МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в оптических системах
(*наименование дисциплины*)

кафедра Информатики и информационных технологий
(*наименование кафедры, обеспечивающей преподавание дисциплины*)

Образовательная программа
10.03.01 – Информационная безопасность
(*код и наименование направления/специальности*)

Профиль подготовки
Безопасность компьютерных систем
(*наименование профиля подготовки*)

Уровень высшего образования
Бакалавриат
(*Бакалавриат, специалитет, магистратура*)

Форма обучения
Очная
(*очная, очно-заочная, заочная*)

Статус дисциплины
Вариативная по выбору
(*базовая, вариативная, вариативная по выбору*)

Махачкала 2018

Рабочая программа по дисциплине «Защита информации в оптических системах» составлена в 2018 году в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 10.03.01 – Информационная безопасность (уровень бакалавриата), утверждённого приказом Минобрнауки РФ от 01.12.2016 № 1515.

Разработчик: _____ д. ф.-м. н. Алиев А. Р., проф. каф. ИиИТ

Рабочая программа дисциплины одобрена на заседании кафедры Информатики и информационных технологий.

Протокол № __7_____ от __22 февраля _____ 2018 г.

Зав. кафедрой ИиИТ _____ С. А. Ахмедов

Рабочая программа дисциплины одобрена на заседании методической комиссии факультета Информатики и информационных технологий.

Протокол № ___1_____ от _6 марта _____ 2018 г.

Председатель методической комиссии факультета ИиИТ _____ К. Б. Камилов

Рабочая программа дисциплины согласована с Учебно-методическим управлением.

_____

14 марта _____ 2018 г.

Аннотация рабочей программы дисциплины

Дисциплина «Защита информации в оптических системах» входит в вариативную часть образовательной программы бакалавриата по направлению (специальности) 10.03.01 – Информационная безопасность. Дисциплина реализуется на факультете Информатики и информационных технологий в 6-м семестре кафедрой Информатики и информационных технологий.

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: профессиональных – ПК-1, ПК-5.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости: текущий контроль в форме устного опроса по результатам лабораторных работ, промежуточный контроль в форме контрольных работ и коллоквиумов и итоговый контроль в форме зачёта.

Объем дисциплины 3 зачётные единицы, в том числе в академических часах по видам учебных занятий:

Семестры	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе зачет	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	Консультации		
6	108	86	18	34	34			22	зачет

1. Цели и задачи освоения дисциплины

Целью изучения дисциплины «Защита информации в оптических системах» 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.
Основными задачами изучения дисциплины является дать знания:
• по концепции инженерно-технической защиты информации;
• по теоретическим основам инженерно-технической защиты информации;
• по физическим основам инженерно-технической защиты информации;
• по техническим средствам добывания и защиты информации;
• по организационным основам инженерно-технической защиты информации;
• по методическому обеспечению инженерно-технической защиты информации.
Настоящий курс предназначен для обучения студентов основам инженерно-технической защиты информации, навыкам и умению в применении знаний для конкретных условий. Курс состоит из лекций, практических и лабораторных работ. Теоретический материал, который дается на лекциях, и практический материал, который даётся на лабораторных занятиях, взаимосвязаны. Поэтому для полного усвоения курса необходимо разобрать теоретический материал и выполнить все лабораторные работы.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Защита информации в оптических системах» входит в вариативную (по выбору) часть образовательной программы бакалавриата по направлению 10.03.01 – Информационная безопасность. Дисциплина реализуется на факультете Информатики и информационных технологий Дагестанского государственного университета кафедрой Информатики и информационных технологий.
Изучение «Защиты информации в оптических системах» 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 «Защита информации в оптических системах» 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.
Выпускник, освоивший программу бакалавриата, должен обладать следующими компетенциями. Профессиональные: способность 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 защиты информации (ПК-5); способность проводить предпроектное обследование объекта проектирования, системный анализ предметной области, их взаимосвязей (ПК-1).

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО по данному направлению:

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ПК-5	Способность организовывать и поддерживать выполнение комплекса	Знать: - принципы организации информационных систем в соответствии с требованиями по

	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 защиты информации.	защите информации; - эталонную модель взаимодействия открытых систем, методы 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», - осуществлять и контролировать выполнение требований по охране труда 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.
ПК-1	Способность проводить предпроектное обследование объекта проектирования, системный анализ предметной области, их взаимосвязей.	Знать: основные подходы к описанию моделей сложных систем и соответствующие формальные модели (клеточные автоматы, графы событий, агрегированные системы, DEVS формализм и т.д.). Уметь: обосновывать выбор способа представления модели и программных средств её реализации. Владеть:

		практическими навыками по использованию средств вычислительной техники и программного обеспечения для организации обработки информации и решения задач.

4. Объем, структура и содержание дисциплины.

Дисциплина «Защита информации в оптических системах» преподаётся на факультете Информатики и информационных технологий ДГУ в 6-м семестре.

4.1. Объем дисциплины и виды учебной работы (в часах).
Общая трудоемкость дисциплины составляет 108 часов, 3 зачётных единиц. Из них 86 часов аудиторной работы и 22 часа самостоятельной работы. Аудиторная работа включает 18 часов лекционных занятий, 34 часа практических занятий, 34 часа лабораторных занятий.
4.2. Структура дисциплины.

Семестр	Раздел (модуль) дисциплины	Недели семестра	Виды учебной работы, и трудоемкость, в час.			Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра). Форма промежуточной аттестации (по семестрам)
			Лекции	Практические работы	Лабораторные работы		
Модуль 1. Концепции инженерно-технической защиты информации							
6	Основные понятия и определения.	1–2	2	2	2	2	Устный опрос, тестирование.
6	Классификация и структура технических каналов утечки информации.	3–4	2	4	4	4	Устный опрос, тестирование, защита лаб. раб.
6	Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы.	5–6	2	4	4	4	Устный опрос, тестирование, защита лаб. раб.
6	Итого за 1-й модуль:	1–6	6	10	10	10	36

Модуль 2. Теоретические основы защиты информации в оптических системах.							
6	Оптические каналы утечки информации.	7–8	2	4	4	2	Устный опрос, тестирование, защита лаб. раб.
6	Радиоэлектронные каналы утечки информации.	9–10	2	4	4	2	Устный опрос, тестирование, защита лаб. раб.
6	Характеристика технической разведки.	11–12	2	4	4	2	Устный опрос, тестирование, защита лаб. раб.
6	Итого за 2-й модуль.	7–12	6	12	12	6	36
Модуль 3. Физические основы защиты информации.							
6	Акустические каналы утечки информации.	13–14	2	4	4	2	Устный опрос, тестирование, защита лаб. раб.
6	Материально-вещественные каналы утечки информации	15–16	2	4	4	2	Устный опрос, тестирование, защита лаб. раб.
6	Системный подход к инженерно-технической защите информации.	17–18	2	4	4	2	Устный опрос, тестирование, защита лаб. раб.
6	Итого за 3-й модуль.	13–18	6	12	12	6	36
6	Всего	1-18	18	34	34	22	108

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1. Концепция инженерно-технической защиты информации

Тема 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.

Тема 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

Тема 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.
Тема 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.
Тема 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.
Тема 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.
Тема 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.
Тема 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

Тема 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.
Тема 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 и различных технических каналов утечки информации. Энергетическое скрытие акустических информативных сигналов.
Тема 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.

4.4. 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.

4.5. Программа лабораторного практикума

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 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 ФГОС ВПО по направлению подготовки и реализации компетентностного подхода в учебном процессе предусмотрены следующие образовательные технологии:

– лекции: устная передача информации с пояснениями сложных моментов и категорий, тезисы излагаемого материала, иллюстрация модулей в интерактивной форме, которые включают в себя лекции-дискуссии, лекции-консультации и проблемные лекции;
– практические занятия;
– лабораторные занятия;
– самостоятельная работа студентов, включающая усвоение теоретического материала, поиск дополнительного материала и эффективных способов выполнения заданий, защита рефератов, докладов, выступлений; оформление, подготовка к текущему контролю знаний и к итоговому зачёту.

Удельный вес занятий, проводимых в интерактивных формах, в соответствии с требованиями ФГОС в целом в учебном процессе составляет не менее 50 % аудиторных занятий.

В учебном процессе помимо традиционных форм проведения занятий используются лекции – визуализации, лекции – диалоги. Лабораторные занятия проводятся в компьютерном классе с использованием Интернет среды. При проведение практических занятий используются деловые игры с разбором конкретных ситуаций.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

(Приводятся виды самостоятельной работы обучающегося, порядок их выполнения и контроля, дается учебно-методическое обеспечение (возможно в виде ссылок) самостоятельной работы по отдельным разделам дисциплины).

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине – зачёт.

Форма текущего контроля – выполнение лабораторных заданий.

В течение семестра студент выполняет задания. За выполнение задания студент получает определенное количество баллов. Однотипные задания собраны в разделы.

Форма промежуточного контроля – контрольная работа, коллоквиум.

Форма итогового контроля, определенная учебным планом – зачёт.

В самостоятельную работу по дисциплине «Защита информации в оптических системах» включена подготовка к текущему, промежуточному и итоговому контролю.

При подготовке к коллоквиуму, зачету каждый студент должен индивидуально готовиться по темам дисциплины, читая конспекты лекций и рекомендуемую учебную и справочную литературу, усваивая определения, схемы и принципы соответствующих расчетов. Самостоятельная работа позволяет студенту в спокойной обстановке подумать и разобраться с информацией по теме, структурировать знания. Чтобы содержательная информация по дисциплине запоминалась надолго, целесообразно изучать ее поэтапно, в предлагаемой последовательности, поскольку последующий материал связан с предыдущим. По каждой из тем для самостоятельного изучения, приведенных в рабочей программе дисциплины следует сначала прочитать рекомендованную литературу и при необходимости составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме и для освоения последующих разделов курса.

При выполнении индивидуальных заданий студент использует приобретенные на практических занятиях навыки расчетов, самостоятельно изучает примеры из лекций и соответствующего раздела дисциплины. Самостоятельная работа при выполнении индивидуальных заданий требует изучения и использования справочных материалов. Залогом успеха в приобретении знаний и навыков по дисциплине является синхронизация

выполняемых индивидуальных заданий по срокам с лекционным материалом и разбираемым на практических занятиях.
Виды самостоятельной работы студентов, обеспечивающие реализацию цели и решение задач данной рабочей программы:
• конспектирование первоисточников;
• подготовка к практическим занятиям;
• подготовка к лабораторным занятиям;
• подготовка и сдача зачета.
Изучение тем дисциплины, выносимых для самостоятельного изучения студентами:

	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 зачету 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.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.
В соответствии с учебным планом предусмотрен зачет в 6-м семестре. Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине.
Форма текущего контроля – выполнение лабораторных заданий. В течение семестра студент выполняет задания, за каждое из которых получает соответствующие баллы. За выполнение задания студент получает определенное количество баллов.
Форма промежуточного контроля – контрольные, коллоквиум.

Форма итогового контроля, определенная учебным планом – зачет.
В результате освоения дисциплины «Защита информации в оптических системах» по специальности 10.03.01 – Информационная безопасность обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ПК-5	Способность 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 защиты информации.	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 контроля показателей технической защиты информации.	-собеседование, дискуссия - отчеты к практическим занятиям - тесты - ситуационные задачи - электронный практикум
ПК-1	Способность проводить предпроектное обследование	Знать: основные подходы к описанию моделей сложных систем и	-собеседование, дискуссия - отчеты к практическим

	объекта проектирования, системный анализ предметной области, их взаимосвязей. Способность проектировать моделирование процессов с помощью интернет технологий.	соответствующие формальные модели (клеточные автоматы, графы событий, агрегированные системы, DEVS формализм и т.д.). Уметь: обосновывать выбор способа представления модели и программных средств её реализации. Владеть: практическими навыками по использованию средств вычислительной техники и программного обеспечения для организации обработки информации и решения задач.	занятиям - тесты - ситуационные задачи - электронный практикум

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

ПК-5

Схема оценки уровня формирования компетенции:

«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 защиты информации».

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетвори-тельно	Хорошо	Отлично
Порого-вый	Способностью организовывать и поддерживать выполнение комплекса мер по	Знает, но допускает ошибки при выполнение комплекса мер по информационной	Достаточно хорошо владеет способностью определять виды и формы	Свободно обладает способностью организовать технологический

	информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации.	безопасности, не может управлять процессом их реализации с учетом решаемых задач и защиты, внешних воздействий, вероятных угроз.	информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов.	процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

ПК-1
Схема оценки уровня формирования компетенции:
«Способностью проводить моделирование процессов и систем».

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетвори-тельно	Хорошо	Отлично
Порого-вый	Знать: этапы имитационного моделирования. Уметь: определять границы системы и цели моделирования	Знает, но допускает ошибки при определении концепций императивного программирования, основных синтаксических конструкций языка, методов программирования.	Достаточно хорошо знает и умеет писать и отлаживать программы на языке С++, осуществлять выбор и анализ необходимых алгоритмов.	Свободно владеет навыками описания алгоритмов, составления программ и методами анализа разработанных программных продуктов.

7.3. Типовые контрольные задания

(Указываются темы эссе, рефератов, курсовых работ и др. Приводятся примерные тестовые задания, контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины.)

1. На рисунке 1 представлена структурная схема:
• оптического канала утечки информации;
• акустического канала утечки информации;
• электронного канала утечки информации;
• акустооптического канала утечки информации.

Рисунок 1 - Структурная схема канала утечки информации.

2. На рисунке 2 представлена структурная схема:
• акустооптического канала утечки информации;
• акусто-радиоэлектронного канала утечки информации;
• радиоэлектронного канала утечки информации;
• акустоэлектронного канала утечки информации.

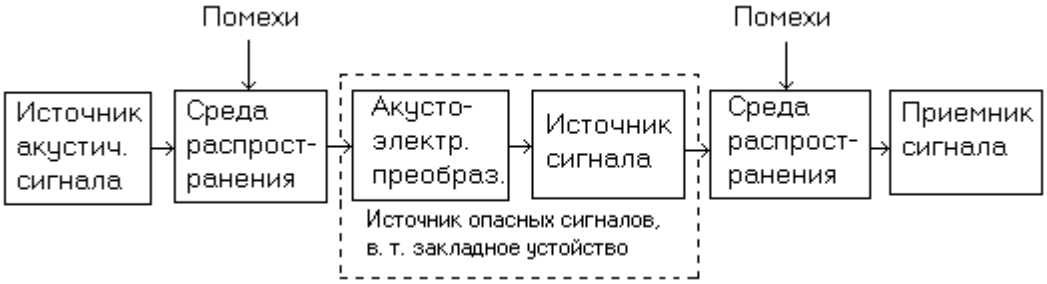

Рисунок 2 - Структурная схема канала утечки информации.

3. На рисунке 3 представлена структурная схема:
• акустооптического канала утечки информации;
• акусто-радиоэлектронного канала утечки информации;
• радиоэлектронного канала утечки информации;
• акустического канала утечки информации.

Рисунок 3 - Структурная схема 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:
• типовой структуры средства наблюдения;
• типовой структуры средства передачи;
• типовой структуры средства телевизионного наблюдения;
• типовой структуры средства ИК наблюдения.

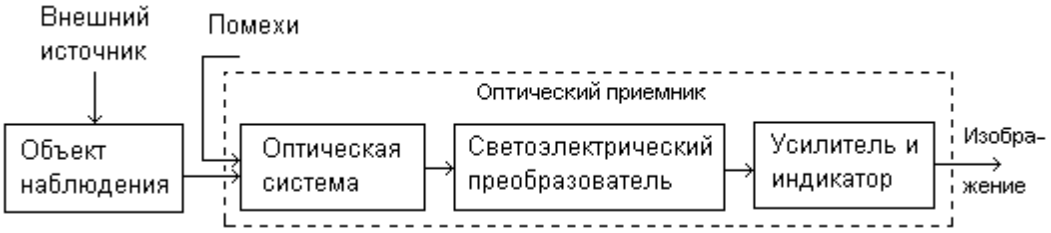

Рисунок 4 – Структурная схема канала.

7. На рисунке 5 представлена структурная схема:
• акусто-радиоэлектронного канала утечки информации;
• радиоэлектронного канала утечки информации;
• радиоэлектронного канала утечки информации;
• акустического канала утечки информации.

Рисунок 5 - Структурная схема канала утечки.

8. На рисунке 6 представлена структурная схема:
• оптического канала утечки информации;
• акустооптического канала утечки информации;
• акусто-радиоэлектронного канала утечки информации;
• радиоэлектронного канала утечки информации.

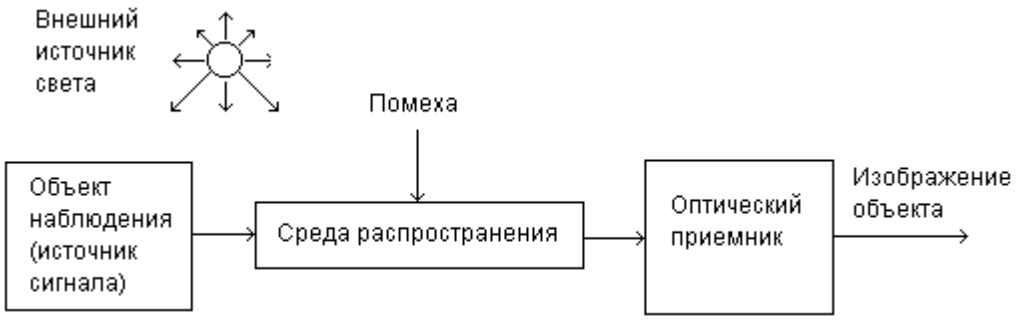

Рисунок 6 - Структурная схема канала утечки.

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;
• в электрическом канале утечки информации;
• в электромагнитном канале утечки информации;
• в параметрическом канале утечки информации.

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

Общий результат выводится как интегральная оценка, складывающая из текущего контроля - _50___% и промежуточного контроля - __50___%.
Текущий контроль по дисциплине включает:
- посещение занятий - _10__ баллов,
- участие на практических занятиях - __ баллов,
- выполнение лабораторных заданий - _30__баллов,
- выполнение домашних (аудиторных) контрольных работ - _10__ баллов.
Промежуточный контроль по дисциплине включает:
- устный опрос - _10__ баллов,
- письменная контрольная работа - __30__ баллов,

- тестирование - 10___ 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. Защита информации в оптических системах : 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 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
5. elibrary.ru [Электронный ресурс]: электронная библиотека / Научная электронная библиотека. – Москва, 1999. – Режим доступа: http://elibrary.ru/defaultx.asp (дата обращения: 01.04.2017). – Яз. рус., англ.
6. 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/(датаобращения: 22.03.2018).
7. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ / Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru, свободный (дата обращения: 21.03.2018).
8. techlibrary.ru [Электронный ресурс]: электронная библиотека / Техническая библиотека. Режим доступа: http://techlibrary.ru/, свободный (дата обращения: 25.11.2018).

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 зачет. На подготовку и сдачу зачета 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).

Лекционный курс. Лекция является основной формой обучения в высшем учебном заведении. В ходе лекционного курса проводится систематическое изложение современных научных материалов.

Студенту необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях. Конспекты лекций следует использовать при подготовке к зачету, контрольным тестам, коллоквиумам, при выполнении самостоятельных заданий.
Лабораторные занятия. Прохождение всего цикла лабораторных занятий является обязательным условием допуска студента к зачету. В случае пропуска занятий по уважительной причине пропущенное занятие подлежит отработке.
Специальное руководство, облегчающее работу студента по изучению темы, выдается для пользования на каждом занятии.
Изучив глубоко содержание учебной дисциплины, целесообразно разработать матрицу наиболее предпочтительных методов обучения и форм самостоятельной работы студентов, адекватных видам лекционных и лабораторных занятий.
Необходимо предусмотреть развитие форм самостоятельной работы, выводя студентов к завершению изучения учебной дисциплины на ее высший уровень.

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.

Рабочая программа по дисциплине «Защита информации в оптических системах» составлена в 2018 году в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 10.03.01 – Информационная безопасность (уровень бакалавриата), утверждённого приказом Минобрнауки РФ от 01.12.2016 № 1515.