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
ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.10**
Трудоемкость в зачетных единицах:	**8 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**8 семестр - 20 часов;**
Практические занятия	**8 семестр - 20 часов;**
Лабораторные работы	**8 семестр - 20 часов;**
Консультации	**8 семестр - 10 часов;**
Самостоятельная работа	**8 семестр - 141,2 часа;**
в том числе на КП/КР	**8 семестр - 15,7 часов;**
Иная контактная работа	**8 семестр - 4 часа;**
включая: **Отчет**	
Промежуточная аттестация:	
Защита курсовой работы **Экзамен**	**8 семестр - 0,3 часа;** **8 семестр - 0,5 часа;** **всего - 0,8 часа**

Москва 2022

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
ПК-4 Способен проводить контроль защищенности информации	ПК-4.1$_{ПК-4}$ Способен проводить специальные исследования на побочные электромагнитные излучения и наводки технических средств обработки информации	знать: - перечень, основное содержание и сущность методических и нормативных документов по защите информации.. уметь: - оценивать эффективность технических средств защиты информации..
ПК-4 Способен проводить контроль защищенности информации	ПК-4.2$_{ПК-4}$ Способен проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	знать: - назначение, общую характеристику и принципы работы технических средств защиты информации.. уметь: - определять рациональные меры и технические средства защиты на объектах и оценивать их эффективность..
ПК-4 Способен проводить контроль защищенности информации	ПК-4.3$_{ПК-4}$ Способен проводить контроль защищенности акустической речевой информации от утечки по техническим каналам	знать: - назначение и порядок проведения инструментального контроля эффективности защиты информации.. уметь: - контролировать эффективность мер инженерно-технической защиты информации..

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	42	8	4	4	4	-	-	-	-	-	30	-	***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 курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Способы и технические средства защиты конфиденциальной информации" подготовка к выполнению заданий на практических занятиях
1.1	Введение	13		1	1	1	-	-	-	-	-	10	-	
1.2	Тема 1	13		1	1	1	-	-	-	-	-	10	-	
1.3	Тема 2	16		2	2	2	-	-	-	-	-	10	-	

														Самостоятельное изучение теоретического материала: Изучение дополнительного материала по разделу "Способы и технические средства защиты конфиденциальной информации" ***Изучение материалов литературных источников:*** [1], 373-396 [4], 13-23 [5], 373-396
2	Защита информации техническими средствами в организации	66		10	10	10	-	-	-	-	-	36	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Защита информации техническими средствами в организации"
2.1	Тема 3	7		1	1	1	-	-	-	-	-	4	-	***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 курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***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
2.2	Тема 4	7		1	1	1	-	-	-	-	-	4	-	
2.3	Тема 5	7		1	1	1	-	-	-	-	-	4	-	
2.4	Тема 6	7		1	1	1	-	-	-	-	-	4	-	
2.5	Тема 7	7		1	1	1	-	-	-	-	-	4	-	
2.6	Тема 8	7		1	1	1	-	-	-	-	-	4	-	
2.7	Тема 9	7		1	1	1	-	-	-	-	-	4	-	
2.8	Тема 10	7		1	1	1	-	-	-	-	-	4	-	
2.9	Тема 11	10		2	2	2	-	-	-	-	-	4	-	

														"Защита информации техническими средствами в организации" ***Изучение материалов литературных источников:*** [1], 350-372 [3], 169-242
3	Принципы оценки эффективности системы инженерно-технической защиты информации	44		6	6	6	-	-	-	-	-	26	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Принципы оценки эффективности системы инженерно-технической защиты информации"
3.1	Тема 12	14		2	2	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 "Принципы оценки эффективности системы инженерно-технической защиты информации" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Принципы оценки эффективности системы инженерно-технической защиты информации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Принципы оценки эффективности системы
3.2	Тема 13	14		2	2	2	-	-	-	-	-	8	-	
3.3	Тема 14	16		2	2	2	-	-	-	-	-	10	-	

														инженерно-технической защиты информации" ***<u>Изучение материалов литературных источников:</u>*** [2], 60-88
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	28.0		-	-	-	8	-	4	-	0.3	15.7	-	
	Всего за семестр	**216.0**		**20**	**20**	**20**	**8**	**2**	**4**	**-**	**0.8**	**107.7**	**33.5**	
	Итого за семестр	**216.0**		**20**	**20**	**20**	**10**		**4**		**0.8**	**141.2**		

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. Применение разделительных трансформаторов и помехоподавляющих фильтров. Электростатическое, магнитостатическое и электромагнитное экранирование. Заземление всех устройств, как необходимое условие эффективной защиты информации..

2.4. Тема 6

Акустическая защита защищаемого помещения. Защита пассивными средствами защищаемых помещений. Акустическая обработка помещения, предполагаемого к использованию в качестве защищаемого. Аппаратура и способы активной защиты помещений от утечки речевой информации. Способы предотвращения несанкционированной записи речевой информации на диктофон..

2.5. Тема 7

Основные принципы подключения ЭУНПИ к телефонной линии. Методы и средства защиты телефонных линий. Методы защиты телефонных аппаратов. Методы контроля телефонных линий. Анализаторы проводных и телефонных линий..

2.6. Тема 8

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..

2.7. Тема 9

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..

2.8. Тема 10

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..

2.9. Тема 11

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 12

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 13

Проведение инструментального контроля. Оценка эффективности применяемых средств активной защиты информации. Ограничения применения генераторов пространственного зашумления. Особенности применения блокираторов сотовой связи..

3.3. Тема 14

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. 10. 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;
2. 9. 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;
3. 8. 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;
4. 7. Практическое занятие по изучению возможностей цифрового анализатора проводных и телефонных линий TALAN;
5. 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;
6. 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;
7. 13. Практическая разработка предложений по защите информации в кабинете руководителя;
8. 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;
9. 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;
10. 6. Практическое занятие по оценке эффективности применения средств активной защиты Соната-Р3.1, Салют 2000Б, подавителя сотовой связи;
11. 14. Практическое занятие по оценке вариантов предложенных решений по защите информации в кабинете руководителя;
12. 11. Практическая разработка типовых вариантов решений по предотвращению утечки информации за счет побочных электромагнитных излучений и наводок;
13. 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;
14. 12. Практическое занятие по оценке вариантов предложенных решений по предотвращению утечки информации за счет побочных электромагнитных излучений и наводок.

3.4. Темы лабораторных работ

1. Лабораторная работа № 7. Методы защиты цифровой информации от утечки по каналу наводок на проводные коммуникации;
2. Лабораторная работа № 6. Методы защиты цифровой информации от утечки по

каналу побочных электромагнитных излучений;
3. Лабораторная работа № 5 Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема видовой информации в ограждающих конструкциях методом оптической локации;
4. Лабораторная работа № 4 Специальные обследования защищаемых помещений по выявлению внедренных электронных средств съема информации в ограждающих конструкциях нелинейным локатором Лорнет-24;
5. Лабораторная работа № 2. Методы защиты речевой конфиденциальной информации от утечки из ЗП по виброакустическому каналу;
6. Лабораторная работа № 1. Методы защиты речевой конфиденциальной информации от утечки из ЗП по воздушному акустическому каналу;
7. Лабораторная работа № 3. Организация и проведение радиомониторинга объекта защиты с использованием индикаторов электромагнитного поля и автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ».

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Способы и технические средства защиты конфиденциальной информации"
2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Защита информации техническими средствами в организации"
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Принципы оценки эффективности системы инженерно-технической защиты информации"

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"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Способы и технические средства защиты конфиденциальной информации"
2. Консультации проводятся по разделу "Защита информации техническими средствами в организации"
3. Консультации проводятся по разделу "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

8 Семестр

Курсовая работа (КР)

Темы:

- 1.Разработка технического проекта системы защиты информации в конференц-зале от утечки по параметрическим и оптико-электронному каналам. 2.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустическим и виброакустическим каналам. 3.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустоэлектрическим и оптико-электронному каналам. 4.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по параметрическим и оптико-электронному каналам. 5.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по электромагнитным и акустическим каналам. 6.Разработка технического задания на создание системы защиты информации в кабинете руководителя от утечки по электрическому и параметрическому каналам. 7.Разработка технического задания системы защиты информации в кабинете руководителя от утечки по электромагнитному и акустическому каналам. 8.Разработка технического задания системы защиты информации в кабинете руководителя от утечки по электромагнитному и акустоэлектрическому каналам. 9.Разработка технического задания системы защиты информации в конференц-зале от утечки по электрическим и акустическому каналам. 10.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки речевой информации по акустическим и виброакустическим каналам. 11.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустическим и виброакустическим каналам. 12.Разработка технического проекта системы защиты информации в конференц-зале комнате от утечки по акустическим и виброакустическим каналам. 13.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по акустоэлектрическим и оптико-электронному каналам. 14.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по акустоэлектрическим и оптико-электронному каналам. 15.Разработка технического проекта системы защиты информации в конференц-зале от утечки по акустоэлектрическим и оптико-электронному каналам. 16.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по параметрическим и оптико-электронному каналам. 17.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по параметрическим и оптико-электронному каналам. 18.Разработка технического проекта системы защиты информации в конференц-зале от утечки по параметрическим и оптико-электронному каналам. 19.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по электромагнитным и электрическим каналам. 20.Разработка технического проекта системы защиты информации в кабинете руководителя от утечки по электрическим и параметрическому каналам. 21.Разработка технического проекта системы защиты информации в переговорной комнате от утечки по электромагнитным и акустическим каналам. 22.Разработка технического проекта системы защиты информации в кабинета

руководителя от утечки по электромагнитным и акустоэлектрическому каналам. 23.Разработка технического проекта системы защиты информации в кабинета руководителя от утечки по акустическому и акустоэлектрическому каналам. 24.Разработка программы (технического задания) специального обследования кабинета руководителя по выявлению электронных средств съема информации. 25.Разработка программы (технического задания) специального обследования переговорной комнаты по выявлению электронных средств съема информации. 26.Разработка программы (технического задания) специального обследования конференц-зала по выявлению электронных средств съема информации. 27.Разработка программы (технического задания) специальной проверки по выявлению электронных средств съема информации в технических средствах и системах в кабинете руководителя. 28.Разработка программы (технического задания) специальной проверки по выявлению схемотехнических и иных доработок технических средств и систем в кабинете руководителя, приводящих к усилению их естественных свойств. 29.Разработка программы (технического задания) специального исследования защищенности средств ТСПИ и ВТСС в кабинете руководителя от утечки опасных сигналов ПЭМИН. 30.Разработка программы (технического задания) специального исследования защищенности ограждающих конструкций переговорной комнаты от утечки речевой информации по акустическому и виброакустическому каналам.

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 15	Зачетная
Раздел курсового проекта	1, 2	2, 3	3, 4	Защита курсового проекта
Объем раздела, %	30	30	40	-
Выполненный объем нарастающим итогом, %	30	60	100	-

Номер раздела	Раздел курсового проекта
1	Введение
2	Глава первая
3	Глава вторая
4	Заключение

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.	ПК-4.1$_{ПК-4}$	+			Отчет/Защита лабораторной работы № 3 Отчет/Защита лабораторных работ № 1-2
назначение, общую характеристику и принципы работы технических средств защиты информации.	ПК-4.2$_{ПК-4}$		+		Отчет/Защита лабораторных работ № 4 - 5
назначение и порядок проведения инструментального контроля эффективности защиты информации.	ПК-4.3$_{ПК-4}$			+	Отчет/Защита лабораторных работ № 6 - 7
Уметь:					
оценивать эффективность технических средств защиты информации.	ПК-4.1$_{ПК-4}$	+			Отчет/Защита лабораторной работы № 3 Отчет/Защита лабораторных работ № 1-2
определять рациональные меры и технические средства защиты на объектах и оценивать их эффективность.	ПК-4.2$_{ПК-4}$		+		Отчет/Защита лабораторных работ № 4 - 5
контролировать эффективность мер инженерно-технической защиты информации.	ПК-4.3$_{ПК-4}$			+	Отчет/Защита лабораторных работ № 6 - 7

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

4.1. Текущий контроль успеваемости

8 семестр

Форма реализации: Защита задания

1. Защита лабораторной работы № 3 (Отчет)
2. Защита лабораторных работ № 1-2 (Отчет)
3. Защита лабораторных работ № 4 - 5 (Отчет)
4. Защита лабораторных работ № 6 - 7 (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

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

Курсовая работа (КР) (Семестр №8)

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 8 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. 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. **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	М-504/1, Учебная аудитория	парта, стол преподавателя, стул, доска маркерная
Учебные аудитории для проведения	М-504/1, Учебная аудитория	парта, стол преподавателя, стул, доска маркерная

лабораторных занятий		
Учебные аудитории для проведения промежуточной аттестации	М-504/1, Учебная аудитория	парта, стол преподавателя, стул, доска 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

Технические средства защиты информации

(название дисциплины)

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Защита лабораторных работ № 1-2 (Отчет)
КМ-2 Защита лабораторной работы № 3 (Отчет)
КМ-3 Защита лабораторных работ № 4 - 5 (Отчет)
КМ-4 Защита лабораторных работ № 6 - 7 (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	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				+	
2.7	Тема 9				+	
2.8	Тема 10				+	
2.9	Тема 11				+	
3	Принципы оценки эффективности системы инженерно-технической защиты информации					

3.1	Тема 12				+
3.2	Тема 13				+
3.3	Тема 14				+
	Вес КМ, %:	25	25	25	25

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Технические средства защиты информации

(название дисциплины)

8 семестр

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

КМ-1 соблюдение графика выполнения КР; качество оформления КР
КМ-2 Соблюдение графика выполнения КР; оценка выполнения разделов КР
КМ-3 Соблюдение графика выполнения КР; оценка выполнения разделов КР

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	15
1	Введение		+		
2	Глава первая		+	+	
3	Глава вторая			+	+
4	Заключение				+
		Вес КМ, %:	30	30	40