МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
_____ И.М. Ажмухамедов

_____

«2» июня 2022 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой ИБ
_____ Р.Ю. Демина
протокол заседания кафедры № 2
от «2» июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации от утечки по техническим каналам

наименование

Составитель(-и)	**Марьенков А.Н., к.т.н., доцент, заведующий кафедрой ЦТ**
	Сахнов Н.В., ассистент кафедры ИБ
Направление подготовки	**10.03.01 Информационная безопасность**
Направленность (профиль) ОПОП	**«Организация и технология защиты информации»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2021**
Курс	**2**
Семестр	**4**

Астрахань, 2022 г.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебная дисциплина «Защита информации от утечки по техническим каналам» является важной составляющей общей профессиональной подготовки специалистов в области информационной безопасности. Она посвящена изучению основных каналов распространения информации и призвана обеспечить освоение слушателями практических навыков защиты информации в этих каналах от несанкционированного доступа.

1.1. Целью освоения дисциплины (модуля) «Защита информации от утечки по техническим каналам» является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях, изучение студентами технических средств защиты конфиденциальной информации, методов и технических средств съема информации, методов и средств контроля эффективности принимаемых мер защиты информации.

1.2. Задачи освоения дисциплины (модуля): – дать знания по:

–ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;

–ознакомление с техническими каналами утечки акустической (речевой) информации;

–изучение способов и средств защиты информации, обрабатываемой техническими средствами;

–изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;

–изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;

–обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

1.2. Бакалавр, изучив дисциплину «Техническая защита информации», должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

–эксплуатационная;

–установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

–проектно-технологическая;

–сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

–проведение проектных расчетов элементов систем обеспечения информационной безопасности;

–организационно-управленческая

–участие в совершенствовании системы управления информационной безопасностью.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) Б1.Б.18 «Защита информации от утечки по техническим каналам» входит в базовую часть Блока 1 подготовки бакалавров по направлению подготовки 10.03.01 Информационная безопасность, изучается в четвертом семестре второго курса, обучение длится один семестр. Форма итогового контроля: экзамен – 4 семестр.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

1. Физика;
2. Информатика.
3. Электротехника;
4. Безопасность жизнедеятельности;

В результате освоения этих дисциплин, студент должен:

знать:

- основные понятия информатики,
- основные понятия информационной безопасности;
- основные понятия электротехники;
- основные понятия охраны труда и техники безопасности;
- основные поражающие факторы электрического тока;
- основные принципы воздействия на организм человека различного рода излучений;
- основные понятия и определения в области информационной безопасности и защиты информации.

уметь:

- использовать программные и аппаратные средства персонального компьютера,
- использовать технические описания и схемы электронных приборов;
- классифицировать возможные угрозы информационной безопасности;
- пользоваться нормативными документами по защите информации.

владеть:

- навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.),
- навыками чтения электрических схем;
- навыками техники безопасности и охраны труда;

– методикой и техникой составления различных управленческих и документов учреждений, организаций и предприятий.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

1. Проектирование и эксплуатация защищенных информационных систем.
2. Комплексное обеспечение защиты информации объекта информатизации.
3. Защита и обработка конфиденциальной информации.
4. Безопасность сетей на базе Microsoft Windows Server.

Также дисциплина «Техническая защита информации» поможет студентам при реализации задач производственной практики и написанию бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) общепрофессиональных (ОПК): способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности (ОПК – 9); способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять

процессом их реализации на объекте защиты (ОПК – 10).

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ОПК-9 способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.1. Знать: принципы работы средств криптографической и технической защиты информации для решения стандартных задач профессиональной деятельности	ИОПК-9.2. Уметь: применять программные программно-аппаратные криптографические и технические средства защиты информации для решения задач профессиональной деятельности	ИОПК-9.3. Владеть: навыками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.1. Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности	ИОПК-10.2. Уметь: в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.3. Владеть: методами формирования и выполнения комплекса мер по информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины – 5 зачетных единиц (ЗЕ). На освоение дисциплины отводится 180 часов. Лекций – 18 часов, лабораторные занятия – 54 часов, самостоятельная работа – 72 часа, курсовая работа – 18 часов.

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	**Раздел 1. Объекты информационной безопасности**								
2	Тема 1.1. Основные свойства информации как предмета техниче-	4	1	1		3		4	Входное тестирование Отчет по лабо-

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
	ской защиты Тема 1.2. Демаскирующие признаки объектов защиты								раторной работе № 1
3	Тема 1.3. Источники и носители конфиденциальной информации Тема 1.4 Источники опасных сигналов	4	2	1		3		4	Отчет по лабораторной работе № 1 Контрольная работа № 1
4	**Раздел 2. Угрозы безопасности информации**								
5	Тема 2.1. Виды угроз безопасности информации Тема 2.2. Органы разведки	4	3	1		3		4	Контрольная работа № 2.
6	Тема 2.3. Технология разведки Тема 2.4. Способы несанкционированного доступа к источникам информации	4	4	1		3		4	Отчет по лабораторной работе № 2
7	Тема 2.5. Способы и средства добывания информации техническими средствами. Способы и средства наблюдения Тема 2.6. Способы и средства перехвата сигналов	4	5	1		3		4	Отчет по лабораторной работе № 2
8	Тема 2.7. Способы и средства подслушивания акустических сигналов	4	6	1		3		4	Отчет по лабораторной работе № 2
9	Тема 2.8. Способы и средства добывания информации о демаскирующих признаках веществ	4	7	1		3		4	Отчет по лабораторной работе № 2
10	Тема 2.9. Технические каналы утечки информации	4	8	1		3		4	Промежуточн. тестирование
11	**Раздел 3. Методы,**								

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
	способы и средства инженерно-технической защиты информации								
12	Тема 3.1. Концепция инженерно-технической защиты информации	4	9	1		3		4	Отчет по лабораторной работе № 3
13	Тема 3.2. Способы и средства инженерной защиты и технической охраны	4	10	1		3		4	Отчет по лабораторной работе № 3
14	Тема 3.3. Способы и средства защиты информации от наблюдения	4	11	1		3		4	Отчет по лабораторной работе 3
15	Тема 3.4. Способы и средства защиты информации от подслушивания	4	12	1		3		4	Отчет по лабораторной работе 3
16	Тема 3.5. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	4	13	1		3		4	Отчет по лабораторной работе № 4
17	Тема 3.6. Способы предотвращения утечки информации по материально-вещественному каналу	4	14	1		3		4	Отчет по лабораторной работе 4
18	**Раздел 4. Организация инженерно-технической защиты информации**								
19	Тема 4.1. Общие положения по инженерно-технической защите информации в организации	4	15	1		3		4	Отчет по лабораторной работе № 5
20	Тема 4.2. Организационные и технические меры по инженерно-	4	16	1		3		4	Отчет по лабораторной работе 5

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
	технической защите информации в организации								
21	**Раздел 5. Основы методического обеспечения инженерно-технической защиты информации**								
22	Тема 5.1. Системный подход к защите информации. Тема 5.2. Моделирование объекта защиты	4	17	1		3		4	Отчет по лабораторной работе № 6
23	Тема 5.3. Моделирование угроз информации Тема 5.4. Методические рекомендации по разработке мер защиты	4	18	1		3		4	Итоговое тестирование. Отчет по лабораторной работе № 6
	Итого			18		54	18	72	экзамен

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы; КР – курсовая работа; СР – самостоятельная работа по отдельным темам

Таблица 3. Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых в них компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Компетенции		Общее количество компетенций
		ОПК 9	*ОПК 10*	
Тема 1.1. Основные свойства информации как предмета технической защиты Тема 1.2. Демаскирующие признаки объектов защиты	*8*	+	+	*2*
Тема 1.3. Источники и носители конфиденциальной информации Тема 1.4 Источники опасных сигналов	*8*	+	+	*2*
Тема 2.1. Виды угроз безопасности информации Тема 2.2. Органы разведки	*8*	+	+	*2*

Тема 2.3. Технология разведки Тема 2.4. Способы несанкционированного доступа к источникам информации	*8*	+	+	*2*
Тема 2.5. Способы и средства добывания информации техническими средствами. Способы и средства наблюдения Тема 2.6. Способы и средства перехвата сигналов	*8*	+	+	*2*
Тема 2.7. Способы и средства подслушивания акустических сигналов	*8*	+	+	*2*
Тема 2.8. Способы и средства добывания информации о демаскирующих признаках веществ	*8*	+	+	*2*
Тема 2.9. Технические каналы утечки информации	*8*	+	+	*2*
Тема 3.1. Концепция инженерно-технической защиты информации	*8*	+	+	*2*
Тема 3.2. Способы и средства инженерной защиты и технической охраны	*8*	+	+	*2*
Тема 3.3. Способы и средства защиты информации от наблюдения	*8*	+	+	*2*
Тема 3.4. Способы и средства защиты информации от подслушивания	*8*	+	+	*2*
Тема 3.5. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	*8*	+	+	*2*
Тема 3.6. Способы предотвращения утечки информации по материально-вещественному каналу	*8*	+	+	*2*
Тема 4.1. Общие положения по инженерно-технической защите информации в организации	*8*	+	+	*2*
Тема 4.2. Организационные и технические меры по инженерно-технической защите информации в организации	*8*	+	+	*2*
Тема 5.1. Системный подход к защите информации. Тема 5.2. Моделирование объекта защиты	*8*	+	+	*2*
Тема 5.3. Моделирование угроз информации Тема 5.4. Методические рекомендации по разработке мер защиты	*8*	+	+	*2*
Курсовая работа	*18*	+	+	*2*
Итого	*180*			

Краткое содержание каждой темы дисциплины

Введение в техническую защиту информации

Предмет, цели, задачи и содержание курса технической защиты информации (ТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

Раздел 1. Объекты информационной безопасности

Тема 1.1. Основные свойства информации как предмета технической защиты

Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты. Понятие о демаскирующих признаках объектов защиты. Характеристики и особенности семантической (смысловой) информации и информации о демаскирующих признаках объекта.

Тема 1.2. Демаскирующие признаки объектов защиты

Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов. Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков. Понятие о признаковых структурах. Основные видовые демаскирующие признаки объектов наблюдения. Особенности видовых признаков в оптическом и радиодиапазонах.

Тема 1.3. Источники и носители конфиденциальной информации

Понятие об источниках, носителях и получателях информации. Классификация источников информации. Источники технической и экономической информации при научных исследованиях, разработке, производстве и эксплуатации продукции, на различных этапах и видах коммерческой деятельности. Виды носителей информации (люди, физические поля, электрические сигналы и материальные тела). Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ. Закон РФ «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 4673.

Тема 1.2. Источники опасных сигналов

1. Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства, и системы. Побочные электромагнитные излучения и наводки. Акустоэлектрические преобразователи, их виды и принципы работы. Принципы высокочастотного навязывания. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС). Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС. Паразитные наводки в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Самостоятельная работа

Статистический и семантический подходы к оценке количества информации. Показатели качества информации. Старение информации. Полезность и цена информации. Копирование информации.

Основные характеристики аналоговых и дискретных (импульсных) электрических сигналов, средств связи, радиолокационных станций, лазерных излучений и других. Ос-

новные признаки, характеризующие физические и химические свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах.

Способы записи информации на различные виды носителей. Виды модуляции (манипуляции) сигналов. Характеристики модулированных сигналов. Принципы съема информации путем демодуляции (детектирования). Искажения информации в результате воздействия на сигналы помех. Виды помех. Методы обеспечения безопасности информации в условиях воздействия помех.

Раздел 2. Угрозы безопасности информации

Тема 2.1. Виды угроз безопасности информации

Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации. Утечка информации и ее особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.

Тема 2.2. Органы разведки

Роль разведки в деятельности государств и коммерческих структур. Структура органов разведки. Виды зарубежной разведки и разведки коммерческих структур. Классификация технической разведки по физической природе носителя. Носители технических средств разведки. Принципы ведения разведки.

Тема 2.3. Технология разведки

Основные принципы и этапы добывания информации. Структура органов управления, добывания и информационной работы. Видовая и комплексная обработка данных и сведений.

Тема 2.4. Способы несанкционированного доступа к источникам информации

Понятие о разведывательном контакте и его условиях. Виды доступа к источникам информации (физический контакт и дистанционный доступ). Принципы доступа к источникам информации без физического проникновения к контролируемую зону. Классификация и характеристики наземных средств дистанционного съема информации с носителей. Принципы доступа к источникам информации без нарушения государственной границы. Возможности зарубежной космической, воздушной и морской разведки в мирное время.

Тема 2.5. Способы и средства добывания информации техническими средствами. Способы и средства наблюдения.

Факторы, влияющие на эффективность обнаружения и распознавания объектов наблюдения. Структура и основные характеристики средств наблюдения. Параметры зрительной системы человека. Классификация и основные характеристики объективов. Виды и технические характеристики визуально-оптических приборов.

Тема 2.6. Способы и средства перехвата сигналов

Задачи, решаемые при перехвате сигналов. Структура средств перехвата и их функции. Классификация и характеристики антенн. Структура радиоприемника и его характеристики. Особенности и основные характеристики сканирующих радиоприемников. Принципы определения координат источников радиоизлучений и анализа сигналов.

Тема 2.7. Способы и средства подслушивания акустических сигналов

Параметры слуховой системы человека. Структура и характеристики технических средств подслушивания. Классификация и характеристики микрофонов. Виды и принципы работы остронаправленных микрофонов. Стетоскопы. Принципы работы и характеристики диктофонов для скрытной записи. Классификация и характеристики закладных устройств. Варианты камуфлирования закладных устройств. Способы и средства лазерного подслушивания и ВЧ-навязывания.

Тема 2.8. Способы и средства добывания информации о демаскирующих признаках веществ

Способы и средства добывания информации о демаскирующих признаках веществ. Способы и возможности определения демаскирующих признаков веществ.

Тема 2.8. Технические каналы утечки информации

2.8.1. Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.

2.8.2. Оптические каналы утечки информации. Структура оптического канала утечки информации. Условия освещенности объектов наблюдения в видимом и ИК-диапазонах в различные периоды времени. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации. Варианты оптических каналов утечки информации для типовых контролируемых зон организации.

2.8.3. Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации.

2.8.4. Акустические каналы утечки информации. Структура акустического канала утечки информации. Отражение и поглощение акустических волн в среде распространения. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации.

2.8.5. Материально-вещественные каналы утечки информации. Структура материально-вещественного канала утечки информации и характеристики ее элементов.

Самостоятельная работа

Текущие и эталонные, первичные и вторичные признаковые структуры. Принципы идентификации и интерпретации, обнаружения и распознавания объектов, измерения характеристик демаскирующих признаков. Методы синтеза информации. Пути автоматизации процессов добывания и обработки информации.

Принципы конструкции и работы, виды и характеристики фото и киноаппаратов. Особенности цифровых фотоаппаратов. Технические эндоскопы. Структура средств телевизионного наблюдения. Принципы работы телевизионных камер на вакуумных трубках и приборах с зарядовой связью. Принципы видеозаписи. Характеристики телевизионных средств наблюдения и регистрации. Принципы работы и характеристики приборов ночного видения. Камуфлирование средств наблюдения. Принципы радиолокационного и радиотеплового наблюдения. Способы повышения разрешающей способности радиолокаторов.

Принципы дистанционного анализа веществ. Виды и показатели радиоактивных излучений. Структура и принципы работы средств радиационной разведки

Направляющие линии связи их характеристики. Классификация радиоволн. Особенности распространения радиоволн различных диапазонов частот. Способы повышения дальности передачи информации в ультракоротком диапазоне радиоволн. Ослабления радиоволн при распространении через различные среды. Классификация и характеристики помех в радиоэлектронных каналах утечки информации.

Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде. Особенности утечки информации о радиоактивных веществах. Принципы физического и химического анализа веществ.

Раздел 3. Методы, способы и средства инженерно-технической защиты информации

Тема 3.1. Концепция инженерно-технической защиты информации

2. Цели и задачи инженерно-технической защиты информации. Принципы инженерно-технической защиты информации. Уровни безопасности информации. Методы защиты информации. Сущность инженерной защиты и технической охраны источников информации. Понятие об информационном портрете объекта защиты. Способы изменения информационного портрета при маскировке и дезинформировании. Зависимость качества информации от отношения мощностей носителя информации и помехи. Сущность энергетического скрытия. Показатели эффективности инженерно-технической защиты информации. Указ Президента Российской Федерации от 24 января 1998 г. № 64 «О перечне сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г.) // СЗ РФ. 1995. № 49. ст. 4775; 1998, № 5, ст. 561. Указ Президента Российской Федерации от 12.05.2009 №537 «О стратегии национальной безопасности Российской Федерации до 2020 года».

Тема 3.2. Способы и средства инженерной защиты и технической охраны

3.2.1. Концепция охраны объектов. Категорирование объектов охраны. Демаскирующие признаки злоумышленника и стихийных сил (пожара, воды). Модели злоумышленников. Уровни физической безопасности объектов охраны. Типовая структура системы охраны. Системы автономной и централизованной охраны. Основные показатели системы охраны. Показатели эффективности инженерно-технической охраны объектов.

3.2.2. Способы и средства инженерной защиты объектов. Типовые инженерные конструкции. Естественные и искусственные преграды. Двери и ворота. Виды замков. Способы и средства защиты окон. Виды стекол, используемых для укрепления окон. Контрольно-пропускные пункты пропуска людей и автотранспорта. Способы и средства идентификации людей. Металлические шкафы, сейфы и хранилища. Показатели стойкости сейфов и хранилищ.

3.2.3. Способы и средства обнаружения злоумышленников и пожара. Структура комплекса технических средств охраны. Классификация извещателей. Принципы работы и основные характеристики контактных извещателей. Акустические извещатели. Оптико-электронные извещатели. Микроволновые (радиоволновые) извещатели. Вибрационные извещатели. Емкостные извещатели. Тепловые и ионизационные извещатели. Комбинированные извещатели. Помехи работе извещателей. Рекомендации по установке извещателей. Приемно-контрольные приборы, их назначение, классификация и основные характеристики. Пульты централизованного наблюдения.

3.2.4. Способы и средства видеоконтроля. Структура системы видеоконтроля.

3.2.5. Способы и средства нейтрализации угроз. Виды способов и средств нейтрализации угроз. Подразделение охраны. Средства тревожной сигнализации.

3.2.6. Средства управления системой охраны. Способы и средства передачи извещений. Автоматизированные интегральные системы охраны объектов, их структура и тенденция развития.

Тема 3.3. Способы и средства защиты информации от наблюдения

3.3.1. Способы и средства противодействия наблюдению в оптическом диапазоне волн. Виды маскировки и их сущность. Особенности маскировки в видимом и ИК-диапазонах света. Виды и принципы применения искусственных масок, аэрозолей и воздушной пены.

3.3.2. Способы и средства противодействия радиолокационному и гидроакустическому наблюдению. Способы информационного скрытия объектов от радиолокационного наблюдения. Средства дезинформирования и пассивного зашумления изображения на экране радиолокатора. Способы уменьшения эффективной площади рассеяния объекта наблюдения. Виды радиопоглощающих покрытий. Способы активного подавления сигналов радиолокаторов.

Тема 3.4. Способы и средства защиты информации от подслушивания

3.4.1. Способы и средства информационного скрытия акустических сигналов и речевой информации. Способы и средства информационного скрытия информации от подслушивания. Виды информационного скрытия речевой информации. Классификация способов технического закрытия. Сущность способов технического закрытия, их сравнительный анализ. Типы и параметры скремблеров.

3.4.2. Способы и средства энергетического скрытия акустических сигналов. Методы энергетического скрытия акустических сигналов: звукоизоляция и звукопоглощение. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей. Способы повышения звукоизоляции окон и дверей. Основные звукопоглощающие материалы и способы их применения. Типы и способы применения генераторов акустического и вибрационного зашумления. Способы оценки энергетических и информационных показателей безопасности речевой информации.

3.4.3. Способы и средства предотвращения утечки информации с помощью закладных устройств. Основные демаскирующие признаки проводных и радиозакладных устройств, качественная оценка их информативности. Классификация средств обнаружения, локализации и подавления закладных устройств. Принципы работы и основные характеристики обнаружителей электромагнитного поля, их достоинства и недостатки, способы применения. Возможности бытовых приемников и селективных вольтметров. Особенности специальных радиоприемников. Типы и параметры сканирующих приемников. Состав, принципы работы, возможности и параметры автоматизированных комплексов радиоконтроля помещений. Способы контроля телефонных линий и цепей электропитания. Способы подавления сигналов закладных устройств. Типы генераторов радиопомех.

Тема 3.5. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки

Требования к средствам подавления сигналов побочных электромагнитных излучений и наводок. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных и электромагнитных полей. Экранирование проводов и кабелей. Материалы для экранирования. Требования к заземлению и конструкция заземлителей. Развязка и фильтрация цепей электропитания. Средства активного линейного и пространственного зашумления..

Тема 3.6. Способы предотвращения утечки информации по материально-вещественному каналу

Классификация способов предотвращения утечки информации по материально-вещественному каналу. Способы и средства уничтожения информации, содержащейся в отходах дело и промышленного производства. Способы и средства стирания информации магнитных носителях. Способы защиты демаскирующих веществ.

Самостоятельная работа

Телевизионные камеры, их классификация, принципы работы и основные характеристики. Мониторы, коммутаторы, квадраторы, мультиплексоры, видеомагнитофоны. Детекторы движения. Способы повышения времени видеозаписи. Дежурное освещение. Виды и основные характеристики источников света.

Средства пожаротушения, тенденция развития средств пожаротушения. Резервное и аварийное электропитание. Основные характеристики источников резервного электропитания (батарей, аккумуляторов).

Средства подавления сигналов закладных устройств в телефонных линиях и цепях электропитания. Принципы работы нелинейных локаторов. Типы и характеристики отечественных и зарубежных локаторов. Физические принципы работы и способы применения обнаружителей пустот для выявления закладных устройств. Принципы работы и характеристики металлодетекторов. Виды рентгеновских установок. Типы, возможности и спосо-

бы применения для выявления закладных устройств флюороскопов и рентгенотелевизионных установок. Виды “чисток” помещения. Способы и средства визуального осмотра помещения. Способы и средства контроля помещения перед и в ходе проведения совещаний. Виды проверки отдельных предметов. Варианты наборов средств для “чистки” помещений. Две основные линии развития ОС: открытые и закрытые - Windows и Unix.

Раздел 4. Организация инженерно-технической защиты информации

Тема 4.1. Общие положения по инженерно-технической защите информации в организации

Краткая характеристика государственной системы защиты информации. Основные руководящие и нормативные документы по организации инженерно-технической защиты информации в организации, их сущность.

Тема 4.2. Организационные и технические меры по инженерно-технической защите информации в организации

Основные направления инженерно-технической защиты информации в организации. Сущность организационных и технических мер по защите информации в организации. Задачи и виды контроля эффективности защиты информации.

Самостоятельная работа

Функции сотрудников службы безопасности, обеспечивающие инженерно-техническую защиту информации.

Сущность технического контроля эффективности защиты информации.

Раздел 5. Основы методического обеспечения инженерно-технической защиты информации

Тема 5.1. Системный подход к защите информации

Сущность системного подхода и системного анализа. Характеристики системы защиты информации. Сущность характеристик системы защиты информации. Частный и глобальный критерии эффективности системы защиты. Алгоритм проектирования системы.

Тема 5.2. Моделирование объекта защиты

Сущность и методические рекомендации по структурированию защищаемой информации. Выявление и описание источников информации. Формы представления моделей объектов информационной безопасности.

Тема 5.3. Моделирование угроз информации

Виды моделей угроз информации: путей физического проникновения злоумышленника к источнику и каналов утечки. Методические рекомендации по определению путей проникновения злоумышленника к источнику информации, формы моделей. Типовые индикаторы каналов утечки. Методические рекомендации по моделированию каналов утечки. Формы представления результатов моделирования. Рекомендации по оценке угроз безопасности информации.

Тема 5.4. Методические рекомендации по разработке мер защиты

Основные способы и средства защиты информации от типовых вариантов угроз. Рекомендации по оценке затрат на защиту и форме их представления. Комплексирование мер защиты. Оптимизация проекта системы (предложений) защиты информации. Требо-

вания к оформлению проекта системы (предложений) при представлении на согласование и утверждений. Тенденции развития методического обеспечения защиты информации.

Самостоятельная работа

Основные этапы и алгоритм проектирования системы или разработки предложений по ее модернизации. Понятие о моделировании как основном процессе системного анализа. Виды моделей и их возможности при исследовании проблем защиты информации.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным (семинарским) занятиям необходимо воспользоваться учебно-методической литературой из п.8. Лекции (семинары) необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8, а также пользоваться ресурсами сети Интернет .

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

Экзамен

Экзамен заключается в письменном ответе на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;

- отсутствие ответов на заданные при собеседовании вопросы.

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

На учебном файловом сервере АГУ (fsever) размещены задания для лабораторной и самостоятельной работы студентов, тесты, а также лекционный материал.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	*Вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Раздел 1.	**Объекты информационной безопасности**		
Тема 1.1.	Основные свойства информации как предмета технической защиты Тема 1.2. Демаскирующие признаки объектов защиты	6	Входное тестирование Отчет по лабораторной работе № 1
Тема 1.3. Тема 1.4	Источники и носители конфиденциальной информации. Источники опасных сигналов	6	Отчет по лабораторной работе № 1 Контрольная работа № 1
Раздел 2.	**Угрозы безопасности информации**		
Тема 2.1. Тема 2.2.	Виды угроз безопасности информации. Органы разведки	6	Контрольная работа № 2.
Тема 2.3. Тема 2.4.	Технология разведки. Способы несанкционированного доступа к источникам информации	6	Отчет по лабораторной работе № 2
Тема 2.5. Тема 2.6.	Способы и средства добывания информации техническими средствами. Способы и средства наблюдения. Способы и средства перехвата сигналов	6	Отчет по лабораторной работе № 2
Тема 2.7.	Способы и средства подслушивания акустических сигналов	6	Отчет по лабораторной работе № 2
Тема 2.8.	Способы и средства добывания информации о демаскирующих признаках веществ	6	Отчет по лабораторной работе № 2
Тема 2.9.	Технические каналы утечки информации	6	Промежуточн. тестирование
Раздел 3.	**Методы, способы и средства инженерно-технической защиты информации**		
Тема 3.1.	Концепция инженерно-технической защиты информации	6	Отчет по лабораторной работе № 3
Тема 3.2.	Способы и средства инженерной защиты и технической охраны	6	Отчет по лабораторной работе № 3

Тема 3.3.	Способы и средства защиты информации от наблюдения	6	Отчет по лабораторной работе 3
Тема 3.4.	Способы и средства защиты информации от подслушивания	6	Отчет по лабораторной работе 3
Тема 3.5.	Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	6	Отчет по лабораторной работе № 4
Тема 3.6.	Способы предотвращения утечки информации по материально-вещественному каналу	6	Отчет по лабораторной работе 4
Раздел 4.	**Организация инженерно-технической защиты информации**		
Тема 4.1.	Общие положения по инженерно-технической защите информации в организации	6	Отчет по лабораторной работе № 5
Тема 4.2.	Организационные и технические меры по инженерно-технической защите информации в организации	6	Отчет по лабораторной работе 5
Раздел 5.	**Основы методического обеспечения инженерно-технической защиты информации**		
Тема 5.1. Тема 5.2.	Системный подход к защите информации. Моделирование объекта защиты	6	Отчет по лабораторной работе № 6
Тема 5.3. Тема 5.4.	Моделирование угроз информации. Методические рекомендации по разработке мер защиты	6	Итоговое тестирование. Отчет по лабораторной работе № 6

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно.

Собеседование

Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Основаниями для снижения оценки при собеседовании являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

Требования к оформлению презентации для защиты курсового проекта

Выбрать одну из предложенных тем и подготовить презентацию.

Презентация включает в себя 15-20 слайдов (1 слайд — титульный (название темы, кто выполнил: №гр, ФИО), последний слайд — список литературы, ссылки на электронные ресурсы (не менее трех источников)).

Слайды должны быть пронумерованы (титульный слайд не нумеруется). Презентация должна включать в себя не только текст, но и картинки, схемы, таблицы с индивидуальным форматированием, диаграммы с данными и т.д, и соответствовать всем требованиям, предъявляемым к её оформлению.

Требования к оформлению презентации

В оформлении презентаций выделяют два блока правил, описывающих:

1) Представление информации
2) Оформление слайдов

Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к организации и оформлению данных блоков.

Презентация предполагает сочетание информации различных типов: текста, графических изображений, анимации и видеофрагментов. Поэтому необходимо учитывать специфику комбинирования фрагментов информации различных типов. Кроме того, оформление и демонстрация каждого из перечисленных типов информации также подчиняется определенным правилам. Так, например, для текстовой информации важен выбор шрифта, для графической — яркость и насыщенность цвета, для наилучшего их совместного восприятия необходимо оптимальное взаиморасположение на слайде.

Представление информации

Объем и форма представления информации:

- Рекомендуется сжатый, информационный способ изложения материала.
- Не стоит заполнять один слайд слишком большим объемом информации: человек в среднем может единовременно запомнить не более трех фактов, выводов, определений.
- Один слайд презентации в среднем рассчитывается на 0,5-1 минуту выступления.
- Для достижения наибольшей эффективности ключевые пункты отображаются по одному на каждом отдельном слайде.
- Желательно присутствие на слайде блоков с разнотипной информацией (текст, графики, диаграммы, таблицы, рисунки), дополняющей друг друга.
- Заголовки должны быть краткими и привлекать внимание аудитории.
- В текстовых блоках необходимо использовать короткие слова и предложения.
- Рекомендуется минимизировать количество предлогов, наречий, прилагательных.
- В таблицах рекомендуется использовать минимум строк и столбцов.
- Вся вербальная информация должна тщательно проверяться на отсутствие орфографических, грамматических и стилистических ошибок.
- При проектировании характера и последовательности предъявления материала должен соблюдаться принцип стадийности: информация может разделяться в пространстве (одновременное отображение в разных зонах одного слайда) или во времени (размещение информации на последовательно демонстрируемых слайдах).

Расположение информационных блоков на слайде

- Структура слайда должна быть одинаковой на всей презентации.
- Логика предъявления информации на слайдах и в презентации должна соответствовать логике ее изложения.
- Наиболее важная информация должна располагаться в центре экрана.
- Информационных блоков на слайде не должно быть слишком много (оптимально 3, максимум 5).
- Рекомендуется объединение семантически связанных информационных элементов в целостно воспринимающиеся группы;
- Рекомендуемый размер одного информационного блока — не более 1/2 размера слайда;

• Информационные блоки рекомендуется располагать горизонтально, связанные по смыслу блоки — слева направо.

• Поясняющая надпись должна располагаться под рисунком (фотографией, диаграммой, схемой).

Способы и правила выделения информации

Все информационные элементы (текст, изображения, диаграммы, элементы схем, таблицы) должны ясно и рельефно выделяться на фоне слайда, для этого используются:

• рамки, прорисовка границ (для оформления изображений, таблиц);
• тени (для отделения контура текста и объектов от фона);
• заливка, штриховка (для дизайна основ информационных блоков);
• стрелки (для оформления схем и логических блоков).

Ключевые слова в информационном блоке необходимо выделить (цветом, подчеркиванием, полужирным и курсивным начертанием, размером шрифта). Для иллюстрации наиболее важных фактов используются рисунки, диаграммы, схемы.

Единый стиль презентации

Вся презентация должна должны быть выдержана в едином стиле, на базе одного шаблона. Стиль включает в себя:

• общую схему шаблона: способ размещения информационных блоков;
• общую цветовую схему дизайна слайда;
• цвет фона или фоновый рисунок, декоративный элемент небольшого размера и др.;
• параметры шрифтов (гарнитура, цвет, размер) и их оформления (эффекты), используемых для различных типов текстовой информации (заголовки, основной текст, выделенный текст, гиперссылки, списки, подписи);
• способы оформления иллюстраций, схем, диаграмм, таблиц и др.

Необходимо обеспечить унификацию структуры и формы представления материала. Цветовая схема должна быть одинаковой на всех слайдах. Это создает у слушателей ощущение связности, преемственности, стильности, комфортности.

В стилевом оформлении презентации не рекомендуется использовать более 3 основных цветов и более 3 типов шрифта. Следует избегать излишне пёстрых стилей — оформление слайда не должно отвлекать внимание слушателей от содержательной части доносимой информации. При выборе элементов стиля (цветовых соотношений, размера текста, иллюстраций, таблиц) рекомендуется проводить проверку шаблона презентации на удобство чтения с экрана компьютера.

Правила использования цвета

Одним из основных компонентов дизайна презентации является учет физиологических особенностей восприятия цветов человеком. К наиболее значимым из них относят:

• стимулирующие (теплые) цвета способствуют возбуждению и действуют как раздражители (в порядке убывания интенсивности воздействия): красный, оранжевый, желтый;
• дезинтегрирующие (холодные) цвета успокаивают, вызывают сонное состояние (в том же порядке): фиолетовый, синий, голубой, сине-зеленый; зеленый;
• нейтральные цвета: светло-розовый, серо-голубой, желто-зеленый, коричневый;
• сочетание двух цветов — цвета знака и цвета фона — существенно влияет на зрительный комфорт, причем некоторые пары цветов не только утомляют зрение, но и могут привести к стрессу (например, зеленые буквы на красном фоне);
• наиболее хорошо воспринимаемые сочетания цветов шрифта и фона: белый на темно-синем, лимонно-желтый на пурпурном, черный на белом, желтый на синем.

Можно сформулировать следующие рекомендации по использованию цвета в презентации:

На одном слайде рекомендуется использовать не более трех базовых цветов: один для фона, один для заголовка, один для текста.

Составление цветовой схемы презентации начинается с выбора:

- трех базовых цветов: фона — текста — заголовка;
- трех главных функциональных цветов, которые используются для представления обычного текста, гиперссылок и посещенных ссылок.

Для фона и текста необходимо использовать контрастные цвета: текст должен хорошо читаться, но не резать глаза. Следует обратить внимание на цвет гиперссылок (до и после использования): их цвет должен заметно отличаться от цвета текста, но не контрастировать с ним.

Правила использования фона

- Фон является элементом заднего (второго) плана, должен выделять, оттенять, подчеркивать информацию, находящуюся на слайде, но не заслонять ее.
- Легкие пастельные тона лучше подходят для фона, чем белый цвет.
- Для фона предпочтительны холодные тона.
- Вместо того, чтобы использовать сплошной цвет лучше выбрать плавный градиентный переход гармонично сочетающихся цветов, мягкую (неконтрастную) текстуру или нейтральный фон.
- Любой активный фоновый рисунок повышает утомляемость глаз обучаемого и снижает эффективность восприятия материала.
- При планировании дизайна слайда следует всячески избегать проецирования текстовых блоков на области фона, содержащие изображения и декоративные элементы.

Правила использования текстовой информации

Не рекомендуется:

- перегружать слайд текстовой информацией;
- использовать блоки сплошного текста;
- в нумерованных и маркированных списках использовать уровень вложения глубже двух;
- использовать переносы слов;
- использовать наклонное и вертикальное расположение подписей и текстовых блоков;
- текст слайда не должен повторять текст, который преподаватель произносит вслух (зрители прочитают его быстрее, чем расскажет преподаватель, и потеряют интерес к его словам).

Рекомендуется:

- сжатость и краткость изложения, максимальная информативность текста: короткие тезисы, даты, имена, термины — главные моменты опорного конспекта;
- использование коротких слов и предложений, минимум предлогов, наречий, прилагательных;
- использование нумерованных и маркированных списков вместо сплошного текста;
- использование табличного (матричного) формата предъявления материала, который позволяет представить материал в компактной форме и наглядно показать связи между различными понятиями;
- выполнение общих правил оформления текста;
- тщательное выравнивание текста, буквиц, маркеров списков;
- горизонтальное расположение текстовой информации, в т.ч. и в таблицах;
- каждому положению, идее должен быть отведен отдельный абзац текста;
- основную идею абзаца располагать в самом начале — в первой строке абзаца (это связано с тем, что лучше всего запоминаются первая и последняя мысли абзаца);
- идеально, если на слайде только заголовок, изображение (фотография, рисунок, диаграмма, схема, таблица и т.п.) и подпись к ней.

Правила использования шрифтов

При выборе шрифтов для представления вербальной информации презентации следует учитывать следующие правила:

• Не рекомендуется смешивать разные типы шрифтов в одной презентации.

• Учитывая, что гладкие (плакатные) шрифты, т.е. шрифты без засечек (типа Arial, Tahoma, Verdana и т.п.) легче читать с большого расстояния, чем шрифты с засечками (типа Times), то:

• для основного текста предпочтительно использовать плакатные шрифты;

• для заголовка можно использовать декоративный шрифт, если он хорошо читаем и не контрастирует с основным шрифтом.

• Текст должен быть читабельным (его должно быть легко прочитать с самого дальнего места).

• Рекомендуемые размеры шрифтов:

• для заголовков — не менее 32 пунктов и не более 50, оптимально — 36 пункта;

• для основного текста — не менее 18 пунктов и не более 32, оптимально — 24 пункта;

• Не следует злоупотреблять прописными буквами (они читаются хуже строчных), поэтому их допустимо использовать только для смыслового выделения небольших фрагментов текста.

• Наиболее важный материал, требующий обязательного усвоения, желательно выделить ярче для включения ассоциативной зрительной памяти.

• Для выделения информации следует использовать цвет, жирный и/или курсивный шрифт.

• Выделение подчеркиванием обычно ассоциируется с гиперссылкой, поэтому использовать его для иных целей не рекомендуется.

Правила использования графической информации

Динамика взаимоотношений визуальных и вербальных элементов и их количество определяются функциональной направленностью учебного материала. Изображение информативнее, нагляднее, оно легче запоминается, чем текст. Поэтому, если можно заменить текст информативной иллюстрацией, то лучше это сделать.

При использовании графики в презентации следует выполнять следующие правила и рекомендации, обусловленные законами восприятия человеком зрительной информации:

• Графика (рисунки, фотографии, диаграммы, схемы) должна органично дополнять текстовую информацию или передавать ее в более наглядном виде.

• Каждое изображение должно нести смысл: желательно избегать в презентации рисунков, не несущих смысловой нагрузки, если они не являются частью стилевого оформления.

• Цвет графических изображений не должен резко контрастировать с общим стилевым оформлением слайда.

• Необходимо использовать изображения только хорошего качества. Для этого все изображения, помещаемые в презентацию, должны быть предварительно подготовлены в графическом редакторе.

Недопустимо:

• искажение пропорций;

• нарушение тонового и цветового баланса фотоизображений;

• использование изображений с пониженной резкостью;

• видимость пикселей на изображении;

• использование необработанных сканированных изображений; например — изображений с "грязным"(серым, желтым) фоном вместо белого, неконтрастных, размытых и т.п.

• При подготовке в графическом редакторе изображения для помещения его на слайд презентации важное значение имеет выбор для него оптимального размера и разрешения:

• Выбор размера изображения (в пикселах) осуществляется в графическом редакторе. Изображение уменьшается (ни в коем случае НЕ увеличивается!) до нужного размера относительно экрана (либо до немного большего, чем нужный, но не более чем в 1.5—2 раза, чтобы более точно отрегулировать его размер уже на слайде путем уменьшения масштаба от 100%).

• При масштабировании помещенного на слайд изображения его масштаб допустимо только уменьшать (от исходных 100%), и крайне нежелательно увеличивать масштаб свыше 100%, так как при этом теряется его качество — на слайде оно будет выглядеть размытым. Если на слайде в масштабе 100% изображение оказалось слишком маленьким, то его необходимо заново подготовить в графическом редакторе из исходного оригинала большого размера.

• Если презентацию предполагается демонстрировать на экране с большим разрешением, чем на том компьютере, на котором она создается (или если презентация предназначена еще и для распечатки), то при данном рабочем разрешении рекомендуется использовать соответственно большие размеры всех изображений, которые после помещения на слайд соответственно масштабируются (уменьшаются).

• Вместе с тем, не рекомендуется перегружать презентацию неоправданно большими размерами файлов изображений. Использование большого числа "тяжелых" файлов перегружает презентацию, что может привести к замедлению ее работы.

• Иллюстрации рекомендуется сопровождать пояснительным текстом, пояснительная надпись преимущественно располагается под рисунком.

• Изображения лучше помещать левее текста: поскольку мы читаем слева-на-право, то взгляд зрителя вначале обращается на левую сторону слайда.

• Сложный рисунок или схему следует выводить постепенно.

• Необходимо четко указать все связи в схемах и диаграммах.

Анимационные эффекты

Возможности анимации позволяют акцентировать внимание учащихся на наиболее важных моментах урока, позволяют понять логику построения логических цепочек, схем, таблиц.

Рекомендуется использовать возможности компьютерной анимации для представления информации на слайде. Однако не стоит чрезмерно насыщать презентацию такими эффектами, иначе это вызовет негативную реакцию аудитории.

• Анимация должна быть сдержанна, хорошо продумана и допустима:

• для демонстрации динамичных процессов;

• для привлечения внимания слушателей и создания определенной атмосферы презентации.

• Не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде.

• Анимация не должна быть слишком активной. Особенно нежелательные такие эффекты, как вылет, вращение, волна, побуквенное появление текста и т.д. В учебных презентациях для детей и подростков такие эффекты, как движущиеся строки по горизонтали и вертикали, запрещены нормативными документами.

• Большое влияние на подсознание человека оказывает мультипликация. Ее воздействие гораздо сильнее, чем действие обычного видео. Четкие, яркие, быстро сменяющиеся картинки легко "впечатываются" в подсознание. Причем, чем короче воздействие, тем оно сильнее.

Правила оформления текста пояснительной записки курсового проекта

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, темы курсового проекта, Ф.И.О. студента, номер группы, Ф.И.О.

преподавателя и оставляется место для проставления оценки и подписи преподавателя . Внизу пишется город и год написания.

Текстовая часть

Изложение текста и оформление работы следует выполнять в соответствии с требованиями.

Текст ПЗ оформляется на одной стороне листа формата А4.

Основной текст набирается шрифтом *Times New Roman 12,* с выравниванием *по ширине*, абзацный отступ должен быть одинаковым по всему тексту и равен *1,25 см*; строки разделяются *полуторным интервалом*.

Поля страницы: верхнее -2,5см, нижнее – 2,5 см, левое – 3,5 см, правое – 1,0 см.

Структурные элементы пояснительной записки **СОДЕРЖАНИЕ, ВВЕДЕНИЕ, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ, ПРИЛОЖЕНИЕ** должны начинаться с нового листа.

Их заголовки оформляются ***прописными буквами, шрифтом 14 Ж***, располагаются *в середине строки без точки в конце*. Дополнительный *интервал после* заголовка - 12 *пт*.

Основную часть работы разделяют на разделы, подразделы и, при необходимости, на пункты.

Каждый раздел необходимо начинать с нового листа. Разделы нумеруют арабскими цифрами в пределах всего текста. После номера и в конце заголовка раздела *точка не ставится*.

Если заголовок состоит из двух предложений, их разделяют точкой. *Переносы слов в заголовках не допускаются.*

Заголовки разделов оформляются ***с прописной буквы, шрифтом 14 Ж,*** с абзацного отступа *1,25* см. Дополнительный *интервал после заголовка - 6 пт.*

(Если заголовок раздела занимает две и большее число строк, то интервал между этими строками – *полуторным*).

Подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из номера раздела и порядкового номера подраздела, разделенных точкой. После номера подраздела точку не ставят.

Заголовки подразделов печатаются с абзацного отступа, ***с прописной буквы шрифтом 12 Ж,*** без точки в конце заголовка.

Дополнительный *интервал перед* заголовком подраздела – *6 пт, после* заголовка - 6 *пт*.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номеров раздела, подраздела и пункта, разделенных точкой. После номера пункта точку не ставят.

Нельзя писать заголовок в конце страницы, если на ней не умещаются, по крайней мере, две строки текста, идущего за заголовком.

Пример оформления заголовков текста:

1 Разработка аппаратных средств

1.1
1.2
1.3

Нумерация пунктов первого раздела отчета

2 Технические характеристики

2.1
2.2
2.3

Нумерация пунктов второго раздела отчета

В пояснительной записке после титульного листа помещается лист **СОДЕРЖАНИЕ**, в котором указываются номера и наименования разделов, подразделов и приложений ТД с указанием номеров страниц, где они начинаются.

Разделы, подразделы записываются в содержании в точном соответствии с их наименованиями без сокращений *строчными буквами кроме первой прописной.*

Перечисления

В тексте пояснительной записки перечисления производятся с абзацного отступа, каждое с новой строки с *дефисом***.**

Примеры написания:

- текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
- приложения;
- перечень терминов;
- перечень сокращений;
- перечень литературы.

При необходимости ссылки в тексте отчета на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

При необходимости дальнейшей детализации перечислений используются арабские цифры и строчные буквы русского алфавита, после которых ставятся скобки:

а)…;

б)…;

1)…;

2)…;

в).

Примеры написания:

1) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
2) приложения;
3) перечень терминов;
4) перечень сокращений;
5) перечень литературы.

Примеры написания:

а) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);

б) приложения;

в) перечень терминов;

г) перечень сокращений;
д) перечень литературы.

Сокращения слов

Сокращение слов в тексте, как правило, не допускается. Исключение составляют сокращения, общепринятые в русском языке: т. е. (то есть), и т. п. (и тому подобное), и т. д. (и так далее), и др. (и другие).

При необходимости применения специфических терминов или сокращений нужно дать их разъяснение при первом упоминании. Например «…создание систем автоматического проектирования (САПР)». В последующем тексте принятые сокращения пишутся без скобок.

Формулы

Составной частью текста пояснительной записки являются математические формулы и соотношения. Формулы создаются в редакторе формул.

Формулы располагают в середине строки и выделяют из текста свободными строками.

Пример оформления расчетов:

Количество населения в заданном пункте и подчиненных окрестностях с учетом среднего прироста населения определяется по формуле (3.1):

$$H_t = H_0\left(1 + \frac{\Delta H}{100}\right)^t, \qquad (3.1)$$

где H_0 – число жителей на время проведения переписи населения, тыс. чел.;

ΔH – средний годовой прирост населения в данной местности, % (принимается 2…3%);

t – период, определяемый как разность между назначенным годом перспективного проектирования и годом проведения переписи населения, год.

$$H_t = 32{,}6\left(1 + \frac{2}{100}\right)^8 = 38{,}2 \text{ тыс.чел.}$$

Расшифровка формулы, при необходимости, приводится непосредственно под формулой. В конце формулы ставится запятая, пояснение значений символов дают с новой строки в той последовательности, в какой они приведены в формуле.

Формулы нумеруются в пределах раздела. Номер формулы состоит из номера раздела и порядкового номера формулы в этом разделе. Номер формулы в круглых скобках помещается в крайнем правом положении на строке.

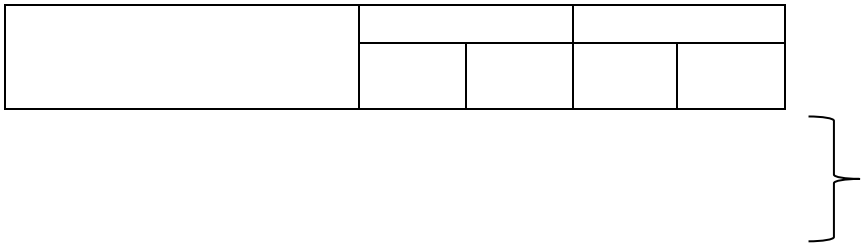
Ссылка в тексте на формулу: «…в формуле (3.1)».

Таблицы

Цифровой материал оформляется в виде таблиц. Таблицу следует располагать непосредственно после ссылки на нее.

Размеры таблиц выбираются произвольно, в зависимости от представляемого материала. Высота строк таблицы должна быть не менее 8 мм

Таблица 2.1 – Наименование таблицы



Заголовки граф

Подзаголовки граф

Строки (горизонтальные ряды)

Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Если подзаголовки граф имеют самостоятельное значение, то их начинают с прописной буквы.

Заголовки указывают в единственном числе. В конце заголовков и подзаголовков таблицы точки не ставят.

Разделять заголовки боковика и граф диагональными линиями не допускается.
Графу «Номер по порядку» в таблицу включать не допускается.

Таблицы нумеруются в пределах раздела. Номер таблицы состоит из номера раздела и порядкового номера таблицы в этом разделе. Номер и наименование таблицы следует помещать над таблицей слева через тире.

Пример оформления таблицы:

Таблица 3.1– Длина участков трассы

Протяженность участка проектируемой трассы, км	Тип кабеля
0,084	ДПС-04-24А06-7,0
0,167	ДПС-04-24А06-7,0
0,301	ДПС-04-24А06-7,0
0,779	ДПС-04-24А06-7,0
Общая длина кабеля: 1,331 км	ДПС-04-24А06-7,0

Таблицу с большим числом строк допускается переносить на другой лист. При этом в первой части таблицы нижнюю горизонтальную линию не проводят. Над второй частью слева пишут: «Продолжение Таблицы 2.1».

Продолжение Таблицы 2.1

Дата	Наименование	Стоимость

Рисунки

Графический материал располагают, возможно, ближе к тексту, в котором о нём упоминается.

Все рисунки нумеруются в пределах раздела и должны иметь наименование, Номер рисунка и его наименование располагают под рисунком следующим образом:

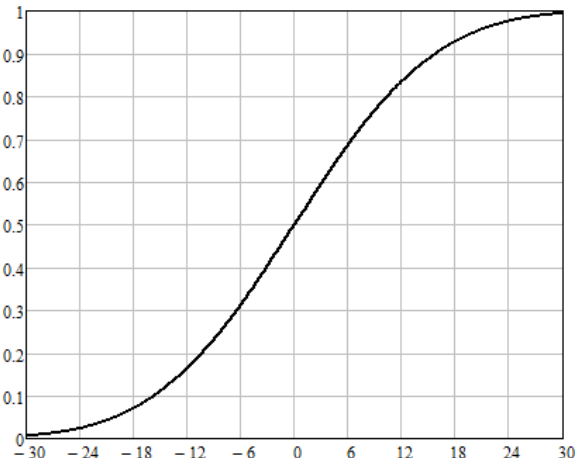


Рисунок 2.12 – Кривая коэффициента восприятия речи

Ссылка в тексте на рисунок: «…в соответствии с рисунком 4.3».
Если в разделе ВВЕДЕНИЕ есть рисунки, то они нумеруются как :
Рисунок В.1 – Название рисунка

Список использованных источников

Список использованных источников приводится в конце пояснительной записки. Список использованных учебников, справочников, статей, стандартов и др. следует располагать в порядке появления ссылок на источники в тексте работы и нумеровать арабскими цифрами без точки, печатать с абзацного отступа.

Список литературы должен быть составлен в алфавитном порядке. Список адресов серверов Internet указывается после литературных источников. При указании веб-адреса рекомендуется давать заголовок данного ресурса (заголовок веб-страницы).

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил:

1) законодательные акты и постановления правительства РФ;

2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи – название издания и его номер). Полное название литературного источника приводится в начале книги на 2-3 странице.

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При указании адресов серверов Internet сначала указывается название организации, которой принадлежит сервер, а затем его полный адрес.

Примеры записей:

1 Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: Автореф. дис. канд. техн. наук. – Новосибирск, 2000. – 18 с.

2 Экономика и политика России и государств ближнего зарубежья : аналит. обзор, апр. 2007, Рос. акад. наук, Ин-т мировой экономики и муждунар. отношений. – М. : ИМЭМО, 2007. – 39 с.

3 Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкого региона : дис. … канд. полит. наук. – М., 2002. – с. 54–55.

4 Официальные периодические издания : электронный путеводитель / Рос. нац. б-ка, Центр правовой информации. [СПб], 200520076. URL: http://www.nlr.ru/lawcrnter/izd/index.html (дата обращения: 18.01.2007).

5 Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).

6 Рынок тренингов Новосибирска: своя игра [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

Оформление приложений

Нумерация приложений осуществляется русскими буквами, кроме букв Ё, Й, Ъ, Ь, Ы, О.

В разделе СОДЕРЖАНИЕ название приложения оформляется следующим образом:

ПРИЛОЖЕНИЕ А – Диаграмма классов

В самом приложении слово **ПРИЛОЖЕНИЕ А** пишется жирным шрифтом по центру, на следующей строке пишется название приложения, по центру жирным шрифтом, например,

ПРИЛОЖЕНИЕ А
Диаграмма классов

Если приложение продолжается на следующей странице, то необходимо сверху по центру, нежирным шрифтом написать слова:

Продолжение Приложения А

Если в приложении, например, в приложении А есть таблицы, то они нумеруются как:

Таблица А.1– Название таблицы

Если в приложении есть рисунки, например, в приложении А, то они нумеруются как:

Рисунок А.1 – Название рисунка

Критерии оценки курсового проекта:

– оценка «отлично» выставляется обучающемуся, если студент представил курсовой проект в соответствии с методическими указаниями, информация в курсовом проекте сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы в области технической защиты информации;

– оценка «хорошо» выставляется обучающемуся, если студент представил курсовой проект в соответствии с методическими указаниями, информация в курсовом проекте сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы в области технической защиты информации, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил курсовой проект в соответствии с методическими указаниями, информация в курсовом проекте сформулирована с нарушением логики, не полная, формулировка общая

или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы в области технической защиты информации;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не представил курсовой проект или выполнил его неверно, без использования методических указаний, обоснования неверные, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы в области технической защиты информации.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Тема 1.1. Основные свойства информации как предмета технической защиты Тема 1.2. Демаскирующие признаки объектов защиты	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы, теста
Тема 1.3. Источники и носители конфиденциальной информации Тема 1.4 Источники опасных сигналов	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, контрольной работы
Тема 2.1. Виды угроз безопасности информации Тема 2.2. Органы разведки	Лекция - презентация	Не предусмотрено	выполнение контрольной работы
Тема 2.3. Технология разведки Тема 2.4. Способы несанкционированного доступа к источникам информации	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 2.5. Способы и средства добывания информации техническими средствами. Способы и средства наблюдения Тема 2.6. Способы и средства перехвата сигналов	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 2.7. Способы и средства подслушивания акустических сигналов	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 2.8. Способы и средства добывания информации о демаскирующих признаках веществ	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 2.9. Технические каналы утечки информации	Обзорная лекция	Не предусмотрено	выполнение теста
Тема 3.1. Концепция инженер-	Лекция -	Не предусмотре-	выполнение ла-

но-технической защиты информации	презентация	но	бораторной работы
Тема 3.2. Способы и средства инженерной защиты и технической охраны	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 3.3. Способы и средства защиты информации от наблюдения	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 3.4. Способы и средства защиты информации от подслушивания	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 3.5. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 3.6. Способы предотвращения утечки информации по материально-вещественному каналу	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 4.1. Общие положения по инженерно-технической защите информации в организации	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 4.2. Организационные и технические меры по инженерно-технической защите информации в организации	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 5.1. Системный подход к защите информации. Тема 5.2. Моделирование объекта защиты	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Тема 5.3. Моделирование угроз информации Тема 5.4. Методические рекомендации по разработке мер защиты	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, теста

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Цифровое обучение») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

В соответствии с ОПОП дисциплина должна быть поддержана соответствующими лицензионными программными продуктами.

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
MathCad 14	Система компьютерной алгебры из класса систем автоматизированного проектирования, ориентированная на подготовку интерактивных документов с вычислениями и визуальным сопровождением, отличается лёгкостью использования
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
MS Visual Studio	Среда разработки программ для ЭВМ

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Ин-

форм-систем»: https://library.asu.edu.ru.

2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.

3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/

4. Электронно-библиотечная система elibrary. http://elibrary.ru

5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru

6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Техническая защита информации» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1	Тема 1.1. Основные свойства информации как предмета технической защиты Тема 1.2. Демаскирующие признаки объектов защиты	ОПК 9, ОПК 10	Входное тестирование Отчет по лабораторной работе № 1
2	Тема 1.3. Источники и носители конфиденциальной информации Тема 1.4 Источники опасных сигналов	ОПК 9, ОПК 10	Отчет по лабораторной работе № 1 Контрольная работа № 1
3	Тема 2.1. Виды угроз безопасности информации Тема 2.2. Органы разведки	ОПК 9, ОПК 10	Контрольная работа № 2.
4	Тема 2.3. Технология разведки Тема 2.4. Способы несанкционированного доступа к источникам информации	ОПК 9, ОПК 10	Отчет по лабораторной работе № 2
5	Тема 2.5. Способы и средства добывания информации техническими средствами. Способы и средства наблюдения Тема 2.6. Способы и средства перехвата сигналов	ОПК 9, ОПК 10	Отчет по лабораторной работе № 2
6	Тема 2.7. Способы и средства подслушивания акустических сигналов	ОПК 9, ОПК 10	Отчет по лабораторной работе № 2

7	Тема 2.8. Способы и средства добывания информации о демаскирующих признаках веществ	ОПК 9, ОПК 10	Отчет по лабораторной работе № 2
8	Тема 2.9. Технические каналы утечки информации	ОПК 9, ОПК 10	Промежуточн. тестирование
9	Тема 3.1. Концепция инженерно-технической защиты информации	ОПК 9, ОПК 10	Отчет по лабораторной работе № 3
10	Тема 3.2. Способы и средства инженерной защиты и технической охраны	ОПК 9, ОПК 10	Отчет по лабораторной работе № 3
11	Тема 3.3. Способы и средства защиты информации от наблюдения	ОПК 9, ОПК 10	Отчет по лабораторной работе 3
12	Тема 3.4. Способы и средства защиты информации от подслушивания	ОПК 9, ОПК 10	Отчет по лабораторной работе 3
13	Тема 3.5. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	ОПК 9, ОПК 10	Отчет по лабораторной работе № 4
14	Тема 3.6. Способы предотвращения утечки информации по материально-вещественному каналу	ОПК 9, ОПК 10	Отчет по лабораторной работе 4
15	Тема 4.1. Общие положения по инженерно-технической защите информации в организации	ОПК 9, ОПК 10	Отчет по лабораторной работе № 5
16	Тема 4.2. Организационные и технические меры по инженерно-технической защите информации в организации	ОПК 9, ОПК 10	Отчет по лабораторной работе 5
17	Тема 5.1. Системный подход к защите информации. Тема 5.2. Моделирование объекта защиты	ОПК 9, ОПК 10	Отчет по лабораторной работе № 6
18	Тема 5.3. Моделирование угроз информации Тема 5.4. Методические рекомендации по разработке мер защиты	ОПК 9, ОПК 10	Итоговое тестирование. Отчет по лабораторной работе № 6

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

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовле-	демонстрирует неполное, фрагментарное знание теоретического ма-

творительно»	териала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

7.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Раздел 1. Объекты информационной безопасности

Тема 1.1. Основные свойства информации как предмета технической защиты
Тема 1.2. Демаскирующие признаки объектов защиты
Тема 1.3. Источники и носители конфиденциальной информации
Тема 1.4 Источники опасных сигналов

Вопросы к входному тестированию.

Вопрос 1

К информации ограниченного доступа относятся:

А) Государственная тайна
Б) Персональные данные
В) Сведения о сущности изобретения
Г) Все вышеперечисленное

Вопрос 2

К конфиденциальной информации не относится:

А) Государственная тайна
Б) Персональные данные
В) Сведения о сущности изобретения

Г) Все вышеперечисленное относится к конфиденциальной информации

Вопрос 3

Найдите лишнее. Демаскирующие признаки по информативности подразделяются на:

А) Именные Б) Сигнальные В) Прямые Г) Косвенные

Вопрос 4

Найдите лишнее. По времени проявления демаскирующие признаки делятся на:

А) Сигнальные Б) Постоянные В) Периодические Г) Эпизодические

Вопрос 5

К источникам информации не относятся:

А) Люди	Б) Документы	В) Поля и элементарные частицы	Г) Продукция

Вопрос 6

Что из перечисленного является носителем информации:

А) Люди. Б) Материальные тела.

В) Поля и элементарные частицы Г) Все из вышеперечисленного

Лабораторно-практическая работа 1. Изучение принципа работы и применения анализатора виброакустической защиты «SI-4000», прибора виброакустической защиты SI-3001.

Цель работы: Проведение измерения относительного уровня интенсивности акустических колебаний.

Задача №1: Изучить теоретический материал по работе с приборами: Анализатор виброакустической защиты «SI-4000», прибор виброакустической защиты SI-3001.

Задача №2: Вычислить относительный уровень интенсивности помехи и сравнить его с излучаемым сигналом SI-3100.

Вопросы к контрольной работе № 1

1. Методы предотвращения наблюдения через окна.
2. Физическая природа каналов утечки информации.
3. Использование извещателей для охраны отдельных объектов.
4. Задачи информационной безопасности, решаемые на организационном уровне.
5. Основные видовые демаскирующие признаки объектов радиолокационного наблюдения.
6. Классификация демаскирующих признаков объекта.
7. Методы противодействия техническим средствам разведки.
8. Характеристики информации, защищаемой техническими средствами.
9. Основные способы наблюдения при помощи технических средств.
10. Основные источники функциональных опасных сигналов.
11. Классификация средств обнаружения злоумышленников.
12. Зоны защиты объекта техническими средствами охраны.
13. Классификация строительных конструкций по степени защиты объекта.
14. Классификация извещателей.
15. Структура системы технической разведки.
16. Основные организационные и режимные мероприятия по защите информации.

17. Основные способы приема информации техническими средствами злоумышленника.

18. Структура комплекса технических средств охраны объекта.

19. Виды инженерных средств защиты (физических барьеров).

20. Классификация критически важных объектов.

Раздел 2. Угрозы безопасности информации

Тема 2.1. Виды угроз безопасности информации

Тема 2.2. Органы разведки

Тема 2.3. Технология разведки

Тема 2.4. Способы несанкционированного доступа к источникам информации

Тема 2.5. Способы и средства добывания информации техническими средствами. Способы и средства наблюдения

Тема 2.6. Способы и средства перехвата сигналов

Тема 2.7. Способы и средства подслушивания акустических сигналов

Тема 2.8. Способы и средства добывания информации о демаскирующих признаках веществ

Тема 2.9. Технические каналы утечки информации

Вопросы к промежуточному тестированию.

Вопрос 1

Элементами структуры канала связи являются:

а) Источник сигнала;

б) Приемник сигнала;

в) Среда распространения;

г) Помехи;

д) Все выше перечисленное.

Вопрос 2

Для какого канала утечки информации средой распространения будут являться безвоздушное пространство, атмосфера, оптические световоды?

а) Радиоэлектронные каналы утечки информации;

б) Оптические каналы утечки информации;

в) Акустические канала утечки информации;

г) Материально-вещественные каналы утечки информации.

Вопрос 3

Для какого канала утечки информации средой распространения будут являться безвоздушное пространство, атмосфера, направляющие?

а) Радиоэлектронные каналы утечки информации;

б) Оптические каналы утечки информации;

в) Акустические канала утечки информации;

г) Материально-вещественные каналы утечки информации.

Вопрос 4

Цена информации при ее утечки:

а) Увеличивается;

б) Уменьшается;

в) Не изменяется.

Вопрос 5

Что относится к источникам сигналов в радиоэлектронных каналах утечки информации?

а) передатчики функциональных каналов связи;
б) источники опасных сигналов;
в) объекты, отражающие электромагнитные волны в радиодиапазоне;
г) объекты, излучающие собственные (тепловые) радиоволны в радиодиапазоне;
д) все выше перечисленное.

Лабораторно-практическая работа 2. Изучение принципа работы и применения универсального анализатора проводных коммуникаций ULAN-2.

Цель работы: Ознакомление с прибором ULAN-2, и проверка работоспособности прибора.
Задача №1: Изучить теоретический материал по работе с прибором: ULAN-2.
Задача №2: Собрать стенд и провести обнаружения подключенных несанкционированных приборов к линии.

Вопросы к контрольной работе № 2

1. Классификация электроакустических преобразователей.
2. Основные источники ПЭМИН.
3. Характеристики случайных антенн и их классификация.
4. Характер распространения электромагнитных волн от сосредоточенного источника. Зоны распространения электромагнитных волн.
5. Средства озвучивания акустической информации как источники низкочастотных колебаний.
6. Законодательство об информации, информационных технологиях и о защите информации
7. Состав источников информации канала утечки информации за счет ПЭМИН.
8. Классификация демаскирующих признаков по времени проявления.
9. Основные направления противодействия техническим средствам разведки.
10. Классификация информации, защищаемой техническими средствами.
11. Способы наблюдения при помощи технических средств.
12. Основные источники функциональных опасных сигналов.
13. Классификация зон защиты объекта техническими средствами охраны.
14. Классификация средств обнажения злоумышленников.
15. Классификация извещателей по принципу обнаружения.
16. Классификация строительных конструкций по степени защиты объекта от проникновения.
17. Классификация электроакустических преобразователей по принципу действия.
18. Типы паразитных связей, приводящих к появлению ПЭМИН.
19. Характеристики среды распространения ПЭМИН.
20. Классификация извещателей по виду зон обнаружения.

Раздел 3. Методы, способы и средства инженерно-технической защиты информации

Тема 3.1. Концепция инженерно-технической защиты информации

Тема 3.2. Способы и средства инженерной защиты и технической охраны

Тема 3.3. Способы и средства защиты информации от наблюдения

Тема 3.4. Способы и средства защиты информации от подслушивания

Тема 3.5. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки

Тема 3.6. Способы предотвращения утечки информации по материально-вещественному каналу

Лабораторно-практическая работа 3. Изучение принципа работы и применения портативного нелинейного радиолокатора ONEGA-23.

Цель работы: Ознакомление с прибором ONEGA-23, и проверка работоспособности прибора.

Задача №1: Изучить теоретический материал по работе с прибором: ONEGA-23.

Задача №2: Провести поиск устройств, содержащих полупроводниковые компоненты, как во включенном, так и в выключенном состоянии.

Лабораторно-практическая работа 4. Изучение принципа работы и применения спектрального коррелятора OSCOR OSC- 5000.

Цель работы: Обнаружение и локализация работающих радиопередающих специальных технических средств съема информации.

Задача №1: Изучить теоретический материал по работе с прибором: OSCOR OSC- 50002.

Задача №2: Ознакомление с методом обнаружения опасных сигналов с использованием спектрального коррелятора «OSCOR OSC- 5000».

Задача №3: Ознакомление с методом обнаружения опасных сигналов с использованием режимов просмотра спектра прибора OSCOR и приобретение навыков использования автоматического режима работы.

Задача №4: Ознакомление с механизмами поиска и сохранения частот прибора OSCOR и приобретение навыков их использования.

Раздел 4. Организация инженерно-технической защиты информации

Тема 4.1. Общие положения по инженерно-технической защите информации в организации

Тема 4.2. Организационные и технические меры по инженерно-технической защите информации в организации

Лабораторно-практическая работа 5. Изучение принципа работы и применения многофункционального поискового прибора ST-031 «Пиранья».

Цель работы: Обнаружение и локализация в ближней зоне радиоизлучающих специальных технических средств (РСТС) негласного получения информации.

Задача №1: Изучить теоретический материал по работе с прибором: ST-031 «Пиранья».

Задача №2: Провести обследование помещения лаборатории на наличии закладных устройств.

Раздел 5. Основы методического обеспечения инженерно-технической защиты информации

Тема 5.1. Системный подход к защите информации.

Тема 5.2. Моделирование объекта защиты

Тема 5.3. Моделирование угроз информации

Тема 5.4. Методические рекомендации по разработке мер защиты

Вопросы к итоговому тестированию.

Вопрос 1

Для уменьшения контраста/фона используют следующие способы маскировки (укажите лишнее):

а) маскировочная обработка местности;

б) маскировочное окрашивание;

в) покрытие объекта радиоотражающими оболочками;

г) нанесение на объект воздушных пен.

Вопрос 2

К способам защиты от подслушивания относятся:

а) информационное скрытие;

б) энергетическое скрытие;

в) обнаружение, локализация и изъятие закладных устройств

г) все выше перечисленное.

Вопрос 3

К информационному скрытию при защите от подслушивания относятся:

а) звукоизоляция акустического сигнала;

б) глушение акустических сигналов;

в) шифрование семантической речевой информации в функциональных каналах связи;

г) все выше перечисленное.

Вопрос 4

Для уменьшения энергии носителя при скрытии акустического сигнала применяют (укажите лишнее):

а) звукоизоляция;

б) генерация акустических помех;

в) глушение звука;

г) звукопоглощение.

Вопрос 5

К основным средствам звукоизоляции НЕ относятся:

а) кабина;

б) кожух;

в) экран;

г) ограждение;

д) все вышеперечисленное относится к средствам звукоизоляции.

Вопрос 6

К средствам обнаружения и локализации закладных устройств относятся:

а) средства радиоконтроля помещений;

б) средства поиска неизлучающих закладных устройств;

в) средства подавления закладных устройств;

г) Все выше перечисленное.

Вопрос 7

Средства подавления закладных устройств.

а) генераторы помех;

б) средства нарушения работы закладки;

в) средства разрушения закладных устройств;

г) все указанное выше.

Вопрос 8

К информационному скрытию НЕ относится:

а) маскировка;

б) зашумление;

в) дезинформирование;

г) все вышеперечисленное относится

к методам информационного скрытия.

Лабораторно-практическая работа 6. Изучение принципа работы и применения прибора ST 006 (Детектор поля).

Цель работы: Обнаружение и локализация в ближней зоне радиоизлучающих специальных технических средств (РСТС) негласного получения информации.

Задача №1: Изучить теоретический материал по работе с прибором: ST 006 (Детектор поля).

Задача №2: Провести обследование помещения лаборатории на наличии закладных устройств.

Критерии оценки лабораторных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам дисциплины.

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, умеет настраивать и использовать технические средства защиты информации;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, умеет настраивать и использовать технические средства защиты информации, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, умеет настраивать и использовать технические средства защиты информации;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания технологий и методов программирования.

Перечень вопросов к экзамену

1. Предмет, цели, задачи инженерно-технической защиты информации.
2. Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты.
3. Классификация демаскирующих признаков.

4. Понятие об источниках, носителях и получателях информации. Классификация источников информации.

5. Виды носителей информации. Способы записи информации на различные виды носителей.

6. Понятие об опасных сигналах и источниках.

7. Виды потенциальных угроз безопасности информации.

8. Разведка.

9. Основные принципы и этапы добывания информации.

10. Способы несанкционированного доступа к источникам информации.

11. Средства и способы наблюдения: средства наблюдения в оптическом диапазоне, средства наблюдения в инфракрасном диапазоне, средства наблюдения в радиодиапазоне.

12. Способы и средства перехвата сигналов.

13. Способы и средства добывания информации о демаскирующих признаках веществ.

14. Типовая структура технического канала утечки информации.

15. Оптические каналы утечки информации.

16. Радиоэлектронные каналы утечки информации.

17. Акустические каналы утечки информации.

18. Материально-вещественные каналы утечки информации.

19. Цели, задачи и принципы инженерно-технической защиты информации.

20. Концепция охраны объекта.

21. Способы и средства инженерной защиты объектов.

22. Способы и средства обнаружения злоумышленников и пожара.

23. Способы и средства видеоконтроля.

24. Способы и средства нейтрализации угроз.

25. Средства управления системой охраны.

26. Способы и средства противодействия наблюдению в оптическом диапазоне волн.

27. Скрытие и маскировка.

28. Способы и средства противодействия радиолокационному и гидроакустическому наблюдению.

29. Способы и средства информационного скрытия акустических сигналов и речевой информации.

30. Способы и средства энергетического скрытия акустических сигналов.

31. Способы и средства предотвращения утечки информации с помощью закладных устройств.

32. Классификация способов предотвращения утечки информации по материально-вещественному каналу.

33. Краткая характеристика государственной системы защиты информации.

34. Основные руководящие и нормативные документы по организации инженерно-технической защиты информации в организации, их сущность.

35. Функции сотрудников службы безопасности, обеспечивающих инженерно-техническую защиту информации.

36. Основные направления инженерно-технической защиты информации в организации.

37. Основные организационные и технические меры по обеспечению инженерно-технической защиты информации.

38. Задачи и виды контроля эффективности защиты информации.

39. Алгоритм проектирования системы защиты информации.

40. Сущность и методические рекомендации по структурированию защищаемой информации.

41. Виды моделей угроз информации.

42. Методические рекомендации по определению путей проникновения злоумышленника к источнику информации, формы моделей.

43. Типовые индикаторы каналов утечки.

44. Методические рекомендации по моделированию каналов утечки. Формы представления результатов моделирования.

Критерии оценки экзамена:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам делопроизводства.

Примерная тематика курсовых проектов

1. Программа фильтрации звуковых файлов
2. Программа расчета основных характеристик для исследования объекта с помощью нелинейного радиолокатора.
3. Программный акустический анализатор.
4. Программный акустический генератор.
5. Виртуальный анализатор проводных коммуникаций.
6. Виртуальная модель поиска сигналов ПЭМИН методом разности панорам
7. Виртуальная модель поиска сигналов ПЭМИН аудио-визуальным методом
8. Виртуальная модель поиска сигналов ПЭМИН экспертным методом
9. Виртуальная модель поиска сигналов ПЭМИН Параметрически - корреляционный метод
10. Корреляционный анализ акустических сигналов
11. Программа расчета основных характеристик для исследования объекта с помощью индикатора поля.
12. Программа для расчета среднестатистического спектра энергии речевого сигнала.
13. Виртуальная модель анализа проводных коммуникаций методом импульсной рефлектометрии.
14. Индикаторы электромагнитного поля
15. Сканирующие радиоприемники
16. Анализаторы спектра, радиочастотомеры
17. Многофункциональные комплекты для выявления каналов утечки информации
18. Нелинейные локаторы
19. Безопасность оптоволоконных кабельных систем
20. Фильтрация информационных сигналов
21. Пространственное и линейное зашумление
22. Устройства контроля и защиты слаботочных линий и сети

23. Статистический анализ загрузки заданного радиодиапазона и обнаружение закладных устройств

24. Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу.

25. Оценка защищенности ограждающих конструкций помещения от утечки информации по виброакустическому каналу.

26. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра

27. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра

28. Акустоэлектрические каналы утечки речевой информации

29. Особенности слаботочных линий и сетей как каналов утечки информации

30. Мероприятия по выявлению и оценке свойств каналов утечки информации

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ОПК-9 способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности				
1.	Задание закрытого типа	К основным видовым демаскирующим признакам объектов радиолокационного наблюдения относятся: в) эффективная поверхность рассеяния б) температура поверхности в) геометрические и яркостные характеристики (форма, размеры, яркость) г) геометрические характеристики объектов д) электропроводимость поверхности	а, в, г	2
2.		В каком канале утечки информации перенос информации возможен сотрудниками организации, воздушными массами атмосферы, жидкой средой? а) Радиоэлектронные каналы утечки информации; б) Оптические каналы утечки информации; в) Акустические канала утечки информации; г) Материально-вещественные каналы утечки информации.	г	2
3.		Для какого канала утечки информации средой распространения будут являться однородные среды (воздух, вода) и неоднородные (воздух, древесина, стекла окон, бетон, кирпичи стен и т.п.)?	в	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		а) Радиоэлектронные каналы утечки информации; б) Оптические каналы утечки информации; в) Акустические канала утечки информации; г) Материально-вещественные каналы утечки информации.		
4.		Какой ТКУИ обладает следующими особенностями: высокая достоверность добываемой информации, большой объем добываемой информации, оперативность получения информации, скрытность перехвата сигнала? а) Радиоэлектронные каналы утечки информации; б) Оптические каналы утечки информации; в) Акустические канала утечки информации; г) Материально-вещественные каналы утечки информации.	а	2
5.		Структура канала утечки информации: а) источник сигнала б) среда распространения в) приемник сигнала г) ПЭМИН д) человек е) скорость распространения	а, б, в	2
6.	Задание открытого типа	Источники опасных сигналов	Источниками опасных сигналов могут быть: 1) акустоэлектрические преобразователи (пьезоэлектрические, емкостные, индуктивные); 2) излучатели низкочастотных сигналов (элементы РЭС, усилительные каскады, генераторы, ПЭВМ); 3) излучатели высокочастотных сигналов; 4) паразитные связи и наводки (гальванические, индуктивные, емкостные).	2
7.		Какими средствами возможен перехват акустических сигналов по виброакустическим техническим	Перехват акустических сигналов по виброакустическим	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		каналам?	техническим каналам возможен: электронными стетоскопами; стетоскопами с передачей информации по радиоканалу; стетоскопами, подключенными к устройствам передачи информации по оптическому каналу в ИК-диапазоне длин волн; стетоскопами, объединенными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям	
8.		Перечислить демаскирующие признаки	Демаскирующие признаки: расположения – признак, определяющий положение объекта среди других объектов и предметов окружающего пространства; структурно-видовой – признак, определяющий структуру и видовые характеристики группового объекта (состав, количество и расположение отдельных объектов, форму и геометрические размеры); деятельности – признак, раскрывающий функционирование объекта через физические проявления.	2
9.		Основные показатели, характеризующие сканирующие радиоприемники	Сканирующие радиоприемники характеризуются следующими основными показателями: диапазоном принимаемых частот; чувствительностью; избирательностью; параметрами сканирования (скоростью	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			перестройки, полосами обзора и т.д.); используемым методом или методами, если они есть, обнаружения сигналов; видом принимаемых радиосигналов; оперативностью управления и возможностями его автоматизации; выходными параметрами (качество воспроизведения сигнала на выходе приемника, наличие выходов по промежуточной и низкой частоте, значения полос пропускания сигнала по этим частотам и т.д.); эксплуатационными параметрами (массогабаритные характеристики, требования по электропитанию, надежность, ремонтопригодность. удобство транспортировки и т.п.).	
10.		Принципы проектирования систем технической защиты	Принципы проектирования систем технической защиты: непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности; многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности; избирательность, заключающаяся в предотвращении угроз в	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			первую очередь для наиболее важной информации; интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности; создание централизованной службы безопасности в интегрированных системах	
ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты				
1.	Задание закрытого типа	В зависимости от местоположения носителей аппаратуры разведки рассматривают следующие виды средств технической разведки (СТР): 1. космические СТР 2. наземные СТР 3. воздушные СТР 4. морские СТР 5. подводные СТР 6. орбитальные СТР	1, 2, 3, 4	2
2.		Электронные устройства перехвата речевой информации могут подключаться к телефонным линиям следующими способами: 1. последовательно 2. параллельно 3. с помощью индукционного датчика 4. с помощью магнитострикционного датчика 5. смешанное подключение	1, 2, 3	2
3.		Специально подготовленная, согласованная по месту, времени и формам деятельность, направленная на извлечение, систематизацию и специальную обработку открытой информации из информационно-вычислительных сетей, телекоммуникационных систем, а также информацию об особенностях их построения и функционирования это	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		1. Компьютерная разведка 2. Фотографическая разведка 3. Визуальная оптическая разведка 4. Акустическая разведка		
4.		К демаскирующим признакам объектов в инфракрасном диапазоне электромагнитного спектра относятся: 1. собственное (естественное) излучение нагретых тел 2. отраженное объектами (искусственное) ИК-излучение 3. фоновое излучение нагретых тел 4. рентгеновское излучение нагретых тел	1, 2	2
5.		Добывание информации, содержащейся в изображениях космических, воздушных, наземных и морских объек тов, получаемых по отраженным от них сигналам в радиодиапазоне электромагнитных волн: 1. радиолокационная видовая разведка 2. радиотехническая разведка 3. радиотепловая разведка 4. разведку ПЭМИН электронных средств обработки информации	1	2
6.	Задание открытого типа	Источники речевого сигнала	Источники речевого сигнала могут быть следующих видов: источник первичного речевого сигнала (говорящий человек): а) локализованный в определенной области пространства, ограниченного ограждающими конструкциями помещения или границами контролируемой зоны; б) неопределенный (нелокализованный) в области пространства, ограниченного ограждающими конструкциями помещения или границами контролируемой зоны; технические средства звукоусиления и	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			звуковоспроизведения; технические средства передачи речевых сигналов по проводным линиям связи; технические средства передачи речевых сигналов по радиоканалу	
7.		Классификация технических разведок по обнаружению и перехвату речевых сигналов	Классификация технических разведок по обнаружению и перехвату речевых сигналов представлена следующими видами разведок: Акустическая речевая разведка (АРР). Вибрационная речевая разведка (ВРР). Оптико-электронная (лазерная) речевая разведка (ОЭРР). Разведка ПЭМИН. Радиоразведка (РР). Визуальная оптическая разведка. Визуальная оптико-электронная разведка.	3
8.		Комплекс мероприятий по защите выделенных помещений (ВП) или защищенных помещений	В общем случае комплекс мероприятий по защите выделенных помещений (ВП) или защищенных помещений (ЗП) включает: защиту речевой информации, обрабатываемой техническими средствами, от утечки за счет электромагнитных излучений и наводок (ПЭМИН); защиту речевой информации от утечки за счет эффекта электроакустического преобразования вспомогательных технических средств и систем (ВТСС); защиту речевой информации от утечки за счет лазерного	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			зондирования стекол или стетоскопического прослушивания ограждающих конструкций; защиту речевой информации от утечки за счет несанкционированного доступа в помещение и скрытой установки в нем подслушивающих приборов; акустическую защиту помещений.	
9.		Технические демаскирующие признаки объекта разведки (ОР), обеспечивающие их распознавание	Технические демаскирующие признаки ОР, обеспечивающие их распознавание, можно разделить на следующие группы: 1. Признаки, характеризующие физические свойства вещества ОР (теплопроводность, электропроводность, структура, твердость и т. д.); 2. Признаки, характеризующие физические поля, создаваемые ОР (электро магнитное, акустическое, радиационное, гидроакустическое и т. д.); 3. Признаки, характеризующие форму, цвет, размеры самого ОР и его элементов; 4. Пространственные признаки, характеризующие как координаты ОР в пространстве, так и их производные; 5. Признаки, характеризующие наличие определенных связей в ОР, между его элементами; 6. Признаки,	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			характеризующие результаты функционирования ОР (задымленность, запыленность, следы ОР на грунте, разработка грунта, последствия взрывов и стрельбы, загрязнение воды, воздуха, земли продуктами функционирования ОР).	
10.		Этапы процесса анализа демаскирующих признаков (ДП)	Процесс анализа ДП определяется следующими этапами: – изучение принципов функционирования ОР и формирования информационных сигналов; – выявление демаскирующих признаков и их параметров, которые могут быть положены в основу ведения разведки относительно анализируемого ОР. В результате этого этапа составляется перечень ДП и их параметров, которые могут быть использованы СТР для ведения разведки; – на основе составленного перечня ДП и их параметров формируется перечень «опасных» видов ТР и возможных технических каналов утечки информации, по которым может осуществлять свою деятельность техническая разведка.	3

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Фонды оценочных средств по дисциплине

Фонд оценочных средств позволяет оценить знания, умения и уровень приобретенных компетенций.

Фонд оценочных средств по дисциплине включает:

- вопросы к экзамену;
- набор вариантов контрольных работ;
- темы для курсовых проектов;
- тестовый комплекс.

Оценка качества освоения программы дисциплины включает текущий контроль успеваемости, промежуточную аттестацию, итоговую аттестацию.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине на экзамен во втором семестре отводится 100 баллов (40 баллов на текущие формы контроля, 10 баллов на бонусы и 50 баллов отводится на экзамен),

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

Критерии оценок на экзамене:

40-50 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности.

35-39 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

25-34 балла – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

20-22 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала. 1

1-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки. 1

0 баллов – ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

6-9 баллов – студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

1-5 баллов – студент имеет лишь частичное представление о теме. 0 баллов – нет ответа.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	6/5	30	По расписанию
2.	*Выполнение контрольной работы*	2/2	4	
3.	*Тест*	3/3	6	
Всего			**40**	-
Блок бонусов				

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
4.	*Посещение занятий без пропусков*	1	3	
5.	*Своевременное выполнение всех заданий*	1	3	
6.	*Активность студента на занятии*	1	4	
Всего			**10**	-
Дополнительный блок				
7.	*Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

8.1. Основная литература

1. Технические средства и методы защиты информации [Электронный ресурс] : Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. - М. : Горячая линия - Телеком, 2012. http://www.studentlibrary.ru/book/ISBN9785991202336.html

2. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М.: ДМК Пресс, 2014. - http://www.studentlibrary.ru/book/ISBN9785940747680.html

8.2. Дополнительная литература

1. Инженерно-техническая и пожарная защита объектов [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 4. - М. : Горячая линия - Телеком, 2012. - (Серия "Обес-

печение безопасности объектов"). - http://www.studentlibrary.ru/book/ISBN9785991201797.html

2. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - http://www.studentlibrary.ru/book/ISBN9785940745181.html

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

Материально-техническое обеспечение дисциплины включает в себя учебные лаборатории и классы, оснащенные современными компьютерами, объединенными локальными вычислительными сетями с выходом в Интернет. Учащимся предоставляется возможность практической работы на ЭВМ различной архитектуры (на базе одноядерных, многоядерных, параллельных процессоров).

Наименование программного обеспечения	Назначение
OSC5000 deLuxe	спектральный коррелятор
SI-2060	устройство защиты телефонной лини
SI-3001	шумогенератор виброакустический
SI-4000	программно-аппаратный комплекс
SP-41/C	шумогенератор сетевой
ST 006	детектор поля
ST-031	«Пиранья» – поисковый комплекс
Гром ЗИ 4	шумогенератор
Кобра	защита проводных линий
КРЦ-3	шумогенератор
Онега-23М	нелинейный локатор импульсный
УЛАН	проверочное устройство проводных линий
ФСП-1Ф-7А	сетевой фильтр

OMS-2000	акустический излучатель

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).