Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.О.35
Защита информации от утечки по техническим каналам

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 96
самостоятельная работа 12
контактная работа во время промежуточной аттестации (ИКР) 0
часов на контроль 34,7

Виды контроля в семестрах:
экзамены 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Практические	32	32	32	32
Контактная работа на аттестации (в период экз. сессий)	0,3	0,3	0,3	0,3
Консультации перед экзаменом	1	1	1	1
В том числе в форме практ.подготовки	4	4	4	4
Итого ауд.	96	96	96	96
Контактная работа	97,3	97,3	97,3	97,3
Сам. работа	12	12	12	12
Часы на контроль	34,7	34,7	34,7	34,7
Итого	144	144	144	144

Программу составил(и):
к.т.н., доцент, Капустин С.А.

Рецензент(ы):
д.т.н. , Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.

Рабочая программа дисциплины
Защита информации от утечки по техническим каналам

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	• формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий;
1.2	• развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.
Задачи: • получение теоретических знаний о концепции инженерно-технической защиты информации; • дать знания по физическим, организационным основам инженерно-технической защиты информации; • получение знаний о средствах и методах добывания и средствах и методах защиты конфиденциальной информации; • методическое обеспечение инженерно-технической защиты информации.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Безопасность систем баз данных
2.1.2	Организационное и правовое обеспечение информационной безопасности
2.1.3	Сети и телекоммуникации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информационных процессов в компьютерных системах
2.2.2	Программно-аппаратные средства защиты информации
2.2.3	Основы управления информационной безопасностью

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	
ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах	
Знать	
Уровень 1	Минимальный необходимый уровень знаний средств криптографической защиты информации в автоматизированных системах
Уровень 2	Уровень знаний средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, без ошибок
ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов	
Уметь	
Уровень 1	Продемонстрированы основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации	
Владеть	
Уровень 1	Имеется минимальный набор навыков для организации защиты информации от утечки по техническим каналам на объектах информатизации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки для организации защиты информации от утечки по техническим каналам на объектах информатизации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки для организации защиты информации от утечки по техническим каналам на объектах информатизации без ошибок и недочётов
ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации	
Уметь	

Уровень 1	Продемонстрированы основные умения оценивать угрозы информационной безопасности объекта информатизации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения оценивать угрозы информационной безопасности объекта информатизации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения оценивать угрозы информационной безопасности объекта информатизации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки использования средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации без ошибок и недочётов

ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	
ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	
Знать	
Уровень 1	Минимальный необходимый уровень знаний определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите
Уровень 2	Уровень знаний определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите в объёме, соответствующем программе подготовки, без ошибок
ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	
Уметь	
Уровень 1	Продемонстрированы основные умения анализирования показателей качества и критериев оценки систем и отдельных методов и средств защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-12.3: Оценивает информационные риски в автоматизированных системах	
Владеть	
Уровень 1	Имеется минимальный набор навыков оценки информационных рисков в автоматизированных системах области с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки оценки информационных рисков в автоматизированных системах области с некоторыми недочётами
Уровень 3	Продемонстрированы навыки оценки информационных рисков в автоматизированных системах области без ошибок и недочётов
ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	
Владеть	
Уровень 1	Имеется минимальный набор навыков разработки основных показателей технико-экономического обоснования соответствующих проектных решений с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки разработки основных показателей технико-экономического обоснования соответствующих проектных решений с некоторыми недочётами
Уровень 3	Продемонстрированы навыки разработки основных показателей технико-экономического обоснования соответствующих проектных решений без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература и эл. ресурсы**	**Практ. подг.**
	Раздел 1. Раздел 1. Характеристика технических каналов утечки информации					
1.1	Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации. Электромагнитные, электрические, параметрические и вибрационные каналы /Лек/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.2	Каналы утечки речевой информации. Акустические каналы. Виброакустические каналы. Акустоэлектрические каналы. Оптико-электронные каналы. Параметрические каналы /Лек/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.3	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.Каналы утечки информации при ее передаче по каналам связи /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.4	Радиомониторинг несанкционированных излучений на базе многоканального комплекса радиоконтроля «Квадрат». /Лаб/	6	10	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.5	Технические каналы утечки информации, возникающей при работе вычислительной техники за счет ПЭМИН. Электрические и магнитные излучатели электромагнитного поля. Электрические каналы утечки информации /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.6	Технические каналы утечки видовой информации /Ср/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

1.7	Технические каналы утечки видовой информации /Пр/	6	10	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	2
	Раздел 2. Раздел 2. Средства обнаружения каналов утечки информации					
2.1	Индикаторы электромагнитных излучений. Радиочастотомеры. Сканирующие приемники, селективные вольтметры, анализаторы спектра. Автоматизированные поисковые комплексы /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.2	Нелинейные локаторы. Досмотровая техника /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.3	Характеристики индикаторов электромагнитных излучений, Радиочастотомеров, сканирующих приемников, селективных вольтметров, анализаторов спектра /Ср/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.4	Характеристики нелинейных локаторов и селективных металлодетекторов /Пр/	6	10	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	2
2.5	Локация полупроводниковых приборов с помощью нелинейного локатора. /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.6	Селективный металлодетектор. /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

	Раздел 3. Раздел 3. Организация инженерно-технической защиты информации					
3.1	Организационно-методические основы защиты информации. Общие требования к защите информации. Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
3.2	Методика принятия решения на защиту от утечки информации в организации. Алгоритм принятия решения. Разработка вариантов и выбор оптимального решения /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
3.3	Организация защиты информации. Основные методы инженерно-технической защиты информации. /Ср/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
3.4	Руководящие и нормативно-методические документы регламентирующие деятельность в области защиты информации /Пр/	6	6	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
3.5	Организация системы видеонаблюдения. /Лаб/	6	6	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 4. Раздел 4. Методы и средства защиты информации					
4.1	Организация защиты речевой информации. Пассивные средства защиты выделекнных помещений. Аппаратура и способы активной защиты помещений от утечки речевой информации. Рекомендации про выбору систем виброакустической защиты. Подавление диктофонов. Нейтрализация радиомикрофонов. Защита электросети. Защита оконечного оборудования слаботочных линий. Защита абонентского участка телефонных линий. /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

4.2	Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН. Методология защиты информации от утечки за счет ПЭМИН. Критерий защищенности средств вычислительной техники. Нормированные уровни помех в каналах утечки. Методика проведения специальных исследований технических средств ЭВТ. Метод расчета радиуса зоны II (R2) технических средств ЭВТ. Организация защиты ПЭВМ от несанкционированного доступа /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.3	Средства инженерной защиты и технической охраны. Средства предотвращения утечки информации по техническим каналам. /Пр/	6	6	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.4	Специальные обследования. Подготовка к проведению специальных обследований. Выполнение поисковых мероприятий. Подготовка отчетных материалов. /Лек/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.5	Специальные проверки. Порядок проведения специальной проверки технических средств /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.6	Специальные исследования. Общие положения, термины и определения. Постановка задачи. Специальные исследования в области защиты речевой информации. Специальные исследования в области цифровой информации. /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
4.7	Контроль эффективности инженерно-технической защиты информации. /Ср/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

4.8	Оценка защищенности речевой информации на базе аппаратно-программного комплекса «VNK-012GL». /Лаб/	6	8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 5. Промежуточная аттестация					
5.1	Консультация /Консл/	6	1	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
5.2	Экзамен /КАЭ/	6	0,3	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-12.1 ОПК-12.2 ОПК-12.3 ОПК-12.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Особенности информации как предмета защиты.
2. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации
3. Каналы утечки речевой информации
4. Каналы утечки информации при ее передаче по каналам связи
5. Технические каналы утечки информации, возникающей при работе вычислительной техники за счет ПЭМИН
6. Базовые принципы инженерно-технической защиты информации.
7. Основные направления инженерно-технической защиты информации.
8. Основные задачи инженерно-технической защиты информации.
9. Показатели эффективности инженерно-технической защиты информации.
10. Индикаторы электромагнитных излучений. Радиочастотомеры
11. Сканирующие приемники, селективные вольтметры, анализаторы спектра
12. Автоматизированные поисковые комплексы
13. Нелинейные локаторы
14. Досмотровая техника
15. Факторы, влияющие на эффективность инженерно-технической.
16. Классификация методов инженерно-технической защиты информации.
17. Виды защищаемой информации.
18. Виды угроз безопасности информации.
19. Классификация информационных сигналов по физической природе.
20. Основные принципы разведки.
21. Классификация технической разведки.
22. Принципы организации и ведения технической разведки.
23. Методы противодействия наблюдению в оптическом диапазоне.
24. Методы противодействия подслушиванию.
25. Технические средства подслушивания.
26. Средства перехвата сигналов.
27. Средства противодействия подслушиванию.
28. Средства противодействия наблюдению.
29. Виды технических каналов утечки информации и их свойства.
30. Демаскирующие признаки каналов утечки информации.
31. Виды волн в акустическом канале утечки информации.
32. Эффект маскировки виброакустических сигналов.
33. Звуковое поле в помещении.

34. Звукопоглощающие материалы и конструкции.
35. Звукоизоляция помещений.
36. Методические подходы к оценке эффективности защиты речевой информации.
37. Оценка защищенности по виброакустическому каналу.
38. Основные виды датчиков перехвата информации виброакустического канала и их характеристики.
39. Направленные и лазерный микрофоны.
40. Основные направления защиты от съема информации с телефонной линии.
41. Зоны перехвата информация и виды подключений закладных устройств в каналах телефонной связи.
42. Метод «синфазной низкочастотной маскирующей помехи» для защиты телефонных линий.
43. Метод «высокочастотной маскирующей помехи» для защиты телефонных линий.
44. Метод «ультразвуковой маскирующей помехи» для защиты телефонных линий.
45. Метод «низкочастотной маскирующей помехи» и «компенсационный» метод для защиты телефонных линий.
46. Методы «повышения напряжения» и «понижения напряжения» для защиты телефонных линий.

5.2. Темы письменных работ

1. Современные цифровые диктофоны.
2. Типы микрофонных систем и их технические характеристики.
3. Область применения электронных стетоскопов (радиостетоскопов).
4. и их конструктивные особенности.
5. Лазерные акустические систем разведки.
6. Цифровые анализаторы спектра.
7. Векторные анализаторы сигналов.
8. Измерительные цифровые приемники.
9. Измерительные антенны, токосъемники, пробники для проведения специальных исследований средств вычислительной техники.
10. Программно-аппаратные комплексы для проведения специальных исследований СВТ на ПЭМИН.
11. Портативные шумомеры и вибромеры.
12. Аудиоанализаторы и область применения.
13. Программно-аппаратные комплексы для проведения акустических и виброакустических измерений.
14. Программно-аппаратные комплексы для выявления акустоэлектромагнитных (акустопараметрических) каналов утечки информации.
15. Программно-аппаратные комплексы для оценки защищенности вспомогательных технических средств и систем от акустоэлектрических преобразований.
16. Индикаторы электромагнитного поля.
17. Радиочастотомеры.
18. Сканирующие радиоприемники.
19. Специальные поисковые приемники ближней зоны и интерсепторы.
20. Программно-аппаратные комплексы радиомониторинга.
21. Анализаторы проводных линий.
22. Программно-аппаратные комплексы для исследования проводных линий.
23. Нелинейные радиолокаторы.
24. Рентгенотелевизионные комплексы.
25. Портативные металлоискатели.
26. Эндоскопы.
27. Нормативно-методические документы ФСТЭК в области технической защиты информации.

5.3. Фонд оценочных средств

1. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым они были доверены по службе или стали известны в процессе работы, называется ...
 потеря информации
 компрометация информации
 утечка информации
 публикация информации
 энтропия информации

2. К вспомогательным техническим средствам относится
 сотовый телефон
 персональный компьютер
 сканер
 кондиционер
 телефонный аппарат городской АТС

3. В документах ФСТЭК России НЕ выделяется среди типовых технических каналов утечки
 канал утечки акустической информации

канал утечки видовой информации
канал побочных электромагнитных излучений и наводок
канал цепи заземления

4. Транспондер - это ...
радиозакладка с дистанционным управлением
полуактивная радиозакладка
радиозакладка с системой управления включением передатчика от голоса
инфракрасная закладка
сетевая закладка

5. Устройство прослушивания помещения по телефону, находящемуся в режиме ожидания звонка, получило название ...
телефонное ухо
электронный глаз
лазерная шея
компьютерный кулак
сетевой нос

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2023, URL: https://znanium.com/catalog/document?id=416550
Л1.2	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2023, URL: https://znanium.com/catalog/document?id=416550
Л1.3	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2023, URL: https://znanium.com/catalog/document?id=420080

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2018, URL: https://znanium.com/catalog/document?id=302894
Л2.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2019, URL: https://znanium.com/catalog/document?id=336219

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Интернет университет информационных технологий ИНТУИТ . - Режим доступа: https://www.intuit.ru/studies/courses
Э2	Естественно-научный образовательный портал . - Режим доступа: http://www.en.edu.ru/
Э3	Федеральный центр информационно-образовательных ресурсов . - Режим доступа: http://fcior.edu.ru/
Э4	Единое окно доступа к образовательным ресурсам Единое окно доступа к образовательным ресурсам . - Режим доступа: http://window.edu.ru
Э5	Электронная библиотечная система Znanium. - Режим доступа: http://new.znanium.com/
Э6	Электронная библиотечная система Ibooks . - Режим доступа: http://www.ibooks.ru
Э7	Электронная библиотечная система BOOK.ru . - Режим доступа: http://www.book.ru

Э8	Электронные ресурсы Академии ИМСИТ . - Режим доступа: http://eios.imsit.ru/
Э9	Web-ресурс «Официальный сайт Академии ИМСИТ . - Режим доступа: http://imsit.ru
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	
6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Кодекс – Профессиональные справочные системы https://kodeks.ru
6.3.2.2	Консультант Плюс http://www.consultant.ru

7. МТО (оборудование и технические средства обучения)			
Ауд	Наименование	ПО	Оснащение
113	Лаборатория технической защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя - 1 шт., доска учебная – 1 шт., персональный компьютер с выходом в интернет – 21 шт., интерактивная доска с проектором - 1 шт., многофункциональное устройство– 1 шт., комплект презентаций, лабораторные учебные макеты, аппаратные средства аутентификации пользователя, средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок, средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и тд.), стенды физической защиты объектов информатизации оснащенными средствами контроля доступа системами видеонаблюдения и охраны объектов, соответствующее программное обеспечение, учебно-наглядные методические пособия, комплект оборудования Arduino - 3 шт., учебный комплект SDK 1.1s - 5 шт., комплект инструментов для сборки ПК - 12 шт., средства защиты информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, акустовибрационному и акустоэлектрическому каналам, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам, антивирусные программные комплексы, аппаратные средства аутентификации пользователя, программно-аппаратные комплексы защиты информации, включающие в том числе средства криптографической защиты информации (средства анализа защищенности компьютерных сетей, аппаратно-программные средства управления доступом к данным, стенды, Сигурд-М19 (автоматизированная система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок) – 1 шт., Шепот-М1 (автоматизированная система оценки защищенности выделенных помещений по виброакустическому каналу) – 1 шт.
114а	Лаборатория сетей и систем передачи информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор

		MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Astra Linux Special Edition	AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Защита информации от утечки по техническим каналам». разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только

знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Защита информации от утечки по техническим каналам».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями