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
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.09.04.01**
Трудоемкость в зачетных единицах:	**6 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**6 семестр - 28 часа;**
Практические занятия	**6 семестр - 28 часа;**
Лабораторные работы	**6 семестр - 14 часов;**
Консультации	**6 семестр - 16 часов;**
Самостоятельная работа	**6 семестр - 125,2 часа;**
в том числе на КП/КР	**6 семестр - 15,7 часов;**
Иная контактная работа	**6 семестр - 4 часа;**
включая: **Тестирование** **Контрольная работа** **Отчет**	
Промежуточная аттестация:	
Защита курсовой работы **Экзамен**	**6 семестр - 0,3 часа;** **6 семестр - 0,5 часа;** **всего - 0,8 часа**

Москва 2019

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 обучаемыми 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-3 способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач		знать: - назначение, общую характеристику и принципы работы технических средств защиты информации.
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		знать: - содержание принципов и основ проведения технического контроля защищенности объектов информатизации.
ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации		знать: - перечень, основное содержание и сущность методических и нормативных документов по защите информации.
ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых		уметь: - определять рациональные меры и технические средства защиты на объектах и оценивать их эффективность; - контролировать эффективность мер инженерно-технической защиты

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
программных, программно-аппаратных и технических средств защиты информации		информации.
ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений		уметь: - разрабатывать технические решения по защите объектов информатизации на основе использования технических средств защиты информации.
ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов		знать: - принципы применения информационных технологий для построения и использования информационных систем, принципы организации хранилищ данных и распределенной обработки. уметь: - проводить эксперименты по заданной методике.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации		знать: - основные физические явления, законы квантовой и атомной физики, а также их математическое описание. уметь: - определять, какие законы квантовой и атомной физики обусловливают явления или процессы в устройствах различной физической природы, и выполнять применительно к некоторым из них простые технические расчёты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений 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	Методы, способы и средства инженерно-технической защиты информации	41	6	8	5	8	-	-	-	-	-	20	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Методы, способы и средства инженерно-технической защиты информации" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Методы, способы и средства инженерно-технической защиты информации" подготовка к выполнению заданий на практических занятиях ***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 контрольной работе:*** Изучение материалов по разделу Методы, способы и средства инженерно-технической защиты информации и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Методы, способы и средства инженерно-
1.1	Тема 1. Общие положения инженерно-технической защиты информации.	7		1	1	1	-	-	-	-	-	4	-	
1.2	Тема 2. Способы и средства инженерной защиты и технической охраны.	7		1	1	1	-	-	-	-	-	4	-	
1.3	Тема 3. Способы и средства обнаружения (поиска) каналов утечки информации.	9		2	1	2	-	-	-	-	-	4	-	
1.4	Тема 4. Способы и средства защиты каналов утечки информации.	9		2	1	2	-	-	-	-	-	4	-	
1.5	Тема 5. Способы и средства предотвращения утечки информации по материально-вещественному каналу.	9		2	1	2	-	-	-	-	-	4	-	

														технической защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***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 "Методы, способы и средства инженерно-технической защиты информации" материалу. ***Подготовка к текущему контролю:*** Повторение материала по разделу "Методы, способы и средства инженерно-технической защиты информации" ***Изучение материалов литературных источников:*** [1], 303-386 [3], 9-16 [5], 13-45 [6], гл. 1-2
2	Организационные основы инженерно-технической защиты информации	52		10	4	10	-	-	-	-	-	28	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Организационные основы инженерно-технической защиты информации" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Организационные основы инженерно-технической защиты информации" подготовка к выполнению заданий на практических занятиях
2.1	Тема 6. Основы организации инженерно-технической защиты информации.	13		2	1	2	-	-	-	-	-	8	-	
2.2	Тема 7. Мероприятия организации	19		4	1	4	-	-	-	-	-	10	-	

	инженерно-технической защиты информации.													
2.3	Тема 8. Организация проведения и сопровождения аттестации объекта защиты на соответствие требованиям безопасности информации.	20		4	2	4	-	-	-	-	-	10	-	***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 контрольной работе:*** Изучение материалов по разделу Организационные основы инженерно-технической защиты информации и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Организационные основы инженерно-технической защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***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 "Организационные основы инженерно-технической защиты информации" материалу. ***Подготовка к текущему контролю:*** Повторение материала по разделу "Организационные основы инженерно-технической защиты информации" ***Изучение материалов литературных***

														источников: [1], 121-221
3	Основы методического обеспечения инженерно-технической защиты информации	53		10	5	10	-	-	-	-	-	28	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основы методического обеспечения инженерно-технической защиты информации" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основы методического обеспечения инженерно-технической защиты информации" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основы методического обеспечения инженерно-технической защиты информации" подготовка к выполнению заданий на практических занятиях ***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 контрольной работе:*** Изучение материалов по разделу Основы методического обеспечения инженерно-технической защиты информации и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Основы методического обеспечения инженерно-технической защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных
3.1	Тема 9. Методические рекомендации по разработке мер защиты информации.	13		2	1	2	-	-	-	-	-	8	-	
3.2	Тема 10. Разработка типовых вариантов решений по защите информации.	20		4	2	4	-	-	-	-	-	10	-	
3.3	Тема 11. Проектирование систем инженерно-технической защиты информации.	20		4	2	4	-	-	-	-	-	10	-	

														заданий. Проверка домашнего задания проводится по представленным письменным работам. ***<u>Подготовка к аудиторным занятиям:</u>*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***<u>Подготовка к лабораторной работе:</u>*** 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 "Основы методического обеспечения инженерно-технической защиты информации" материалу. ***<u>Изучение материалов литературных источников:</u>*** [2], гл. 1-3 [4], 79-100 [7], 25-35
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	34.0		-	-	-	14	-	4	-	0.3	15.7	-	
	Всего за семестр	**216.0**		**28**	**14**	**28**	**14**	**2**	**4**	**-**	**0.8**	**91.7**	**33.5**	
	Итого за семестр	**216.0**		**28**	**14**	**28**	**16**		**4**		**0.8**	**125.2**		

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. Методы, способы и средства инженерно-технической защиты информации

1.1. Тема 1. Общие положения инженерно-технической защиты информации.

Цели и задачи инженерно-технической защиты информации. Принципы инженерно-технической защиты информации. Факторы обеспечения инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Физическая защита информации и ее методы. Методы скрытия информации. Методы структурного скрытия. Техническое дезинформирование. Зависимость качества информации от соотношения сигнал/шум. Методы энергетического скрытия сигналов..

1.2. Тема 2. Способы и средства инженерной защиты и технической охраны.

Структура системы физической защиты информации. Классификация средств подсистем предупреждения, обнаружения, ликвидации угроз и управления. Автономная и централизованные системы охраны. Естественные и искусственные преграды инженерной защиты. Способы и средства управления доступом в контролируемые зоны людей и автотранспорта. Показатели эффективности инженерной защиты. Способы и средства обнаружения злоумышленников и очагов пожара. Способы видеонаблюдения и видеоконтроля объектов. Способы нейтрализации действий злоумышленника. Способы управления системами физической защиты. Интегрирование средств и систем инженерной защиты, охраны объектов и видеоконтроля. Классификация средств инженерно-технической защиты информации по назначению. Основные средства инженерной защиты информации (заборы, окна, двери, ограждения зданий и помещений, металлические шкафы, сейфы и хранилища) и показатели их защищенности от злоумышленника. Технические средства охраны (извещатели, шлейфы, приемо-контрольные приборы). Виды и основные характеристики извещателей. Комбинированные извещатели. Средства видеонаблюдения и видеоконтроля (телевизионные передающие камеры, мониторы, коммутаторы, квадраторы, мультиплексоры, специальные видеомагнитофоны, видеоменеджеры). Средства дежурного освещения. Средства нейтрализации угроз (тревожная сигнализация, аварийное электропитание, средства и комплексы пожаротушения). Интегрированные системы безопасности организаций..

1.3. Тема 3. Способы и средства обнаружения (поиска) каналов утечки информации.

Способы и средства предотвращения утечки информации с помощью электронных устройств негласного получения информации (ЭУНПИ). Основные демаскирующие признаки проводных и радио ЭУНПИ. Классификация 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. Принципы работы и характеристики металлодетекторов и эндоскопов. Особенности применения способов и средств контроля помещений перед совещаниями и в ходе их проведения. Виды проверок отдельных предметов. Способы обнаружения ЭУНПИ. Наборы средств, способы и средства обнаружения (поиска) каналов утечки информации за счет ПЭМИН. Классификация средств обнаружения радиоизлучающих и неизлучающих ЭУНПИ. Принципы работы и основные характеристики обнаружителей электромагнитного поля, их достоинства и недостатки, способы применения. Радиоприемные устройства, универсальные поисковые приборы, автоматизированных поисковые комплексы, их состав, возможности, принципы работы, параметры функционирования и порядок применения. Принципы работы непрерывных и импульсных нелинейных локаторов. Типы и характеристики отечественных и зарубежных локаторов. Физические принципы работы и способы применения

обнаружителей пустот для выявления ЭУНПИ. Виды рентгеновских установок. Переносные рентгенотелевизионные комплексы. Тепловизионные приборы..

1.4. Тема 4. 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. Методы и способы защиты информации циркулирующей в телефонных аппаратах и двупроводных линиях. Методология защиты информации от утечки за счет ПЭМИН. Требования к уровню подавления опасных сигналов, вызванных побочными электромагнитными излучениями и наводками. Средства ослабления ПЭМИ ТСПИ и их наводок. Защита электросети, защита оконечного оборудования слаботочных линий. Защита абонентского участка телефонной линии. Защита информации обрабатываемой техническими средствами. Пассивные способы защиты акустической (речевой) информации от ее утечки через несущие конструкции защищаемого помещения.. Звуко- и виброизоляция. Акустическая защита защищаемого помещения. Акустическая обработка помещения, предполагаемого к использованию в качестве защищаемого. Активные и комплексные способы защиты акустического информативного сигнала. Виды активных помех. Способы создания искусственных акустических и виброакустических помех для защиты несущих конструкций и объема защищаемого помещения. Активные и комбинированные способы защиты информации. Пассивные средства защиты защищаемых помещений. Аппаратура и способы активной защиты помещений от утечки речевой информации. Способы предотвращения несанкционированной записи речевой информации на диктофон. Нейтрализация радиомикрофонов..

1.5. Тема 5. Способы и средства предотвращения утечки информации по материально-вещественному каналу.

Способы предотвращения утечки информации по материально-вещественному каналу. Классификация и характеристика основных средств предотвращения утечки информации по материально-вещественному каналу. Средства защиты и экстренного уничтожения информации на различных носителях..

2. Организационные основы инженерно-технической защиты информации

2.1. Тема 6. Основы организации инженерно-технической защиты информации.

Органы, обеспечивающие защиту информации от технических средств разведки в субъектах РФ и организациях (на предприятиях). Функции сотрудников службы безопасности и структурных подразделений организации, обеспечивающих инженерно-техническую защиту информации. Вариант структуры подразделения инженерно-технической защиты информации службы безопасности организации, его основные задачи и функции. 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 7. Мероприятия организации инженерно-технической защиты информации.

Основные направления инженерно-технической защиты 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 8. Организация проведения и сопровождения аттестации объекта защиты на соответствие требованиям безопасности информации.

Объекты, подлежащие обязательной и добровольной аттестации. Порядок проведения аттестации объектов защиты на соответствие требованиям безопасности информации. Состав и содержание документа «Аттестат соответствия». Категорирование защищаемой информации. Мероприятия по организации выявления технических каналов. Специальные проверки. Порядок проведения специальной проверки технических средств. Специальные обследования. Подготовка к проведению специальных обследований. Оценка вероятного противника, Оценка условий, в которых решается задача выявления технических каналов утечки информации. Порядок и последовательность решения проблемы поисковой операции. Выполнение поисковых мероприятий, радиообнаружение. Первичный осмотр и техническая проверка. Проверка электрических и электронных приборов. 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..

3. Основы методического обеспечения инженерно-технической защиты информации

3.1. Тема 9. Методические рекомендации по разработке мер защиты информации.

Основные способы и средства защиты информации от типовых вариантов угроз. Типовые рекомендации по выбору мер инженерно-технической защиты информации. Способы оценки значений показателей моделей..

3.2. Тема 10. Разработка типовых вариантов решений по защите информации.

Особенности кабинета руководителя как объекта инженерно-технической защиты, содержащего источники защищаемой информации. Задачи и технология обеспечения инженерно-технической защиты информации в кабинете руководителя. Пространственная модель кабинета руководителя. Виды защищаемой в кабинете руководителя информации и оценка ее цены. Типовые источники защищаемой информации в кабинете и их оценка защищенности. Варианты проникновения злоумышленника к источникам информации и оценка. Источники наблюдения в кабинете руководителя организации. Потенциальные оптические каналы утечки информации. Оценки возможностей средств оптической разведки по наблюдению источников информации в кабинете руководителя организации.

Предложения по защите информации в кабинете от наблюдения. Потенциальные каналы утечки речевой информации из кабинета руководителя. Методические рекомендации по оценке уровня речевой информации в потенциальных местах размещения злоумышленника и его средств подслушивания. Способы повышения звукоизоляции ограждений помещения. Способы проверки помещения на наличие в нем ЭУНПИ. Рекомендации по обеспечению защиты информации во время проведения совещания. Основные и вспомогательные технические средства в кабинете руководителя, создающие побочные электромагнитные излучения и наводки. Рекомендации по оценке угрозы потенциальных радиоэлектронных каналов утечки информации из помещения. Рекомендации по предотвращению утечки информации через побочные электромагнитные излучения и наводки..

3.3. Тема 11. Проектирование систем инженерно-технической защиты информации.

Стадии создания системы защиты информации. Предпроектная стадия (предпроектное обследование объекта информатизации, разработка аналитического обоснования создания СЗИ и технического (частного технического) задания на ее создание). Стадия проектирования (разработки проектов) и реализации объекта информатизации. Стадия ввода в действие СЗИ (опытная эксплуатация и приемо-сдаточные испытания средств защиты информации, аттестация объекта информатизации на соответствие требованиям безопасности информации. Содержание документа (проекта, пояснительной записки, предложений) по обеспечению защиты информации в кабинете руководителя. Исходные данные. Постановка задачи. Содержание основной части с обоснованием предложений. Заключение и приложения..

3.3. Темы практических занятий

1. 12.Основные положения организации инженерно-технической защиты информации на предприятии;
2. 11.Нормативно-правовая база организации инженерно-технической защиты информации на предприятии Разработка основного содержания документов нормативно-методической базы инженерно-технической защиты информации;
3. 10.Способы и средства защиты информации, обрабатываемой в телефонных аппаратах, циркулирующей в двухпроводных линиях и каналах связи;
4. 9.Способы и средства защиты акустической информации в защищаемом помещении;
5. 8.Способы и средства защиты информации, обрабатываемой в ТСПИ;
6. 6.Способы и средства выявления радиоизлучающих средств негласного съема информации;
7. 15.Характеристика основ технического контроля эффективности мер инженерно-технической защиты информации;
8. 1.Классификация методов инженерно-технической защиты информации;
9. 4.Характеристика способов и средств инженерной защиты и технической охраны объектов;
10. 3.Характеристика способов и средств инженерно-технической защиты территорий и помещений подсистем предупреждения, обнаружения и ликвидации угроз;
11. 2.Комплексные и интегрированные системы безопасности организаций;
12. 13.Разработка руководящих и методических документов регламентирующих организацию инженерно-технической защиты информации на предприятии;
13. 7.Способы и средства выявления неизлучающих средств негласного съема информации;
14. 16.Организация и порядок выполнения мероприятий по выявлению каналов утечки информации на основе проведения специальных исследований в области акустоэлектрических преобразований;
15. 5.Способы и средства визуального осмотра помещений;

16. 14.Характеристика особенностей организации мероприятий инженерно-технической защиты информации.

3.4. Темы лабораторных работ

1. 1.Лабораторная работа № 1. Организация и проведение радиомониторинга с использованием индикаторов электромагнитного поля и автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ».;
2. 2.Лабораторная работа № 2. Специальное обследование защищаемого помещения по выявлению внедренных электронных средств съема информации в ограждающих конструкциях.;
3. 3.Лабораторная работа № 3. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу.;
4. 4. Лабораторная работа № 4. Методы защиты речевой конфиденциальной информации от утечки по виброакустическому канал.;
5. 5. Лабораторная работа № 5. Специальное обследование проводных коммуникаций защищаемого помещения от утечки речевой конфиденциальной информации..

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 "Методы, способы и средства инженерно-технической защиты 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 "Организационные основы инженерно-технической защиты информации"
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 "Основы методического обеспечения инженерно-технической защиты информации"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Методы, способы и средства инженерно-технической защиты информации"
2. Консультации проводятся по разделу "Организационные основы инженерно-технической защиты информации"
3. Консультации проводятся по разделу "Основы методического обеспечения инженерно-технической защиты информации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методы, способы и средства инженерно-технической защиты информации"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Организационные основы инженерно-технической защиты информации"

3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основы методического обеспечения инженерно-технической защиты информации"

3.6 Тематика курсовых проектов/курсовых работ

6 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 - 13	Зачетная
Раздел курсового проекта	1	2, 3	3, 4	Защита курсового проекта
Объем раздела, %	20	20	60	-
Выполненный объем нарастающим итогом, %	20	40	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:					
назначение, общую характеристику и принципы работы технических средств защиты информации	ОПК-3(Компетенция)	+			Тестирование/Тестирование
содержание принципов и основ проведения технического контроля защищенности объектов информатизации	ПК-1(Компетенция)	+	+		Контрольная работа/Контрольная работа
перечень, основное содержание и сущность методических и нормативных документов по защите информации	ПК-5(Компетенция)		+	+	Отчет/Защита лабораторных работ № 1 - 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ». Специальное обследование защищаемого помещения по выявлению внедренных электронных средств съема информации в ограждающих конструкциях.
принципы применения информационных технологий для построения и использования информационных систем, принципы организации хранилищ данных и распределенной обработки	ПК-11(Компетенция)			+	Отчет/Защита лабораторных работ № 4 - 5. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам.
основные физические явления, законы квантовой и атомной физики, а также	ПК-12(Компетенция)	+			Тестирование/Тестирование

их математическое описание					
Уметь:					
контролировать эффективность мер инженерно-технической защиты информации	ПК-6(Компетенция)	+			Контрольная работа/Контрольная работа
определять рациональные меры и технические средства защиты на объектах и оценивать их эффективность	ПК-6(Компетенция)		+		Отчет/Защита лабораторных работ № 1 - 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ». Специальное обследование защищаемого помещения по выявлению внедренных электронных средств съема информации в ограждающих конструкциях.
разрабатывать технические решения по защите объектов информатизации на основе использования технических средств защиты информации	ПК-7(Компетенция)			+	Отчет/Защита лабораторных работ № 4 - 5. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам.
проводить эксперименты по заданной методике	ПК-11(Компетенция)	+			Тестирование/Тестирование
определять, какие законы квантовой и атомной физики обусловливают явления или процессы в устройствах различной физической природы, и выполнять применительно к некоторым из них простые технические расчёты	ПК-12(Компетенция)		+		Контрольная работа/Контрольная работа

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: Защита задания

1. Защита лабораторных работ № 1 - 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ». Специальное обследование защищаемого помещения по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. (Отчет)
2. Защита лабораторных работ № 4 - 5. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам. (Отчет)

Форма реализации: Письменная работа

1. Контрольная работа (Контрольная работа)
2. Тестирование (Тестирование)

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

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

Курсовая работа (КР) (Семестр №6)

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

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. Невский, А. Ю. Технические средства охраны : учебное пособие для студентов инженерно-экономического ин-та / А. Ю. Невский, О. Р. Баронов, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" . – М. : ВНИИгеосистем, 2015 . – 186 с. - ISBN 978-5-8481-0196-6 .;

3. 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;
4. 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 .;
5. Северин, В. А. Комплексная защита информации на предприятии : учебник для вузов по направлению и специальности "Юриспруденция" / В. А. Северин ; Ред. Б. И. Пугинский . – М. : Городец, 2008 . – 368 с. - ISBN 978-5-9584020-4-5 .;
6. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468;
7. А. Д. Фефилов- "Методы и средства защиты информации в сетях", Издательство: "Лаборатория книги", Москва, 2011 - (105 с.) https://biblioclub.ru/index.php?page=book&id=140796.

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. **База данных Web of Science** - http://webofscience.com/
4. **База данных Scopus** - http://www.scopus.com
5. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
6. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
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. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
13. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.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	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 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
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	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
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

Инженерно-техническая защита информации

(название дисциплины)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Тестирование (Тестирование)

КМ-2 Контрольная работа (Контрольная работа)

КМ-3 Защита лабораторных работ № 1 - 3. Организация и проведение радиомониторинга объекта защиты индикаторами электромагнитного поля и с использованием автоматизированного программно-аппаратного комплекса обнаружения радиоизлучающих средств «Крона НМ». Специальное обследование защищаемого помещения по выявлению внедренных электронных средств съема информации в ограждающих конструкциях. (Отчет)

КМ-4 Защита лабораторных работ № 4 - 5. Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому и виброакустическому каналам. (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	Методы, способы и средства инженерно-технической защиты информации					
1.1	Тема 1. Общие положения инженерно-технической защиты информации.		+	+		
1.2	Тема 2. Способы и средства инженерной защиты и технической охраны.		+	+		
1.3	Тема 3. Способы и средства обнаружения (поиска) каналов утечки информации.		+	+		
1.4	Тема 4. Способы и средства защиты каналов утечки информации.		+	+		
1.5	Тема 5. Способы и средства предотвращения утечки информации по материально-вещественному каналу.		+	+		
2	Организационные основы инженерно-технической защиты информации					
2.1	Тема 6. Основы организации инженерно-технической защиты информации.			+	+	
2.2	Тема 7. Мероприятия организации инженерно-технической защиты информации.			+	+	
2.3	Тема 8. Организация проведения и сопровождения аттестации объекта защиты на соответствие требованиям безопасности информации.			+	+	
3	Основы методического обеспечения инженерно-технической защиты информации					

3.1	Тема 9. Методические рекомендации по разработке мер защиты информации.			+	+
3.2	Тема 10. Разработка типовых вариантов решений по защите информации.			+	+
3.3	Тема 11. Проектирование систем инженерно-технической защиты информации.			+	+
	Вес КМ, %:	25	25	25	25

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Инженерно-техническая защита информации

(название дисциплины)

6 семестр

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

КМ-1 Оценка выполнения разделов КР
КМ-2 Качество оформления КР
КМ-3 Качество содержания 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	13
1	Введение		+		
2	Глава первая			+	
3	Глава вторая			+	+
4	Заключение				+
		Вес КМ, %:	20	20	60