МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и Информационных Технологий

Рабочая программа дисциплины

Техническая защита информации

Кафедра **Информатики и Информационных технологий**

Образовательная программа

10.03.01 Информационная безопасность

Профиль подготовки:
Безопасность компьютерных систем

Уровень высшего образования:
Бакалавриат

Форма обучения: очная

Статус дисциплины: базовая

Махачкала, 2018

Рабочая программа дисциплины «Техническая защита информации» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01– Информационная безопасность
(уровень: бакалавриата) от «01» декабря 2016 г. № 1515.

Составитель: Ахмедова З.Х, доцент каф. ИИиТ

Рабочая программа одобрена на заседании кафедры «Информатики и информационных технологии».

Протокол № 12 от 02.07 2018г

Зав кафедрой ИииТ _____ С.А. Ахмедов

Одобрена на заседании Методической комиссии факультета Информатики и информационных технологий

Протокол № 10 от 03.07 2018г

Председатель _____ Камилов К.Б.

Рабочая программа согласована с учебно-методическим управлением

4.07 2018г _____

Аннотация рабочей программы дисциплины.

Дисциплина «Техническая защита информации» входит в базовую часть образовательной программы бакалавриата по направлению 10.03.01 Информационная безопасность.

Содержание дисциплины направлено теоретически и практически 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-3, ОПК -7, профессиональных: ПК-1, ПК-6.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, 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 5 зачетных единиц, в том числе в академических часах по видам учебных занятий

Семестр		Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	Общая трудоемкость	в том числе							
		Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		Всего	из них						
			Лекции	Лабораторные занятия	Практические занятия		контроль		
6-7	180	88	54	18	16		36	56	экзамен

1. Цели освоения дисциплины.

Целью дисциплины «Техническая защита информации» является формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий.

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

Задачи дисциплины - дать знания:

- по концепции инженерно-технической защиты информации;
- теоретическим основам инженерно-технической защиты информации;
- физическим основам инженерно-технической защиты информации;
- по техническим средствам добывания
- по техническим средствам добывания и защиты информации;
- по организационным основам инженерно-технической защиты информации;
- по методическому обеспечению инженерно-технической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП бакалавриата.

Дисциплина «Техническая защита информации» входит в базовую часть образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность. Изучение еѐ базируется на следующих дисциплинах: «Математика», «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 компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ОПК -3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знает: принципы организации информационных систем в соответствии с требованиями по защите информации; Умеет: применять на практике методы анализа электрических цепей; Владеет: методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - профессиональной терминологией;
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает: эталонную модель взаимодействия открытых систем методы коммутации и маршрутизации, сетевые протоколы; Умеет: анализировать и оценивать степень риска проявления факторов опасности системы «человек – среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности; Владеет: навыками безопасного использования технических средств в профессиональной деятельности.
ПК -1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает: основные требования по защите информации; Умеет: организовать работу малого коллектива исполнителей с учетом требований защиты информации; Владеет: навыками управления информационной безопасностью
ПК - 6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знает: возможные последствия аварий, катастроф, стихийных бедствий; Умеет: использовать основные методы защиты; Владеет: навыками защиты производственного персонала и населения

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 5 зачетных единиц, 180 академических часа.

4.2. Структура дисциплины.

№ п/п	Названия разделов и тем	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоят. работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практ. занятия	Лабор. работы	КСР		
	Модуль 1. Концепции инженерно-технической защиты информации								
1	Основные понятия и определения	6	1	4	2				Входной контроль, тест
2	Классификация и структура технических каналов утечки информации.	6	2	4	4	-		4	Опрос
3	Характеристики каналов утечки информации	6	3	4	2	-		4	Опрос
4	Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы.			4				4	Опрос
	Итого за модуль:			16	8	-		12	
	Модуль 2. Теоретические основы инженерно-технической защиты информации								
1	Оптические каналы утечки информации	6	4-6	4	4	-	2	4	коллоквиум
2	Радиоэлектронные каналы утечки информации	6	7-8	4	4	-	2	6	Опрос, тестирование
3	Источники опасных сигналов.			4					Опрос,
4	Характеристика			6					Опрос,

	технической разведки**.**								
	Итого за модуль:			18	8	-		10	
		Модуль 3. Физические основы защиты информации.							
1	Акустические каналы утечки информации	7	1	4		4		6	Опрос тестирование
2	Материально-вещественные каналы утечки информации	7	2	4		2		4	Тест, к/р, коллоквиум, тематическая дискуссия Отчет по работе
3	Системный подход к инженерно-технической защите информации	7	3	2		4		6	Тест, к/р, коллоквиум, тематическая дискуссия Отчет по работе
	Итого за модуль:			10		10		16	
		Модуль 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей							
1	Основные этапы проектирования системы защиты информации техническими средствами	7	4	4		2		8	Тест, к/р, коллоквиум, тематическая дискуссия Отчет по работе
2	.Средства технической разведки.			4		4		8	тематическая дискуссия
3	Организационные основы инженерно-технической защиты информации.			2		2		2	тематическая дискуссия
	Итого за модуль:			10		8		18	
		Модуль 5. Подготовка к экзамену						36	
	ИТОГО:		180	54	16	18		92	

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

4.3.1. Содержание лекционных занятий по дисциплине

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.

Модуль 2. Теоретические основы инженерно-технической защиты информации.

2.1. Информации как предмет защиты.

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.

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.

2.3. 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.

2.4. Технические каналы утечки информации.

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

2.5. 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.

2.6. 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.

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; возможности 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.

4.1. 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.

4.2. 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.

Раздел 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. Контроль 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.

Раздел 6. Методическое обеспечение инженерно-технической защиты информации.

6.1. Моделирование 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. Методи-

ческие рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

6.2. Принципы оценки 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 практических занятий.

Темы практических занятий объединены сценарием разработки мер защиты объекта (помещения) с конкретными параметрами.

1. Определение источников защищаемой информации и уровня ее безопасности.
2. Определение угроз безопасности информации в помещении.
3. Расчет уровней опасных сигналов в помещении и в выходящих из помещения проводах кабелей.
4. Расчет зон I и II для основных технических средств и систем, размещенных в помещении.
5. Расчет уровней речевых сигналов в местах возможного нахождения злоумышленника или его подслушивающих технических средств.
6. Определение разрешения объектов защиты (людей, документов на столах, плакатов на стенах, продукции и др.) возможного наблюдения с использованием современных визуально-оптических и оптико-электронных приборов.
7. Определение вариантов мер защиты с оценкой затрат на их обеспечение

5.Образовательные технологии

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
1	Основные понятия и определения.	Подготовка к опросу
2	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
3	Классификация радиоволн. Особенности распространения радиоволн различных диапазонов частот. Классификация и характеристики помех в радиоэлектронных каналах утечки информации.	Подготовка к опросу
4	Получение сигнальных характеристик объекта с помощью аппаратуры подслушивания.	Подготовка к опросу и тестированию

5	Особенности, характеризующие задачи технической защиты информации. Моделирование объектов и процессов защиты.	Подготовка к опросу
6	Основные направления инженерно- технической защиты информации в организации.	Подготовка к опросу
7	Выявление и описание источников информации. Требования к оформлению проекта системы (предложений) при представлении на согласование и утверждение.	Подготовка к выполнению лабораторных работ
8	Возможности слухового аппарата человека. Факторы, от которых зависит возможность образования акустического канала утечки информации.	Подготовка к опросу
9	Способы повышения дальности передачи информации в ультракоротком диапазоне радиоволн. Ослабления радиоволн при распространении через различные среды.	Конспект, тематический контроль

Рекомендуемая литература (основная и дополнительная).

а)основная:

1. Альбрехт С., Венц Дж., Уильямс Т.. Мошенничество. Луч света в темные стороны бизнеса. - С.-Пб.: "ПИТЕР", 2015 г.

2. Н. Боттом, Р. Галатти.. Экономическая разведка и контрразведка. Практическое пособие. Новосибирск, 2014 г., 414 с, пер. с англ.

3. Ч. Хант, В. Зартарьян.. Разведка на службе вашего предприятия, киев, 2008 г., 168 с, пер. с франц.

б) дополнительная:

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации / Под ред. Ю.С. Ковтанюка – К.: Издательство "ЮНИОР", 2003. – 504 с.

2. Калинцев Ю.К. Разборчивость речи в цифровых вокодерах. М.: Радио и связь, 1991. – 220 с.

3. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: ООО "Издательство

"Полигон", 2000. – 896 с.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ОПК -3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знает: принципы организации информационных систем в соответствии с требованиями по защите информации; Умеет: применять на практике методы анализа электрических цепей; Владеет: методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - профессиональной терминологией;	- собеседование, дискуссия -отчеты к практическим занятиям
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает: эталонную модель взаимодействия открытых систем методы коммутации и маршрутизации, сетевые протоколы; Умеет: анализировать и оценивать степень риска проявления факторов опасности системы «человек – среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности; Владеет: навыками безопасного использования технических средств в профессиональной деятельности.	- собеседование, дискуссия -отчеты к практическим занятиям

ПК -1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает: основные требования по защите информации; Умеет: организовать работу малого коллектива исполнителей с учетом требований защиты информации; Владеет: навыками управления информационной безопасностью	- собеседование, дискуссия -отчеты к практическим занятиям - тесты - ситуационные задачи - электронный практикум
ПК - 6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знает: возможные последствия аварий, катастроф, стихийных бедствий; Умеет: использовать основные методы защиты; Владеет: навыками защиты производственного персонала и населения	- собеседование, дискуссия -отчеты к практическим занятиям - тесты - ситуационные задачи - электронный практикум

7.2. 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
- акустОПОПтического канала утечки информации

2. На рисунке 2 представлена структурная схема

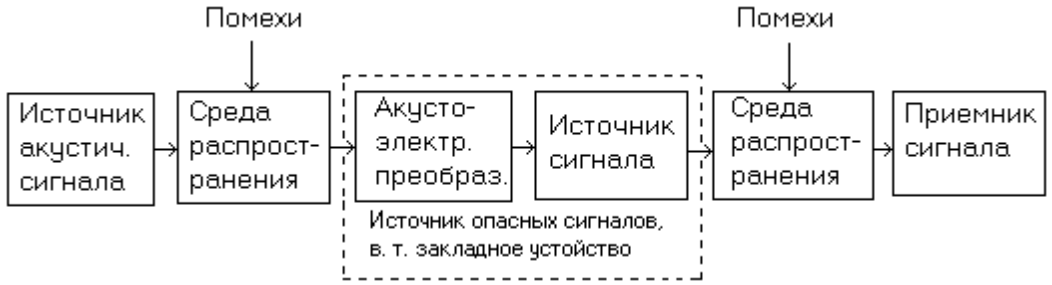

Рисунок 2 - Структурная схема канала утечки информации

- акустОПОПтического 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

- акустОПОПтического 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

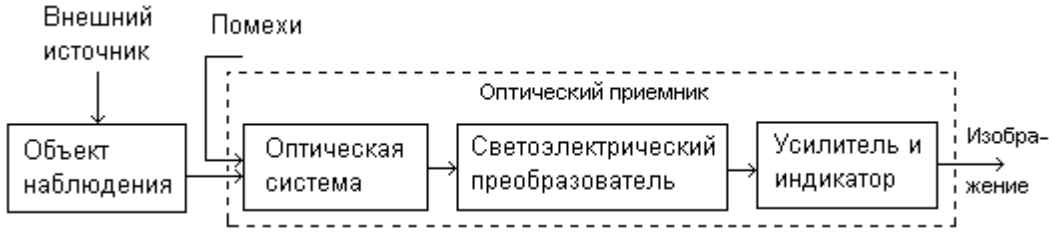

Рисунок 4 - Структурная схема канала

• 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

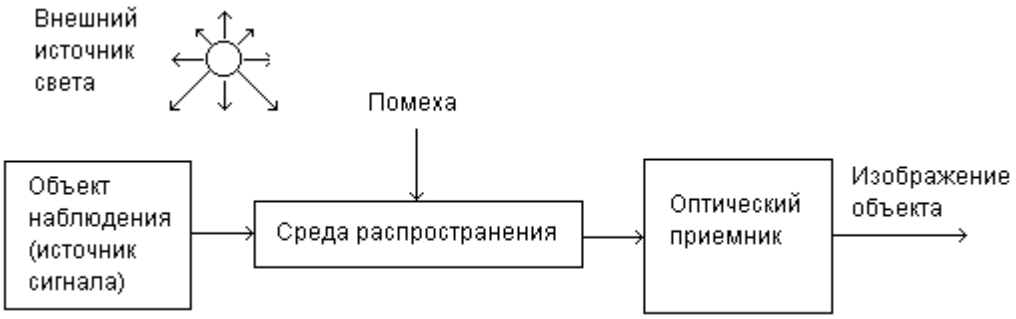

Рисунок 6 - Структурная схема канала утечки

- оптического канала утечки информации
- акустОПОПтического 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.

7.3. 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 во 6-м семестре 3 курса и 7-ом семестре 4 курса. Период времени, отведенный на обучение по данной дисциплине, планируется разделить на 4 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. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература

1. Девянин, Пётр Николаевич. Модели безопасности компьютерных систем [Текст]: учеб. пособие для студентов вузов, обуч. по специальностям 075200 "Компьютерная безопасность" и 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" / Девянин, Пётр Николаевич. - М. : Academia, 2005. - 142,[1] с. - (Высшее профессиональное образование. Информационная безопасность).

2. Рагозин Ю.Н. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю.Н. Рагозин. — Электрон. текстовые данные. — СПб. : Интермедия, 2018. — 168 c. — 978-5-4383-0161-5. — Режим доступа: http://www.iprbookshop.ru/73641.html [Свободный доступ]

3. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52161.html **[Свободный доступ]**

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.

1. eLIBRARY.Ru [Электронный ресурс]: электронная библиотека / Науч. электр. б-ка.- МОСКВА.1999. – Режим доступа: http//elibrary.ru (дата обращения 15.04.2018). – Яз. рус., англ.
2. Электронный каталог НБ ДГУ Ru [Электронный ресурс]: база данных содержит сведения о всех видах лит., поступающих в фонд НБ ДГУ / Дагестанский гос.унив. – Махачкала. – 2010. – Режим доступа: http//elib.dgu.ru. свободный (дата обращения 11.03.2018)
3. Национальный Открытый Университете «ИНТУИТ» [Электронный ресурс]: электронно-библиотечная система, издательство «Лань» - www.intuit.ru (дата обращения 12.03.2018).

10. Методические указания для обучающихся по освоению дисциплины.

Примерным учебным планом на изучение дисциплины отводится один семестр. В конце семестра в качестве итогового контроля предусмотрен экзамен. На подготовку и сдачу зачета и экзамена в соответствии с Госстандартом и 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 мультимедийным набором средств D-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.