МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Дагестанский государственный университет»

Факультет Информатики и Информационных технологий

Рабочая программа

Техническая защита информации

Кафедра **Информатики и Информационных технологий**

Образовательная программа

10.03.01- Информационная безопасность

Профиль подготовки:
Безопасность компьютерных систем

Уровень высшего образования:
Бакалавр

Форма обучения: очная

Статус дисциплины: базовая

Махачкала 2017

Рабочая программа по дисциплине «Техническая защита информации» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01- Информационная безопасность от «01» XII 2016 г. № 1515

Составитель: Ахмедова З.Х, доцент каф. ИИиТ

Рабочая программа одобрена на заседании кафедры Информатики и информационных технологии

Протокол № 8 от 04.03 2017г

Зав кафедрой ИииТ С.А. Ахмедов

Одобрена на заседании Методической комиссии факультета Информатики и информационных технологий

Протокол № 7 от 29.03 2017г

Председатель Камилов К.Б.

Рабочая программа согласована с учебно-методическим управлением

29.03 2017г

2

Аннотация

Дисциплина«Техническая защита информации» входит в базовую часть образовательной программы бакалавриатапо направлению10.03.01.-Информационная безопасность.

Содержание дисциплины направленотеоретически 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:профессиональных -ПК-5.

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 опросипромежуточный контроль в форме экзамена.

Объем дисциплины 5 зачетных единиц, в том числе в академических часах по видам учебных занятий

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

1. Цели и задачи 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 ООП ВО.

Дисциплина «Техническая защита информации» относится к базовой части профессионального цикла. 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.

В результате изучения дисциплины студенты должны иметь представление:

- о задачах, структуре и возможностях технической разведки, основных этапах и процессах добывания ею информации;
- о физических процессах в технических средствах и системах, способствующих утечке защищаемой информации;
- о характеристиках используемых и перспективных технических средств

добывания и защиты информации;

- о государственной системе защиты информации и ее основных документах;

знать:

- виды, источники и носители защищаемой информации;
- основные угрозы безопасности информации;
- концепцию инженерно-технической защиты информации;
- основные принципы и методы защиты информации;
- основные руководящие и нормативные документы по инженерно-технической защите информации;
- порядок организации инженерно-технической защиты информации;

уметь:

- выявлять угрозы и технические каналы утечки информации;
- описывать (моделировать) объекты защиты и угрозы безопасности информации;
- применять наиболее эффективные методы и средства инженерно-технической защиты информации;
- контролировать эффективность мер защиты;

владеть:

- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- профессиональной терминологией.
- инженерными расчетами размеров контролируемой зоны.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ПК-5	способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий	Знать:принципы организации информационных систем в соответствии с требованиями по защите информации; - эталонную модель взаимодействия открытых системметоды коммутации и маршрутизации, сетевые протоколы; Уметь: применять на практике методы анализа электрических цепей; - анализировать и оценивать степень риска проявления факторов опасности системы"человек - среда обитания",

	защиты информации	осуществлять и контролировать выполнение требований по охранетруда и технике безопасности в конкретной сфере деятельности Владеть:методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - профессиональной терминологией; -навыками безопасного использования технических средств в профессиональной деятельности.

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 4 зачетные единицы,

144академических 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 ин-формации 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 технической разведки**.**			6					Опрос,
	Итого за модуль:			18	8	-		10	
		Модуль 3. Физические основы защиты информации.							
1	Акустические каналы утечки информации	7	1	4		4		6	Опростестирование
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).

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 охраныобъектов. 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 опасныхсигналов 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. Методические 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. 1. Темы 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, выбор рациональных вариантов.

4.3.2. Лабораторный практикум

Лабораторные работы могут быть двух видов:

1. демонстрационные лабораторные работы:

2. моделирующие лабораторные работы.

Демонстрационные лабораторные работы представляют собой рассказ и показ преподавателем принципов работы и применения современных технических средств обеспечения информационной безопасности, которые в силу их высокой стоимости могут быть приобретены в единичном количестве. К таким средствам относятся:

1. закладные устройства (2-3 вида);
2. поисковый прибор для демонстрации поиска радиоизлучающих и закладных закладных устройств в помещении;
3. сканирующий радиоприемник с интерфейсом для информационно- технического сопряжения ПЭВМ и программным обеспечением для обработки на ней принимаемых сигналов;
4. нелинейный локатор для поиска дистанционно-управляемых закладных устройств.

Для наглядного представления физических условий обеспечения информационной безопасности при изучении методов и средств защиты информации от скрытного наблюдении и подслушивании целесообразно вместо дорогостоящей измерительной аппаратуры проводить лабораторные работы путем моделирования изучаемых процессов добывания и защиты информации на ПЭВМ. При этом в качестве программного обеспечения таких работ используются программы графических редакторов и обработки звука.

Для выполнения лабораторных работ этой группы необходим для оборудования одного рабочего места компьютер не ниже 486 с мультимедийным набором средств (СБ-КОМ, звуковая карта, 2 электродинамических микрофона и акустическая система) и соответствующим программным обеспечением.

5.Образовательные технологии

В соответствии с требованиями ГОС ВОпо 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 вцелом в учебном процессе составляет не менее50% аудиторных занятий(определяется требованиями ГОС с учетом специфики

ООП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 50% аудиторных занятий (определяется соответствующим ГОС).

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 выполнению лабораторных работ.
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

Примерный перечень вопросов к экзамену по всему курсу

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС).
2. Технический канал утечки информации (определение). Схема технического канала утечки информации.
3. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).
4. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.
5. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.
6. Линейные и энергетические характеристики акустического поля.
7. Основные характеристики речи и речевого сигнала.
Разборчивость речи.
8. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.

9. Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные возможности, схема канала перехвата).
10. Дальность перехвата речевого сигнала средством акустической разведки направленными микрофонами.
11. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.
12. Способы и средства наблюдения. Факторы, влияющие на эффективность обнаружения и распознавания объектов наблюдения.
13. Структура и основные характеристики средств наблюдения.
14. Принципы работы и характеристики приборов ночного видения.
15. Структура средств перехвата и их функции.
16. Классификация и характеристики антенн.
17. Структура радиоприемника и его характеристики.
18. Параметры слуховой системы человека.
19. Принципы работы и характеристики диктофонов для скрытной записи.
20. Классификация и характеристики закладных устройств.
21. Способы и средства лазерного подслушивания и ВЧ-навязывания.
22. Способы и возможности определения демаскирующих признаков веществ.
23. Способы комплексного использования злоумышленниками технических каналов утечки информации.
24. Характеристики среды распространения оптических лучей.
25. Основные показатели оптоэлектронных линий связи и способы снятия с них информации.
26. Структура материально-вещественного канала утечки информации и характеристики ее элементов.
27. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде.
28. Особенности утечки информации о радиоактивных веществах.
29. Принципы физического и химического анализа веществ.
30. Цели и задачи технической защиты информации.

Рекомендуемая литература (основная и дополнительная) для СРС.

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

Компетенция	Знания, умения, навыки	Процедура освоения
ПК-5	Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Российской Федерации, по техническому и экспортному контролю в данной области; Уметь: применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; Владеть: методами расчета и инструментального	- собеседование, дискуссия -отчеты к практическим занятиям - тесты - ситуационные задачи - электронный практикум

	контроля показателей технической защиты информации;	

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания.

ПК- 5

Схема оценки уровня формирования компетенции

«способностью организовывать и поддерживать выполнениекомплекса мер по информационной безопасности, управлятьпроцессом их реализации с учетом решаемых задач иорганизационной структуры объекта защиты, внешнихвоздействий, вероятных угроз и уровня развития технологий защиты информации»

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних	Знает, но допускаетошибки при выполнение комплекса мер по информационной безопасности, не может управлять процессом их реализации с учетом решаемых задач и защиты, внешних воздействий, вероятных угроз.	Достаточно хорошо владеет способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов.	Свободно обладает способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и

	воздействий, вероятных угроз и уровня развития технологий защиты информации			экспортному контролю

7.3. 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

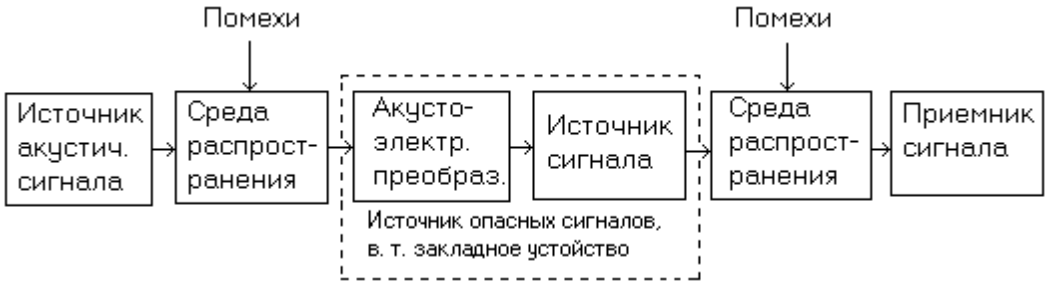

Рисунок 2 - Структурная схема канала утечки информации

- 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

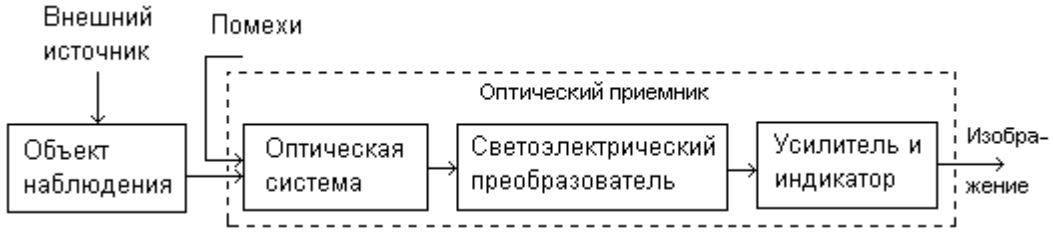

Рисунок 4 - Структурная схема канала

- 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

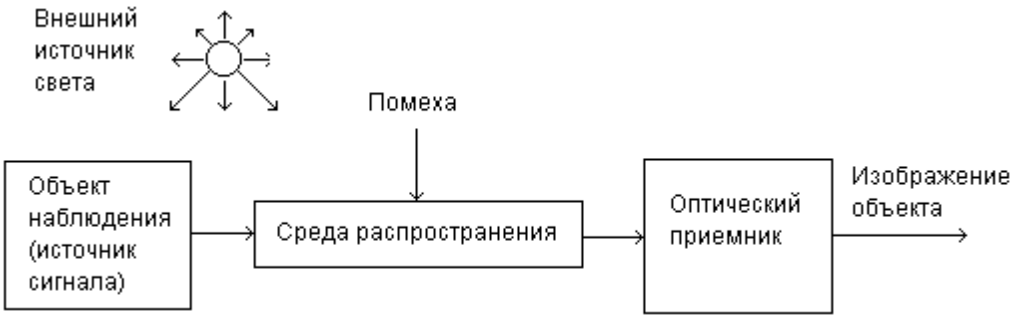

Рисунок 6 - Структурная схема канала утечки

• 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.

7.4. 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 балльно-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 (max60 баллов)

Показатель	Содержание показателя	Баллы
П1	Посещение всех лекций	max 5 баллов
П2	Присутствие на всех практических и лабораторных занятиях	max 5 баллов
П3	Оценивание работы на практических занятиях	max30 баллов
П4	Оценивание самостоятельной работы	max20 баллов

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература

1.Зайцев А. П. Технические средства и методы защиты информации : учеб. пособие для студентов вузов / под ред. А. П. Зайцева, А.А. Шелупанова. – изд.

4-е испр. и доп. - М. : Горячая линия- Телеком, 2012.

2.Торокин А. А. Основы инженерно-технической защиты информации: учебник для вузов / А. А. Торокин. – М. : Ось, 2013.

3. Хорев А.А. Техническая защита информации : учеб. пособие для студентов вузов. В 3 т. / А. А. Хорев. — М. : Аналитика, 2014

б) дополнительная литература

1.Анимов В. П. Блокировка акустоэлектрических преобразователей в электронных технических средствах и системах общего применения: сборник рекомендаций / В. П. Анимов, И. В. Коровин, В. И. Рыбальченко. – М. : Гелиос АРВ, 2010.

2. Бузов Г. А. Защита от утечки по информации техническим каналам : учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005.

3. Лунегов А.Н. Технические средства и способы добывания и защиты информации : учебник для вузов / А. Н. Лунегов. – М.: ВНИИ, 2009.

4. Меньшаков Ю. К. Виды и средства иностранных технических разведок : учебник для вузов / Ю. К. Меньшаков. – М.: МГТУ им. Н.Э. Баумана, 2009.

5. Меньшаков Ю.К. Теоретические основы технических разведок: учебник для вузов/ Ю. К. Меньшаков. – М.: МГТУ им. Н. Э. Баумана, 2008

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

1. Трушин В. А. Защита конфиденциальной информации от утечки по цепям электропитания : учебно-методическое пособие / В. А. Трушин, С. В. Быков ; Новосиб. гос. техн. ун-т. - Новосибирск, 2007. - 34, [1] с. : схемы, табл.. - Режим доступа: http://www.ciu.nstu.ru/fulltext/textbooks/2007/trushin.pdf. - Инновационная образовательная программа НГТУ "Высокие технологии".

2. Быков С. В. Защита информации от утечки по каналам побочных электромагнитных излучений (ПЭИТ) : учебно-методическое пособие / С. В.

Быков, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2008. - 41, [2] с. : ил., табл.. - Режим доступа: http://www.library.nstu.ru/fulltext/metodics/2008/bik.rar

3. Теличко Е. А. Теория и практика применения нелинейного локатора : учебно-методическое пособие / Е. А. Теличко, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2007. - 25, [2] с. : ил.. - Режим доступа: http://**www.library.nstu.ru/fulltext/metodics/2007/trushin.rar**

4. Исследование возможностей и особенностей применения программно-аппаратного комплекса радиомониторинга RS turbo : методическое пособие к лабораторному практикуму / Новосиб. гос. техн. ун-т ; [сост. С. В. Быков]. - Новосибирск, 2007. - 20, [2] с. : схемы, ил., табл.. - Режим доступа: http://**www.library.nstu.ru/fulltext/metodics/2007/3386.rar**

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 обладаютмультимедио-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.