МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет Информатики и Информационных Технологий

Кафедра информационных технологий и безопасности
компьютерных систем

Рабочая программа дисциплины

Техническая защита информации

Кафедра информационных технологий и безопасности компьютерных систем

Образовательная программа бакалавриата
10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Уровень высшего образования:
Бакалавриат

Форма обучения:
очная

Статус дисциплины:
входит в обязательную часть ОПОП

Махачкала
2022

Рабочая программа **«Техническая защита информации»** составлена в 2022 году в соответствии с требованиями ФГОС ВО - бакалавриат по направлению подготовки **10.03.01 Информационная безопасность** от 17 ноября 2020 г. №1427

Разработчик: кафедра Информационных технологий и безопасности компьютерных систем,

к.ф.-м.н., доцент Нурмагомедов Ш.А._____

Рабочая программа дисциплины одобрена на заседании кафедры Информационных технологий и безопасности компьютерных систем

от « 16» _03_ 2022 г., протокол № 8

Зав. кафедрой _____ Ахмедова З.Х.

на заседании Методической комиссии факультета Информатики и Информационных технологий от «_17_» _03_2022 г., протокол № 7.

Председатель _____ Бакмаев А.Ш.

Рабочая программа дисциплины согласована с учебно-методическим управлением «_____» _____ 2022 г.

Начальник УМУ ДГУ _____ Гасангаджиева А.Г.

Аннотация рабочей программы дисциплины.

Дисциплина «Техническая защита информации» входит в обязательную часть ОПОП бакалавриата по направлению 10.03.01 Информационная безопасность.

Содержание дисциплины направлено на формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения применять специальные знания для решения конкретных научно- практических задач и подготовить бакалавра к организации и проведению мероприятий по выявлению возможных технических каналов утечки информации на объектах информатизации и в выделенных помещениях.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных: ОПК-12, и профессиональных: ПК-2, ПК-8.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, лабораторные работы, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме коллоквиум, устный опрос и промежуточный контроль в форме экзамена.

Объем дисциплины составляет 6 зачетных единиц, в том числе в академических часах (216 часов) по видам учебных занятий

Очная форма обучения

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
5	72	60	30	30				12	
6	144	64	32	32				80	экзамен

1. Цели освоения дисциплины.

Целью дисциплины «Техническая защита информации» является формирование знаний в области принципов добывания (разведки) информации, способов организационно-технической и технической защиты информации, активных и пассивных способов и средств скрытия и защиты, способов и средств технической дезинформации, принципов технического контроля защищенности объектов.

Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Задачами дисциплины являются:

- изучение систем и средств инженерно-технической разведки, методов и способов организации защиты объектов активными и пассивными способами и техническими средствами, выбора оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации, нормативно-методических и правовых документов, регламентирующих вопросы технической защиты информации;
- формирование умения выявлять каналы утечки на конкретных объектах и оценивать их возможности;
- формирование умения определять рациональные меры защиты на объектах и оценивать уровень эффективности их защиты;

2. Место дисциплины в структуре ОПОП бакалавриата.

Дисциплина «Техническая защита информации» входит в базовый модуль образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность. Изучение её базируется на следующих дисциплинах: «Физика», «Теория вероятностей и математическая статистика», «Основы информационной безопасности», «Электротехника», «Электроника и схемотехника», «Аппаратные средства вычислительной техники», «Организационное и правовое обеспечение информационной безопасности».

Дисциплина «Техническая защита информации» является базовой дисциплиной профессионального цикла подготовки выпускной квалификационной работы.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины.

Код и наименование компетенции из ОПОП	*Код и наименование индикатора достижения*	*Планируемые результаты обучения*	*Процедура освоения*
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ИД 1 ОПК-12.1. Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта ИД 2 ОПК-12.2. Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ИД 3 ОПК-12.3. Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений	**Знает** принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта **Умеет** определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации **Владеет** навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений	Устный опрос, письменный опрос
ПК-2 Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации	ПК 2.1. Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации; ПК 2.2.Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией	**Знает:** Технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении; **Умеет**: проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; **Владеет**: Проведением контроля защищенности акустической речевой информации от утечки по техниче-	Устный опрос, письменный опрос

	ПК 2.3.Способом проведения специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации;	ским каналам	
ПК-8. Администрирование средств защиты информации в компьютерных системах и сетях	ПК-8.1. Теоретикочисловые методы и алгоритмы, применяемые в средствах защиты информации ПК-8.2. Решать сравнений по простому и составному модулям ПК-8.3. методами решения задач разложения больших целых чисел на множители	**Знает**: теоретические основы теории квантовой информации **Умеет**: решать типовые задачи и формулировать прикладные задачи в терминах теории квантовой информации **Владеет**: основными методами исследования, использующими теории квантовой информации	Устный опрос, письменный опрос

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины

Объем дисциплины составляет 6 зачетных единиц, 216 академических часа.

4.2. Структура дисциплины.

4.2.1. Объем дисциплины

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа (в т.ч. экзамен)	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1. Концепции инженерно-технической защиты информации								
1.	Основные понятия и определения. Системный подход к защите информации	5		4		4		2	Входной контроль, тест
2.	Основные концептуальные положения инженерно-технической защиты информации.	5		10		10		6	Опрос

	Итого за модуль 1.			14		14		8	
	Модуль 2. Теоретические основы инженерно-технической защиты информации								
1.	Источники опасных сигналов.	5		4		4			Опрос, тестирование
2.	Характеристики технической разведки	5		2		2		1	Опрос Отчет по работе
3.	Технические каналы утечки информации	5		4		4		1	Опрос Отчет по работе
4.	Методы инженерной защиты и технической охраны объектов	5		4		4		1	Опрос, тестирование Отчет по работе
5.	Методы скрытия информации и ее носителей.	5		4		4		1	Опрос. Отчет по работе
	Итого за модуль 2.			16		16		4	
	ИТОГО за семестр 5			**30**		**30**		**16**	
	Модуль 3. Физические основы защиты информации.								
1.	Физические основы побочных излучений и наводок	6		4		4		4	Опрос, тестирование
2.	Распространение сигналов в технических каналах утечки информации.	6		4		4		4	Тест, к/р, коллоквиум, тематическая дискуссия. Отчет по работе
3.	Физические процессы при подавлении опасных сигналов	6		4		4		4	Тест, к/р, коллоквиум, тематическая дискуссия. Отчет по работе
	Итого за модуль 3.			12		12		12	
	Модуль 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей								
1.	Средства технической разведки.	6		2		2		4	Тест, к/р, коллоквиум, тематическая дискуссия. Отчет по работе
2.	Средства инженерной защиты и технической охраны.	6		4		4		6	тематическая дискуссия
3.	Средства предотвращения утечки информации по техническим каналам	6		4		4		6	Опрос. Отчет по работе.
	Итого за модуль 4.			10		10		16	
	Модуль 5. Организационные основы инженерно-технической защиты информации.								
1.	Государственная система защиты информации.	6		2		2		4	тематическая дискуссия
2.	Методическое обеспечение инженерно-технической защиты информации	6		4		4		4	Опрос. Отчет по работе.

3.	Принципы оценки эффективности систем инженерно-технической защиты информации	6		4		4		8	тематическая дискуссия, опрос. Отчет по работе
	Итого за модуль 5.			10		10		16	
	Модуль 6. Подготовка к экзамену								
	Подготовка к экзамену	6						36	
	ИТОГО за семестр 6			32		32		80	

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине

Семестр 5

Модуль1. Концепция инженерно-технической защиты информации

1.1. Системный подход к защите информации.

Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Виды, источники и носители защищаемой информации.

1.2. Основные концептуальные положения инженерно-технической защиты информации.

Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации; методы и средства инженерной защиты и технической охраны объектов.

Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ; опасные сигналы и их источники. Понятие о текущей и эталонной признаковой структуре.

Модуль 2. Теоретические основы инженерно-технической защиты информации.

2.2. Источники опасных сигналов.

Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и краткая характеристика

основных и вспомогательных технических средств и систем. Образование опасных сигналов в результате побочных электромагнитных излучений и наводок.

2.2. Характеристика технической разведки.

Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

2.3. Технические каналы утечки информации.

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Опти-ческие, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности.

2.4. Методы инженерной защиты и технической охраны объектов.

Классификация способов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления охраной. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Автоматизация процессов охраны.

2.5. Методы скрытия информации и ее носителей.

Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления.

Семестр 6

Модуль 3. Физические основы защиты информации

3.1. Физические основы побочных излучений и наводок.

Акустоэлектрические преобразования. Побочные электромагнитные излучения и наводки. Источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Утечка опасных сигналов по цепям электропитания и заземления. Обнаружение и локализация закладных устройств, подавление их сигналов.

3.2. Распространение сигналов в технических каналах утечки информации.

Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Характеристика среды распространения сигналов различных технических каналов

утечки информации. Энергетическое скрытие акустических информативных сигналов

3.3. Физические процессы при подавлении опасных сигналов.

Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами. Подавление опасных сигналов акустоэлектрических преобразователей;

Модуль 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей

4.1.Средства технической разведки.

Структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; возмож-ности видов технической разведки; скрытие объектов наблюдения. Визуально-оптические приборы. Фотоаппараты. Оптоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах.

Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.

4.2. Средства инженерной защиты и технической охраны.

Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

4.3. Средства предотвращения утечки информации по техническим каналам.

Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления.

Модуль 5. Организационные основы инженерно-технической защиты информации.

5.1. Государственная система защиты информации.

Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.

Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств.

5.2. Методическое обеспечение инженерно-технической защиты информации.

Основные положения методологии инженерно-технической защиты информации; методы расчета и инструментального контроля показателей защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

5.3. Принципы оценки эффективности инженерно-технической защиты информации.

Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении. Принципы оценки размеров зон I и II. Оценка дальности перехвата сигналов.

4.3. 2. Содержание лабораторных занятий.

1. Лабораторная работа по теме "Системный подход к защите информации".
2. Лабораторная работа по теме "Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения".
3. Лабораторная работа по теме "Средства инженерно-технической защиты и технической охраны".
4. Лабораторная работа по теме "Распространение сигналов в технических каналах утечки информации".
5. Лабораторная работа по теме "Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания".
6. Лабораторные занятия по теме "Средства предотвращения утечки информации по техническим каналам"
7. Лабораторная работа по теме "Физические основы утечки информации по каналу побочных электромагнитных излучений и наводок".
8. Лабораторная работа по теме: "Определение основных показателей эффективности инженерно-технической защиты информации".

9. Лабораторная работа по теме "Контроль эффективности инженерно-технической защиты информации".
10. Лабораторная работа по теме "Моделирование процессов инженерно-технической защиты информации".

5. Образовательные технологии

Занятия проводятся в форме лекций и лабораторных работ. Материалы лекций демонстрируются с помощью мультимедийного оборудования, допускаются дискуссии, обсуждения, совместные решения типичных задач, связанных с практической деятельностью в рамках рассматриваемой темы. Лабораторные работы посвящены формированию основных практических навыков по дисциплине и призваны сформировать у студентов навыки самостоятельного решения задач. Часть заданий по лабораторным работам выполняется с использованием профессиональных технических средств инженерно-технической защиты информации, другая часть выполняется с привлечением персонального компьютера. Контроль осуществляется в форме проверки домашних заданий и контрольных работ, а также обсуждения отчётов по результатам выполнения лабораторных работ. В соответствии с требованиями ФГОС ВО по направлению подготовки предусмотрено широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, разбор конкретных моделей) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся, и в целом в учебном процессе составляет не менее 50% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ОПОП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 50% аудиторных занятий (определяется соответствующим ФГОС).

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Виды самостоятельной работы студентов, обеспечивающие реализацию цели и решение задач данной рабочей программы:

- подготовка к практическим (семинарским) занятиям;
- подготовка и сдача экзамена;
- конспектирование первоисточников.

Изучение тем дисциплины, выносимых для самостоятельного изучения студентами

№ п/п	Темы дисциплины	Форма (вид) самостоятельной работы для очной и очно-заочной форм обучения
1	Получение видовых характеристик объекта с помощью аппаратуры наблюдения. Возможности зрительной системы человека. Факторы, от которых зависит возможность образования оптического канала утечки информации.	Подготовка к опросу
2	Классификация радиоволн. Особенности распространения радиоволн различных диапазонов частот. Классификация и характеристики помех в радиоэлектронных каналах утечки информации.	Подготовка к опросу
3	Получение сигнальных характеристик объекта с помощью аппаратуры подслушивания.	Подготовка к опросу и тестированию
4	Особенности, характеризующие задачи технической защиты информации. Моделирование объектов и процессов защиты.	Подготовка к опросу
5	Основные направления инженерно- технической защиты информации в организации.	Подготовка к опросу
6	Выявление и описание источников информации. Требования к оформлению проекта системы (предложений) при представлении на согласование и утверждение.	Подготовка к выполнению лабораторных работ
7	Возможности слухового аппарата человека. Факторы, от которых зависит возможность образования акустического канала утечки информации.	Подготовка к опросу
8	Способы повышения дальности передачи информации в ультракоротком диапазоне радиоволн. Ослабления радиоволн при распространении через различные среды.	Конспект, тематический контроль

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Типовые контрольные задания.

1. На рисунке 1 представлена структурная схема

Рисунок 1 - Структурная схема канала утечки информации

- оптического канала утечки информации
- акустического канала утечки информации
- электронного канала утечки информации
- акустооптического канала утечки информации

2. На рисунке 2 представлена структурная схема

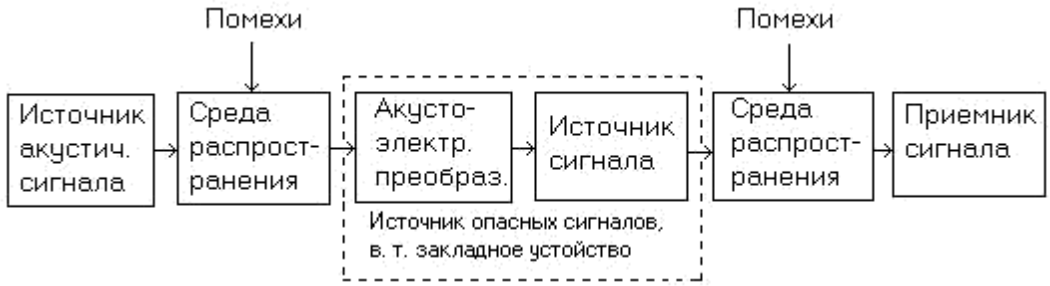


Рисунок 2 - Структурная схема канала утечки информации

- акустооптического канала утечки информации
- акусто-радиоэлектронного канала утечки информации
- радиоэлектронного канала утечки информации
- акустоэлектронного канала утечки информации

3. На рисунке 3 представлена структурная схема

Рисунок 3. Структурная схема канала утечки информации

- акустооптического канала утечки информации
- акусто- радиоэлектронного канала утечки информации
- радиоэлектронного канала утечки информации
- акустического канала утечки информации

4. Важнейшим свойством поверхности объекта, определяющий его цвет и яркость, является
- коэффициент отражения поверхности на различных частотах
- коэффициент отражения поверхности на средних частотах
- коэффициент отражения поверхности на низких частотах

• коэффициент отражения поверхности на высоких частотах

5. Одним из демаскирующих признаков объекта в ИК диапазоне является
• температура поверхности объекта
• электропроводность объекта
• площадь рассеяния объекта
• высота объекта

6. На рисунке 4 представлена структурная схема

Рисунок 4 - Структурная схема канала
• типовой структуры средства наблюдения
• типовой структуры средства передачи
• типовой структуры средства телевизионного наблюдения
• типовой структуры средства ИК наблюдения

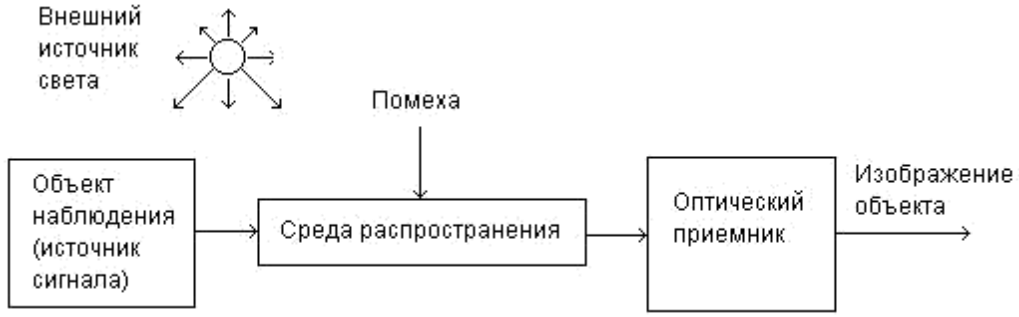
7. На рисунке 5 представлена структурная схема

Рисунок 5 - Структурная схема канала утечки
• акусто-радиоэлектронного канала утечки информации
• радиоэлектронного канала утечки информации
• радиоэлектронного канала утечки информации
• акустического канала утечки информации

8. На рисунке 6 представлена структурная схема

Рисунок 6 - Структурная схема канала утечки

- оптического канала утечки информации
- акустооптического канала утечки информации
- акусто-радиоэлектронного канала утечки информации
- радиоэлектронного канала утечки информации



9. Потенциальными излучателями _____ в виде ПЭМИН могут быть сигнальный кабель, видеоусилитель, потенциальный рельеф на экране кинескопа.

- видеосигнала
- электрического сигнала
- акустического сигнала
- электромагнитного сигнала

10. В _____ каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений и инженерные коммуникации.

- виброакустических
- акустоэлектрических
- акустических
- параметрических

11. _____ сложный акустический сигнал, основная энергия которого сосредоточена в диапазоне частот от 300 до 4000 Гц.

- тональный сигнал
- высокочастотный сигнал
- оптический сигнал
- речевой сигнал

12. Эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов используется в:

- индукционном канале утечки информации;
- электрическом канале утечки информации;
- электромагнитном канале утечки информации;
- параметрическом канале утечки информации.

Примерные вопросы для контроля.

1) Цели и задачи технической защиты информации.
2) Что представляет собой информация и носитель защищаемой информации?
3) Что собой представляет системный подход к защите информации?
4) Назовите основные параметры системы технической защиты информации?
5) Назовите основные направления инженерно-технической защиты информации?
6) Что собой представляет утечка информации?
7) Что собой представляет технический канал утечки информации?
8) Основные классификации технических каналов утечки информации?
9) Какие разновидности технических каналов утечки речевой информации вам известны?
10) Что такое "опасные сигналы"?
11) Что такое "демаскирующие признаки объектов наблюдения"?
12) Какие разновидности демаскирующих признаков вам известны?
13) Какие демаскирующие признаки сигналов вам известны?
14) Что собой представляют акустоэлектрические преобразования и как они способствуют утечке информации?
15) Какие типы технических каналов утечки (оптические, акустические, радиоэлектронные, материально-вещественные и т.д.) представляют наибольшую угрозу информационной безопасности?
16) Что собой представляют активные методы технической защиты информации?
17) Что собой представляют пассивные методы технической защиты информации?
18) Каковы основные принципы технической охраны объектов?
19) Какие методы скрытия информации и ее носителей вам известны?
20) Какова структура государственной системы защиты информации?
21) Какие государственные ведомства курируют область технической защиты информации?
22) Какова методика обследования контролируемого помещения на предмет наличия технических каналов утечки?
23) Какова методика обследования контролируемого помещения на предмет наличия устройств несанкционированного съёма информации?

24) Что собой представляет "закладное устройство"?
25) Какие способы классификации закладных устройств вам известны?
26) Какие демаскирующие признаки наиболее распространённых закладных устройств вам известны?
27) Каковы преимущества и недостатки закладных устройств, работающих в инфракрасном диапазоне?
28) Каковы принципы работы сканирующих радиоприемников и комплексов радиомониторинга?
29) Какие разновидности комплексов радиоконтроля и радиомониторинга вам известны?
30) Какие средства управления доступом вам известны?
31) Что такое "разборчивость речи"?
32) Какие методы подавления опасных акустических сигналов вам известны?
33) Каковы основные закономерности распространения акустических волн?
34) Каковы основные закономерности ослабления радиосигналов при их распространении?
35) Что собой представляют "побочные электромагнитные излучения" (ПЭМИ) и какова их физическая природа?
36) Что такое "наводки" и какова их физическая природа?
37) В чём состоит принцип действия кабеля типа "витая пара"?
38) Какие методы экранирования ПЭМИ вам известны?
39) Каковы основные принципы экранирования электрических полей?
40) Каковы основные принципы экранирования низкочастотных магнитных полей?
41) Какие функциональные узлы персонального компьютера являются наиболее активными источниками ПЭМИ?
42) Каковы основные принципы моделирования объектов технической защиты?
43) Каковы основные принципы моделирования технических каналов утечки информации?
44) Каковы основные принципы моделирования каналов технического добывания информации?

Примерные вопросы для экзамена

1. Понятие информации. Виды представления и классификация информации.
2. Понятия безопасности и системы безопасности информации. Системный подход к защите информации.
1. Угрозы конфиденциальной информации и их классификация.
2. Источники угроз безопасности информации, их классификация и ранжирование.

3. Уязвимости безопасности информации, их классификация и ранжирование.
4. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
5. Правовая и организационная защита информации.
6. Инженерно-техническая защита информации.
7. Классификация и общая характеристика каналов утечки информации.
8. ехнические каналы утечки информации и их образование.
9. Классификация и характеристика каналов утечки речевой информации.
10. Технические каналы утечки речевой информации и методы ее съема.
11. Методы дистанционного проникновения в помещение для скрытого съема аудио - и видеоинформации.
12. Технические средства съема аудиоинформации. Микрофоны и их виды.
13. Методы съема информации в телефонных линиях связи.
14. Технические средства съема видеоинформации и их общая характеристика.
15. Методы и средства съема информации по радиоканалу.
16. Методы и средства съема информации телевизионной и вычислительной техники.
17. Методы и средства съема информации в высокочастотных и волоконно-оптических кабелях.
18. Защита речевой информации с помощью маскирующих сигналов.
19. Системы виброакустического зашумления.
20. Защита речевой информации от лазерного съема.
21. Методы и средства обнаружения радиозакладных устройств. Индикаторы поля, панорамные сканирующие приемники, аппаратно-программные комплексы.
22. Методы и средства обнаружения радиозакладных устройств. Обнаружители диктофонов и нелинейные радиолокаторы.
23. Звукоизоляция помещений.
24. Общие принципы защиты телефонных линий связи. Методы и средства пассивной защиты.
25. Методы подавления телефонных закладных устройств.
26. Методы и средства обнаружения и противодействия в телефонных линиях связи.
27. Общая характеристика методов защиты информации от утечки по электромагнитным каналам.
28. Защита линий связи. Защита информации от утечки в волоконно-оптических линиях связи.
29. Защита информации от утечки за счет микрофонного эффекта.

30. Защита информации от утечки за счет электромагнитного излучения.
31. Защита информации от утечки за счет паразитной генерации, по цепям питания и по цепям заземления.
32. Защита информации от утечки за счет взаимного влияния проводов и линий связи и высокочастотного навязывания.
33. Экранирование технических средств и помещений.
34. Использование специализированных пленок, тканей, эмалей и ферритовых фильтров для защиты информации от утечки по электромагнитным каналам.
35. Детекторы видеокамер.
36. Применение радиоэлектронных помех для защиты информации от утечки по электромагнитному каналу.

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Контроль и оценка знаний студентов очной формы обучения осуществляется в соответствии с Положением о бально-рейтинговой системе контроля и оценки знаний студентов ДГУ. Программой дисциплины в целях проверки прочности усвоения материала предусматривается проведение различных форм контроля:

1. **Предварительный контроль** необходим для установления исходного уровня знаний студентов.
2. **Тематический контроль** определяет степень усвоения обучающимися каждого раздела (темы в целом), их способности связать учебный материал с уже усвоенными знаниями, проследить развитие, усложнение явлений, понятий, основных идей.
3. **Рубежной формой** контроля является экзамен Занятия проводятся в 5м и 6-семстрах 3 курса.

Период времени, отведенный на обучение по данной дисциплине, планируется разделить на модуля, каждый из которых заканчивается контрольной точкой. За текущую работу в семестре студент может заработать 60 баллов и 40 баллов составляет максимальная оценка за экзаменационный ответ. Количество баллов за текущую работу выставляется в соответствии со сложностью темы и количеством заданий, выносимых для практических работ в аудитории и самостоятельных занятий.

Изучение дисциплины завершается экзаменом, проводимым в виде устного опроса с учетом текущего рейтинга. Критерии рейтинга представлены в таблицах. Текущий рейтинг (max 60 баллов)

8. Учебно-методическое обеспечение дисциплины.

а) основная литература

1. Зайцев, А.П. Технические средства и методы защиты информации : учебник / Р.В. Мещеряков, А.А. Шелупанов, А.П. Зайцев, 7-е изд., испр., М, Горячая линия - Телеком, 2012, 443 с.
2. Бузов Г. А., Калинин СВ., Кондратьев А. В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия-Телеком, 2005. — 416 с: ил.
3. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/73641.— Режим доступа: для авторизир. пользователей
4. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89451.html. — Режим доступа: для авторизир. пользователей

б) дополнительная литература

1. Петраков,А.В. Основы практической защиты информации [Текст] : учеб. пособие для студентов вузов / А.В Петраков. – 2-е изд. – М. :Радио и связь, 2000. – 361с.
2. Государственная тайна и ее защита: Собр.законод.и нормат.актов. –М.: Ось-89, 2004. – 159с.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

Для усвоения дисциплины используются электронные базы учебно-методических ресурсов, электронные библиотеки.

Интернет ресурсы:

1. ЭБС IPRbooks:http://www.iprbookshop.ru/
2. Электронно-библиотечная сис*тема* «Университетская библиотека онлайн» www.biblioclub.ru.
3. Электронной библиотека на http://elibrary.ru.
4. Электронный каталог НБ ДГУ[Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru.
5. Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг.гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/
6. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru.
7. Сайт образовательных ресурсов Даггосуниверситетаhttp://edu.icc.dgu.ru
8. **Springer.** http://link.springer.com, http://materials.springer.com/
9. **Scopus:** https://www.scopus.com
10. **WebofScience:** webofknowledge.com
11. www.nanotech.ru

10. Методические указания для обучающихся по освоению дисциплины.

Примерным учебным планом на изучение дисциплины отводится два семестра. В конце 6 семестра в качестве итогового контроля предусмотрен экзамен. На подготовку и сдачу зачета и экзамена в соответствии с Госстандартом примерным учебным планом выделяется дополнительно 36 часов. В течение изучения дисциплины проводятся две контрольные работы практические и лабораторные работы.

Примерная программа обеспечивает реализацию системного подхода к образовательному процессу.

Он предусматривает:

- представление знаний по дисциплине в виде иерархической структуры (пирамиды), каждый уровень которой соответствует определенному уровню обобщения знаний: концепция инженерно-технической защиты, теория, физика, техника,

организация, методика. Последовательность изложения соответствует конкретизации знаний, рассмотренных на предыдущем уровне;

- лабораторные и практические работы объединены в единый цикл работ по единым разрабатываемым преподавателем сценариям, предусматривающих решение практических задач по обеспечению информационной безопасности на объекте защиты (помещении, здании, организации).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

1. Для проведения лекций и практических занятий по дисциплине целесообразно аудиторию оснастить средствами проекции на экран фотографий, рисунков, схем, чертежей, систематизированных блоков текста, таблиц, формул. Наибольшими возможностями обладают мультимедио-проекторы (ЖК-матрицы) и сканеры, сопряженные с ПЭВМ. Использование этих средств предусматривает предварительное создание необходимой видеоинформации на компьютере с помощью известных офисных программ и ввод ее в компьютер с помощью сканера. Кроме того, средства видеопроекции позволяют демонстрировать принципы работы изучаемых средств с помощью мультипликации, предварительно созданной с использованием анимационных компьютерных программ. Более дешевый и практически доступный вариант - использование для проекции видеоматериала, предварительно нанесенного на прозрачную пленку, оптических видеопроекторов типа «Пеленг». Сопровождение лекций видеоматериалами позволяет: более активно использовать студентами оптический канал восприятия информации, представлять в конспектах изучаемый материал в систематизированном и сжатом виде, сократить потери времени преподавателем на отображение материала на доске.

2. Расчеты и компьютерные лабораторные работы проводятся в компьютерных классах. Для выполнения лабораторных работ этой группы необходим, для оборудования одного рабочего места, компьютер не ниже 486 с мультиме-

дийным набором средств CD-ROM, звуковая карта, 2 электродинамических микрофона и акустическая система с соответствующим программным обеспечением.

3. Анализатор спектра с демодуляторами с полосой частот 9КГц-3ГГц. Интерфейс анализатора спектра с компьютером (GPIB, USB). Набор антенн электрических и магнитных антенн (полоса частот 9КГц-3ГГц). Эквивалент сети. Генераторы пространственного и линейного зашумления. Фильтры питания ФСП или аналогичные. Специализированное программное обеспечение для проведения специальных исследований средств вычислительной техники. Комплект аппаратуры для проведения акустических и вибрационных измерений в диапазоне частот от 88 до 11200 Гц.