспечении информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к обязательной части блока дисциплин основной профессиональной образовательной программе Безопасность компьютерных 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	Теоретические основы технической защиты информации	35	5	6	3	6	-	-	-	-	-	20	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Теоретические основы технической защиты информации" подготовка к выполнению заданий на практических занятиях ***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: ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***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 "Теоретические основы технической защиты информации" материалу. ***Проведение исследований:*** Работа выполняется по индивидуальному заданию. Для проведения исследования применяется
1.1	Введение	11		2	1	2	-	-	-	-	-	6	-	
1.2	Тема 1. Общие положения технической защиты информации	11		2	1	2	-	-	-	-	-	6	-	
1.3	Тема 2. Особенности информации, как предмета технической защиты	13		2	1	2	-	-	-	-	-	8	-	

														следующие материалы: ***Подготовка к текущему контролю:*** Повторение материала по разделу "Теоретические основы технической защиты информации" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Теоретические основы технической защиты информации" ***Изучение материалов литературных источников:*** [1], 1-528 [2], 8-23
2	Технические каналы утечки информации	38		6	4	6	-	-	-	-	-	22	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Технические каналы утечки информации" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Технические каналы утечки информации" подготовка к выполнению заданий на практических занятиях ***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: ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а
2.1	Тема 3. Понятие, назначение и классификация технических каналов утечки информации	7		1	1	1	-	-	-	-	-	4	-	
2.2	Тема 4. Технические каналы утечки речевой информации	9		1	1	1	-	-	-	-	-	6	-	
2.3	Тема 5. Технические каналы утечки информации при ее передаче по каналам связи	11		2	1	2	-	-	-	-	-	6	-	
2.4	Тема 6. Технические каналы утечки видовой информации. Материально-вещественный канал утечки информации.	11		2	1	2	-	-	-	-	-	6	-	

														так же изучить вопросы вариантов обработки результатов по изученному в разделе "Технические каналы утечки информации" материалу. ***Подготовка к текущему контролю:*** Повторение материала по разделу "Технические каналы утечки информации" ***Изучение материалов литературных источников:*** [2], 25-105 [3], 2-23 [6], 373-396
3	Принципы, способы и средства добывания информации	57		10	5	10	-	-	-	-	-	32	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Принципы, способы и средства добывания информации" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Принципы, способы и средства добывания информации" подготовка к выполнению заданий на практических занятиях ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***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, способы и средства добывания информации" материалу. ***Проведение исследований:*** Работа выполняется по индивидуальному заданию. Для проведения исследования применяется следующие материалы: ***Подготовка к текущему контролю:*** Повторение материала по разделу
3.1	Тема 7. Способы и средства добывания информации техническими средствами	11		2	1	2	-	-	-	-	-	6	-	
3.2	Тема 8. Способы и средства наблюдения	13		2	1	2	-	-	-	-	-	8	-	
3.3	Тема 9. Технические средства перехвата радио и электрических сигналов	13		2	1	2	-	-	-	-	-	8	-	
3.4	Тема 10. Способы и средства подслушивания акустических сигналов	20		4	2	4	-	-	-	-	-	10	-	

														"Принципы, способы и средства добывания информации" ***Изучение материалов литературных источников:*** [2], 124-176 [3], 57-122 [4], 1-88 [5], 1-505
4	Системный подход к обеспечению защиты информации	50		10	4	10	-	-	-	-	-	26	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Системный подход к обеспечению защиты 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 "Системный подход к обеспечению защиты информации" материалу. ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Системный подход к обеспечению защиты информации" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Системный подход к обеспечению защиты информации" подготовка к выполнению заданий на практических занятиях ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Изучение материалов литературных источников:*** [3], 126-158
4.1	Тема 11. Основы системного подхода к защите информации	22		4	2	4	-	-	-	-	-	12	-	
4.2	Тема 12. Моделирование объектов защиты и каналов утечки информации	28		6	2	6	-	-	-	-	-	14	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**216.0**		**32**	**16**	**32**	-	**2**	-	-	**0.5**	**100**	**33.5**	
	Итого за семестр	**216.0**		**32**	**16**	**32**	**2**		**-**		**0.5**	**133.5**		

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. Теоретические основы технической защиты информации

1.1. Введение

Место технической защиты информации в обеспечении информационной безопасности. Предмет, цели, задачи, содержание и структура дисциплины техническая защита информации (ТЗИ). Базовые знания, необходимые для изучения курса. Виды и формы отчетности. Рекомендуемые учебные пособия основной и дополнительной литературы по дисциплине..

1.2. Тема 1. Общие положения технической защиты информации

Особенности задач технической защиты информации. Основные параметры системы ТЗИ. Представление сил и средств технической защиты информации в виде системы технической защиты информации. Цели и задачи технической защиты информации. Понятие о безопасности информации. Затраты на информацию. Ресурсы системы. Меры технической защиты информации. Процесс преобразования входов в выходы. Критерии эффективности мер технической защиты информации. Основные направления организации технической защиты информации..

1.3. Тема 2. Особенности информации, как предмета технической защиты

Демаскирующие признаки объектов и их классификация. Информативность. Понятие признаковой структуры. Видовые, сигнальные и вещественные демаскирующие признаки. Демаскирующие объекты, сигналы и вещества. Носители информации. Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства, и системы как источники сигналов. Источники случайных опасных сигналов. Пути распространения опасных сигналов из помещения. Классификация побочных электромагнитных излучений и наводок. Виды акустоэлектрических преобразователей и их параметры. Побочные низкочастотные излучения и их источники. Источники высокочастотных побочных излучений. Условия возникновения паразитной генерации в усилителях. Способы высокочастотного навязывания. Сосредоточенные и распределенные источники электромагнитного поля. Понятие ближней и дальней зон. Характер распространения электромагнитных полей сосредоточенных источников в ближней и дальней зонах. Виды излучений распределенных источников электромагнитного поля. Понятие о цепях Пикара. Виды паразитных связей. Факторы, вызывающие проникновению опасных сигналов в цепи электропитания и заземления..

2. Технические каналы утечки информации

2.1. Тема 3. Понятие, назначение и классификация технических каналов утечки информации

Понятие технического канала утечки информации. Простые и составные каналы утечки информации. Структура и основные показатели технических каналов утечки информации (общая схема образования каналов утечки информации). Классификация технических каналов утечки информации в зависимости от источника конфиденциальной информации (объекта защиты). Характеристика первоочередных источников, образующих каналы утечки информации и воздействия на информацию. Каналы утечки информации из технических систем и средств передачи, обработки, хранения и отображения информации. Виды технических каналов утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации..

2.2. Тема 4. Технические каналы утечки речевой информации

Характеристика акустических сигналов технических каналов утечки информации. Основные физические характеристики акустических волн. Параметры речевого сигнала (речевой информации). Понятность и разборчивость речи. Метод артикуляции. Акустический и виброакустический каналы утечки информации, принципы подслушивания речевой информации. Структура акустического канала утечки информации. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации. Особенности акустоэлектрических каналов утечки информации. Назначение, устройство и общая характеристика акустоэлектрических преобразователей. Технические характеристики акустоэлектрического канала утечки информации. Оптико-электронный технический канал утечки акустической информации. Параметрический технический канал утечки акустической информации..

2.3. Тема 5. Технические каналы утечки информации при ее передаче по каналам связи

Средства передачи электрических сигналов. Напряженность электрического и магнитного полей в пространстве. Электрическое поле. Магнитное поле. Электромагнитная волна. Проводные линии связи (симметричные, несимметричные, коаксиальные). Электромагнитные каналы утечки информации. Электромагнитные излучения элементов ТСПИ. Электромагнитные излучения на частотах работы генераторов ВЧ ТСПИ и ВТСС. Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Побочные электромагнитные излучения персонального компьютера. Электрические каналы утечки информации. Наводки электромагнитных излучений ТСПИ. Просачивание информационных сигналов в цепи электропитания. Паразитные связи через цепи питания. Просачивание информационных сигналов в цепи заземления. Индукционный съем информации с электрического каналам утечки информации. Параметрический канал утечки информации..

2.4. Тема 6. Технические каналы утечки видовой информации. Материально-вещественный канал утечки информации.

Визуально-оптический канал утечки информации. Особенности визуально-оптических каналов утечки информации. Структура визуально-оптического канала утечки информации. Условия освещенности объектов наблюдения в видимом и ИК-диапазонах в различные периоды времени. Варианты визуально-оптических каналов утечки информации для типовых контролируемых зон организации. Материально-вещественные каналы утечки информации. Особенности материально-вещественных каналов утечки информации. Структура материально-вещественных каналов утечки информации и характеристики ее элементов..

3. Принципы, способы и средства добывания информации

3.1. Тема 7. Способы и средства добывания информации техническими средствами

Типовая структура средства добывания информации. Классификация технических средств добывания по видам носителя информации. Средства обеспечения дистанционного доступа к источникам информации без нарушения контролируемой зоны организации. Классификация и характеристика закладных устройств..

3.2. Тема 8. Способы и средства наблюдения

Структура и основные характеристики средств наблюдения. Основные показатели средств наблюдения. Виды и технические характеристики визуально-оптических приборов, фото- и киноаппаратов..

3.3. Тема 9. Технические средства перехвата радио и электрических сигналов

Способы и средства перехвата сигналов. Задачи решаемые при перехвате сигналов. Типовая структура комплекса средств перехвата радио и электрических сигналов. Виды и характеристики антенн и радиоприемников. Основные функции средств анализа сигналов. Особенности и основные характеристики сканирующих радиоприемников..

3.4. Тема 10. Способы и средства подслушивания акустических сигналов

Типовая структура средства подслушивания. Структура и характеристика технических средств подслушивания. Средства акустической разведки. Классификация и характеристика микрофонов Основные показатели средств подслушивания. Виды микрофонов. Остронаправленные микрофоны. Проводные системы, портативные диктофоны и электронные стетоскопы. Параметрические акустоэлектрические преобразователи. Способы и средства высокочастотного навязывания. Лазерные средства подслушивания. Контроль и прослушивание телефонных каналов связи. Средства снятия речевой информации с телефонной линии. Подслушивающие закладные устройства, их классификация и основные параметры функционирования..

4. Системный подход к обеспечению защиты информации

4.1. Тема 11. Основы системного подхода к защите информации

Сущность системного подхода и системного анализа. Характеристики системы защиты информации. Характеристика системы защиты информации. Частные и глобальные критерии эффективности системы защиты. Понятие о моделировании как основном процессе системного анализа. Виды моделей и их возможности при исследовании проблем защиты информации..

4.2. Тема 12. Моделирование объектов защиты и каналов утечки информации

Сущность моделирования. Структурные, функциональные и информационные модели объектов защиты и каналов утечки информации. Принципы построения комплексных моделей объектов защиты и каналов утечки. Подходы к оценке угрозы каналов утечки безопасности конфиденциальной информации. Методические рекомендации по структурированию защищаемой информации. Выявление и описание источников информации. Формы представления моделей объектов информационной безопасности..

3.3. Темы практических занятий

1. 13. Параметрические акустоэлектрические преобразователи. Способы и средства высокочастотного навязывания. Лазерные средства подслушивания. Подслушивающие закладные устройства, их классификация и основные параметры функционирования.;
2. 12. Характеристика технических средств подслушивания акустических сигналов. Классификация и характеристика микрофонов. Виды микрофонов. Остронаправленные микрофоны. Стетоскопы. Диктофоны. Средства снятия речевой информации с телефонной линии.;
3. 11.Технические средства и способы добывания информации перехватом радио и электрических сигналов. Назначение, классификация и характеристика закладных устройств. Основное предназначение и характеристика технических способов и средств перехвата сигналов.;
4. 10. Технические средства и способы добывания информации наблюдением. Характеристика основных способов и средств наблюдения.;
5. 9. Материально-вещественные каналы утечки информации. Особенности материально-вещественных каналов утечки информации. Структура материально-вещественных каналов утечки информации и характеристики ее элементов.;

6. 8.Характеристика технического канала утечки видовой информации.;
7. 1. Пути распространения опасных сигналов из помещения. Классификация побочных электромагнитных излучений и наводок. Виды акустоэлектрических преобразователей и их параметры. Побочные низкочастотные излучения и их источники. Источники высокочастотных побочных излучений. Условия возникновения паразитной генерации в усилителях. Способы высокочастотного навязывания.;
8. 6.Характеристика радиоэлектронных каналов утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации.;
9. 5. Особенности акустоэлектрических каналов утечки информации. Назначение, устройство и общая характеристика акустоэлектрических преобразователей. Технические характеристики акустоэлектрического канала утечки информации.;
10. 4. Характеристика акустических и виброакустических каналов утечки информации. Структура акустического канала утечки информации. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации.;
11. 3. Характеристика первоочередных источников, образующих каналы утечки информации и воздействия на информацию. Каналы утечки информации из технических систем и средств передачи, обработки, хранения и отображения информации.;
12. 2. Сосредоточенные и распределенные источники электромагнитного поля. Понятие ближней и дальней зон. Характер распространения электромагнитных полей сосредоточенных источников в ближней и дальней зонах. Виды излучений распределенных источников электромагнитного поля. Понятие о цепях Пикара. Виды паразитных связей. Факторы, вызывающие проникновению опасных сигналов в цепи электропитания и заземления.;
13. 14. Моделирование объекта защиты. Порядок выявления и описания источников информации. Разработка модели объекта информационной безопасности.;
14. 7. Характеристика основных показателей оптоэлектронных линий связи и способы снятия с них информации.;
15. 15. Порядок моделирования технических каналов утечки информации..

3.4. Темы лабораторных работ

1. 5. Лабораторная работа №5. Тема: Исследование электромагнитного канала утечки информации за счет наводок на линии и коммуникации, выходящие за пределы контролируемой зоны.;
2. 4. Лабораторная работа №4. Тема: Исследование электромагнитного канала утечки информации из средств вычислительной техники.;
3. 3. Лабораторная работа №3. Тема: Исследование акустоэлектрического канала утечки речевой конфиденциальной информации.;
4. 2. Лабораторная работа №2. Тема: Исследование виброакустического канала утечки речевой конфиденциальной информации.;
5. 1. Лабораторная работа № 1. Тема: Исследование воздушного акустического канала утечки речевой конфиденциальной информации..

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Теоретические основы технической защиты информации"

2. Обсуждение материалов по кейсам раздела "Технические каналы утечки информации"
3. Обсуждение материалов по кейсам раздела "Принципы, способы и средства добывания информации"
4. Обсуждение материалов по кейсам раздела "Системный подход к обеспечению защиты информации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Теоретические основы технической защиты информации"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Технические каналы утечки информации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Принципы, способы и средства добывания информации"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Системный подход к обеспечению 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	4	
Знать:						
особенности информации, как предмета технической защиты, классификацию и общую характеристику основных источников и носителей защищаемой информации	ПК-1(Компетенция)			+		Отчет/Тестирование: тест №3, тест №4; Защита лабораторной работы №4
перечень и характеристику основных демаскирующие признаков объектов защиты и носителей информации	ПК-1(Компетенция)				+	Отчет/Контрольная работа №2; Защита лабораторной работы №5
классификацию и степень актуальности угроз безопасности информации	ПК-1(Компетенция)		+			Отчет/Контрольная работа №1; Защита лабораторной работы №2; Защита лабораторной работы №3
возможности, классификацию и технические характеристики технических каналов утечки информации	ПК-1(Компетенция)	+				Отчет/Тестирование: тест №1, тест №2; Защита лабораторной работы №1
методы, способы и средства выявления технических каналов утечки информации	ПК-5(Компетенция)		+			Отчет/Тестирование: тест №1, тест №2; Защита лабораторной работы №1
методы оценки уровня угрозы на объектах защиты информации	ПК-5(Компетенция)	+				Отчет/Контрольная работа №1; Защита лабораторной работы №2; Защита лабораторной работы №3
нормативные и методические документы, необходимые для оформления технической документации	ПК-8(Компетенция)			+		Отчет/Тестирование: тест №3, тест №4; Защита лабораторной работы №4
способы проведения экспериментальных исследований	ПК-12(Компетенция)				+	Отчет/Контрольная работа №2; Защита лабораторной работы №5
общие теоретические основы технической защиты информации в обеспечении информационной безопасности	ОК-5(Компетенция)			+		Отчет/Тестирование: тест №3, тест №4; Защита лабораторной работы №4
принципы, способы и средства добывания информации	ОК-5(Компетенция)				+	Отчет/Контрольная работа №2; Защита

						лабораторной работы №5
Уметь:						
выявлять и оценивать актуальность угроз безопасности информации на конкретных объектах	ПК-4(Компетенция)	+				Отчет/Тестирование: тест №1, тест №2; Защита лабораторной работы №1
выявлять технические каналы утечки информации на конкретных объектах и оценивать их возможности	ПК-4(Компетенция)		+			Отчет/Контрольная работа №1; Защита лабораторной работы №2; Защита лабораторной работы №3
оформлять техническую документацию	ПК-8(Компетенция)		+			Отчет/Тестирование: тест №3, тест №4; Защита лабораторной работы №4
проводить экспериментальные исследования системы защиты информации	ПК-12(Компетенция)			+	+	Отчет/Контрольная работа №2; Защита лабораторной работы №5

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

4.1. Текущий контроль успеваемости

5 семестр

Форма реализации: Смешанная форма

1. Контрольная работа №1; Защита лабораторной работы №2; Защита лабораторной работы №3 (Отчет)
2. Контрольная работа №2; Защита лабораторной работы №5 (Отчет)
3. Тестирование: тест №1, тест №2; Защита лабораторной работы №1 (Отчет)
4. Тестирование: тест №3, тест №4; Защита лабораторной работы №4 (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №5)

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

В диплом выставляется оценка за 5 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Тихонов, В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты : учебное пособие для вузов по специальностям в области информационной безопасности / В. А. Тихонов, В. В. Райх . – М. : Гелиос АРВ, 2006 . – 528 с. - ISBN 5-85438-153-2 .;
2. 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 .;
3. Бузов, Г. А. Защита от утечки информации по техническим каналам : учебное пособие для подготовки экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев . – М. : Горячая Линия-Телеком, 2005 . – 416 с. - ISBN 5-935172-04-6 .;
4. 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;
5. Белов, П. Г. Системный анализ и моделирование опасных процессов в техносфере : Учебное пособие для вузов по направлению 656500 "Безопасность жизнедеятельности" специальность 330100 "Безопасность жизнедеятельности в техносфере" / П. Г. Белов . – М. :

АКАДЕМИЯ, 2003 . – 505 с. – (Высшее профессиональное образование) . - ISBN 5-7695-1039-0 .;
6. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А.- "Технические средства и методы защиты информации", (7-е изд., испр.), Издательство: "Горячая линия-Телеком", Москва, 2018 - (442 с.)
https://e.lanbook.com/book/111057.

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. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
7. **Портал открытых данных Российской Федерации** - https://data.gov.ru
8. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
9. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
10. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
11. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
12. **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	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-504/1, Учебная аудитория	парта, стол преподавателя, стул, доска маркерная
Учебные аудитории для проведения лабораторных занятий	М-504/1, Учебная аудитория	парта, стол преподавателя, стул, доска маркерная
Учебные аудитории для	М-504/1, Учебная	парта, стол преподавателя, стул, доска

проведения промежуточной аттестации	аудитория	маркерная
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
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	М-504/1, Учебная аудитория	парта, стол преподавателя, стул, доска маркерная
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

Техническая защита информации

(название дисциплины)

5 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Тестирование: тест №1, тест №2; Защита лабораторной работы №1 (Отчет)

КМ-2 Контрольная работа №1; Защита лабораторной работы №2; Защита лабораторной работы №3 (Отчет)

КМ-3 Тестирование: тест №3, тест №4; Защита лабораторной работы №4 (Отчет)

КМ-4 Контрольная работа №2; Защита лабораторной работы №5 (Отчет)

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	Теоретические основы технической защиты информации					
1.1	Введение		+	+		
1.2	Тема 1. Общие положения технической защиты информации		+	+		
1.3	Тема 2. Особенности информации, как предмета технической защиты		+	+		
2	Технические каналы утечки информации					
2.1	Тема 3. Понятие, назначение и классификация технических каналов утечки информации		+	+	+	
2.2	Тема 4. Технические каналы утечки речевой информации		+	+	+	
2.3	Тема 5. Технические каналы утечки информации при ее передаче по каналам связи		+	+	+	
2.4	Тема 6. Технические каналы утечки видовой информации. Материально-вещественный канал утечки информации.		+	+	+	
3	Принципы, способы и средства добывания информации					
3.1	Тема 7. Способы и средства добывания информации техническими средствами				+	+
3.2	Тема 8. Способы и средства наблюдения				+	+
3.3	Тема 9. Технические средства перехвата радио и электрических сигналов				+	+
3.4	Тема 10. Способы и средства подслушивания акустических сигналов				+	+

4	Системный подход к обеспечению защиты информации				
4.1	Тема 11. Основы системного подхода к защите информации				+
4.2	Тема 12. Моделирование объектов защиты и каналов утечки информации				+
	Вес КМ, %:	10	30	20	40