МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института (филиал) СКФУ
_____ Т.А. Шебзухова
«__» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Техническая защита информации

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки/специальность 10.03.01 Информационная безопасность
Квалификация выпускника: бакалавр
Форма обучения очная
Год начала обучения 2021
Изучается в 5 семестре

г. Пятигорск 20__ г.

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Техническая защита информации» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачами дисциплины являются:

- 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.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока. Ее освоение происходит в 5 и 6 семестрах.

3. Связь с предшествующими дисциплинами

Пререквизитом является дисциплина «Основы информационной безопасности».

4. Связь с последующими дисциплинами

Кореквизитами являются: «Программно-аппаратные комплексы защиты объектов информатизации», «Комплексная система защиты информации на предприятии», «Многоканальные цифровые системы передачи и средства их защиты», «Подготовка к сдаче и сдача государственного экзамена».

5. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

5.1 Наименование компетенций

Код	Формулировка:
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-13	способность принимать участие в формировании, организовывать и

	поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

5.2 Знания, умения и навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации **Уметь:** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации **Владеть:** способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**ПК-1**
Знать: работу по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты **Уметь:** участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты **Владеть:** способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**ПК-4**
Знать: организацию и сопровождение аттестации объекта информатизации по требованиям безопасности информации **Уметь:** принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации **Владеть:** способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**ПК-5**
Знать: экспериментальные исследования системы защиты информации **Уметь:** принимать участие в проведении экспериментальных исследований системы защиты информации **Владеть:** способностью принимать участие в проведении экспериментальных исследований системы защиты информации	**ПК-12**
Знать: участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации **Уметь:** принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации **Владеть:** способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	**ПК-13**
Знать: информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе	**ОПК-7**

анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты **Уметь:** определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты **Владеть:** способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.	

6. Объем учебной дисциплины/модуля

	Астр. часы
Объем занятий: Итого	189 ч. 7 з.е.
В том числе аудиторных	76,5 ч.
Из них:	
Лекций	39 ч.
Лабораторных работ	25,5 ч.
Практических занятий	12 ч.
Самостоятельной работы	58,5 ч.
Курсовая работа	6 семестр
Экзамен	5, 6 семестр

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества астрономических часов и видов занятий

7.1 Тематический план дисциплины

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
5 семестр							
1.	Тема 1. Законодательные акты в области технической защиты информации.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3				3
2.	Тема 2. Классификация технических каналов утечки информации. Типы носителей информации в технических каналах связи. Основные показатели технического канала утечки информации.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3				3

3.	Тема 3. Способы получения информации по визуально-оптическому каналу. Средства получения видовой информации	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3				
4.	Тема 4. Основные способы обнаружения видеокамер. Средства и способы защиты информации от утечки по визуально-оптическому каналу.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3		1,5		
5.	Тема 5. Основные понятия в области акустики. Классификация акустических каналов утечки информации	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3				3
6.	Тема 6. Средства акустической разведки. Оценка утечки речевой информации по виброакустическим каналам	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3		6		3
7.	Тема 7. Звукоизоляция. Зашумление. Подавление диктофонов.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3		1,5		
8.	Тема 8. Краткая классификация закладочных устройств. Спецобследование помещений	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3		3		
9.	Тема 9. Защита информации по каналу низкочастотного акустоэлектрического преобразования	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	3		1,5		1,5
	Итого за 5 семестр		**27**		**13,5**		**13,5**
		6 семестр					
10.	Тема 10. Побочные электромагнитные излучения СВТ. Средства перехвата радиосигналов.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	1,5	1,5	1,5		7,5
11.	Тема 11. Пассивные методы защиты. Заземление. Фильтрация опасных сигналов.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	1,5	1,5	1,5		7,5
12.	Тема 12. Активные методы защиты. Зашумление.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	1,5	1,5	1,5		7,5
13.	Тема 13. Индикаторы электромагнитных излучений. Радиочастотометры. Сканирующие приемники.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	1,5	1,5	1,5		7,5
14.	Тема 14. Автоматизированные поисковые комплексы.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	1,5	1,5	1,5		7,5
15.	Тема 15. Паразитные связи и наводки.	ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	4,5	4,5	4,5		7,5
	Итого за 6 семестр		**12**	**12**	**12**		**45**
	Итого		**39**	**12**	**25,5**		**58,5**

7.2 Наименование и содержание лекций

№ темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Интерактивная форма проведения
	5 семестр		

1.	**Тема** Законодательные акты в области технической защиты информации. Правовые и организационно-распорядительные документы по технической защите конфиденциальной информации составляющие: • общие сведения; • Сведения об аттестации объектов информатизации; • Сведения о сертификации средств защиты информатизации; • о лицензировании; • перечень основных НМД по защите информации СВТ по каналу ПЭМИН; • Руководящие документы; • Постановления правительства; • ГОСТы. Основные понятия и определения по теме; понятие утечки по техническому каналу; типовая схема утечки информации за пределы КЗ.	3	
2.	**Тема** Классификация технических каналов утечки информации. Типы носителей информации в технических каналах связи. Основные показатели технического канала утечки информации. Виды технических каналов утечки информации. Классификация технических каналов утечки информации по: • физической природе носителя; • по информативности; • по времени функционирования; • по структуре. Примеры технических каналов утечки информации. Носителем информации в оптическом канале. В радиоэлектронном канале. В соответствии с видами носителей информации радиоэлектронный канал целесообразно разделить на 2 подвида: электромагнитный и электрический канал. Носителями информации в акустическом канале. В материально-вещественном канале.	3	
3.	**Тема** Способы получения информации по визуально-оптическому каналу. Средства получения видовой информации. В зависимости от характера информации можно выделить три способа ее получения: наблюдение за объектами, съёмка объектов, съёмка документов.	3	
4.	**Тема** Основные способы обнаружения видеокамер. Средства и способы защиты информации от утечки по визуально-оптическому каналу. Существует несколько способов обнаружения скрытых видеокамер:	3	

	• обнаружение видеокамер с помощью НЛ; • обнаружение беспроводных видеокамер с помощью средств радиомониторинга; • обнаружение видеокамер за счет анализа ПЭМИ; Средства: индикаторы поля, устройства, работающих по оптическому принципу, “универсальные” устройства.		
5.	**Тема** Основные понятия в области акустики. Классификация акустических каналов утечки информации Определить понятия и природу звука, какая информация называется акустической. Что такое звуковое давление, уровень звукового давления, сила (интенсивность) звука, уровень силы звука, порог слышимости, громкость звука, динамический диапазон. Источником образования акустического канала утечки информации являются вибрирующие, колеблющиеся тела и механизмы, такие как голосовые связки человека, движущиеся элементы машин, телефонные аппараты, звукоусилительные системы и т.д. В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронный и параметрические	3	Мультимедиа лекция
6.	**Тема** Средства акустической разведки. Оценка утечки речевой информации по виброакустическим каналам По способу применения технические средства съема акустической информации можно подразделить на две большие категории: 1. Средства, требующие физического проникновения в защищаемые помещения: • радиозакладки; • закладки с передачей акустической информации в ИК-диапазоне; • закладки с передачей по сети 220 В; • закладки с передачей информации по телефонной линии; • диктофоны; • проводные микрофоны; • "телефонное ухо". 2. средства, не требующие физического проникновения в защищаемые помещения: • аппаратура, использующая "микрофонный эффект" устройств; • аппаратура высокочастотного навязывания; • стетоскопы; • лазерные микрофоны; • направленные микрофоны.	3	Мультимедиа лекция
7.	**Тема** Звукоизоляция. Зашумление. Подавление	3	Мультимедиа лекция

	диктофонов. Методы защиты акустической (речевой) информации разделяются на пассивные и активные. Основным пассивным методом защиты акустической (речевой) информации является звукоизоляция. Когда пассивные методы защиты не могут обеспечить необходимый уровень безопасности, применяют активные методы защиты, в частности, зашумление. Для защиты помещений применяют генераторы шума и системы вибрационного зашумления. Заблуждения о подавителях диктофонов. Характеристики прибора и на что обратить внимание в первую очередь? Принцип работы. Условия эксплуатации.		
8.	**Тема** Краткая классификация закладочных устройств. Спецобследование помещений Пять признаков классификации: - по каналу передачи информации; - по способу восприятия информации; - по наличию устройства управления; - по внешнему виду; - по используемому источнику питания. Процедуру спецобследования помещения можно условно разделить на следующие этапы: - подготовительный этап: - инструментальный контроль: - анализ выявленных демаскирующих признаков; - подготовка отчетной документации.	3	Мультимедиа лекция
9.	**Тема** Защита информации по каналу низкочастотного акустоэлектрического преобразования. Взаимное расположение элементов устройства под воздействием звукового сигнала может изменяться. Возможность подобных преобразований получила название - микрофонный эффект. Классификация акустоэлектрических преобразователей по физическим процессам, создающим опасные сигналы. По способам формирования электрического сигнала активные акустоэлектрические преобразователи могут быть электродинамическими, электромагнитными и пьезоэлектрическими. Добывание информации путем высокочастотного навязывания Принцип явления, пример реализации. Способы защиты.	3	Мультимедиа лекция
	Итого за 5 семестр	**27**	**15**
	6 семестр		
10.	**Тема** Побочные электромагнитные излучения СВТ. Средства перехвата радиосигналов. Общая характеристика технических каналов утечки	1,5	

	информации, обрабатываемой средствами вычислительной техники. Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники. Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники: – вывод информации на экран монитора; – ввод данных с клавиатуры; – запись информации на накопители; – чтение информации с накопителей; – передача данных в каналы связи; – вывод данных на периферийные печатные устройства (принтеры, плоттеры); – запись данных от сканера на магнитный носитель и т.д. Упрощенная схема типового комплекса для перехвата радиосигналов. К средствам радио- и радиотехнической разведки относятся: · портативные сканирующие приемники, различного вида цифровые анализаторы спектра, селективные микровольтметры, радиотестеры и комплексы для измерения параметров приемопередающих устройств и т.п.; · специальные средства для контроля радиотелефонов и сотовой связи; · программно-аппаратные комплексы, построенные на базе сканерных приемников; · портативные радиопеленгаторы и т.п.		
11.	**Тема** Пассивные методы защиты. Заземление. Фильтрация опасных сигналов. Перехват электромагнитного, магнитного, электрического полей, а также электрических сигналов с информацией называется радио- и радиотехнической разведкой. К основным этапам перехвата можно отнести следующее: • обнаружение сигналов в пространстве, представляющих ценность для злоумышленника; • усиление сигналов; • анализ технических характеристик принимаемых сигналов и съем информации; • определение расположения источников сигналов. Защитное действие заземления основано на двух принципах: • уменьшение до безопасного значения разности потенциалов между заземляемым проводящим предметом и другими проводящими предметами, имеющими естественное заземление. • отвод тока утечки при контакте заземляемого проводящего предмета с фазным проводом.	1,5	

	Схемы заземлений: одноточечные, многоточечные и комбинированные. Фильтрация опасных сигналов. Примеры устройств.		
12.	**Тема** Активные методы защиты. Зашумление. Защита информации от утечки через ПЭМИН осуществляется с применением пассивных и активных методов и средств. Активные методы защиты, основаны на создании помех для технических средств злоумышленника с целью уменьшения отношения сигнал/шум на входе его приемной аппаратуры. Примеры генераторов шума.	1,5	
13.	**Тема** Индикаторы электромагнитных излучений. Радиочастотомеры. Сканирующие приемники. Структурная схема индикатора электромагнитных излучений. Классификация индикаторов электромагнитного поля. Примеры и функциональные возможности современных приборов. Сканирующие приемники делятся на перевозимые и переносимые и имеют три режима работы "Методы защиты информации от утечки через ПЭМИН". Алгоритмы сканирования, основные: • сканирование прекращается, если уровень принимаемого сигнала превышает заданный порог. Происходит звуковое или световое оповещение оператора. Возобновление сканирование осуществляется только по его команде; • сканирование прекращается при обнаружении сигнала и возобновляется после его пропадания; • сканирование прекращается при анализе сигнала оператором и продолжается через некоторое время; • ручное сканирование. Пример приборов, основные возможности.	1,5	
14.	**Тема** Автоматизированные поисковые комплексы. Комплект сканирующий приемник+ПЭВМ (со специальным программным обеспечением) является простейшим примером автоматизированного поискового комплекса (далее АПК). Более сложные системы построены также на базе ПЭВМ и сканирующего приемника, но имеют дополнительные блоки, повышающие быстродействие и расширяющие функциональные возможности комплекса. Пример приборов, основные возможности.	1,5	

15.	**Тема Паразитные связи и наводки.** Основными видами паразитных связей в схемах электромагнитных устройств являются емкостные, индуктивные, электромагнитные, электромеханические связи и связи через источники питания и заземления радиоэлектронных средств.	4,5	
	Итого за 6 семестр	**12**	
	Итого	**39**	**15**

7.3 Наименование лабораторных работ

№ Темы	Наименование работы	Объем часов	Форма проведения
	5 семестр		
4	Лабораторная работа №1. **Тема: «Обнаружение скрытых видеокамер с помощью поискового прибора «Оптик»».** Изучение методики поиска объектива скрытой видеокамеры	1,5	Компьютерные симуляции
6	Лабораторная работа №2 **Тема: «Качественная оценка утечки речевой информации по акустическим каналам с помощью многофункционального поискового прибора «Спайдер»»** Отработка навыков проведения исследований по выявлению акустических каналов утечки речевой информации.	1,5	
6	Лабораторная работа №3 Тема: **«Качественная оценка утечки речевой информации по виброакустическим каналам с помощью многофункционального поискового прибора «Спайдер»»** Отработка навыков проведения измерений по выявлению виброакустических каналов утечки речевой информации.	1,5	
6	Лабораторная работа №4 Тема: **«Количественная оценка защищенности речевой информации по акустическому каналу через двери с использованием ПАК «Шёпот»»** Отработка навыков проведения измерений по выявлению виброакустических каналов утечки речевой информации с использованием системы оценки защищенности выделенных помещений по виброакустическому каналу «Шепот»	1,5	
6	Лабораторная работа № 5 **Тема: «Количественная оценка защищенности речевой информации по акустическому каналу через окна с использованием ПАК «Шёпот»»** Отработка навыков проведения измерений по выявлению	1,5	Компьютерные симуляции

	виброакустических каналов утечки речевой информации с использованием системы оценки защищенности выделенных помещений по виброакустиче-скому каналу ПАК «Шепот»		
7	Лабораторная работа №6 **«Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования. Оценка защищенности речевой информации по телефонной линии».** Отработка навыков проведения измерений по выявлению каналов утечки речевой информации, обусловленной низкочастотными акустоэлектрическими преобразованиями (НЧ АЭП) и ее защита.	1,5	
8	Лабораторная работа № 7 **Тема: «Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования. Оценка защищенности речевой информации по шлейфу пожарной сигнализации»** Отработка навыков проведения измерений по выявлению каналов утечки речевой информации, обусловленной низкочастотными акустоэлектрическими преобразованиями (НЧ АЭП) и ее защита.	1,5	Компьютерные симуляции
8	Лабораторная работа № 8 **Тема: «Поиск и выявление инфракрасного канала утечки информации, с помощью многофункционального поискового прибора «Спайдер» и имитатора сигналов «ИМФ-3»»** Изучение канала утечки информации, создаваемого за счет применения специальных технических средств с передачей перехваченной информации в инфракрасном диапазоне.	1,5	Компьютерные симуляции
8	Лабораторная работа № 9. **Тема: «Анализ имитаторов закладок на наличие электронных компонентов с помощью импульсного нелинейного локатора «ЛОРНЕТ-36»»** Изучить методику работы нелинейного локатора «ЛОРНЕТ-36», приобрести навыки работы по выявлению искусственных p-n переходов	1,5	Компьютерные симуляции
	Итого 5 семестр	**13,5**	**7,5**
	6 семестр		
10	Лабораторная работа № 10 **Тема: «Поиск и выявление радиопередающих устройств, прослушивание их несущей частоты, с помощью многофункционального поискового прибора «Спайдер» и имитатора сигналов «ИМФ-3»»** Изучить методику выявления канала утечки закладных радиопередающих устройств различных типов.	1,5	Компьютерные симуляции
10	Лабораторная работа № 11 **Тема: «Изучение радиоэлектронной обстановки с запоминанием частот сигнала»** Выявление самой низкой частоты с помощью метода	1,5	Компьютерные симуляции

	автоисключения		
11	Лабораторная работа № 12 **Тема: «Подавление канала приема сигнала обнаруженной частоты путем постановки на его частоте прицельной помехи»** Исследовать особенности работы «Скорпиона» при постановки прицельной помехи на симплексную связь.	1,5	Компьютерные симуляции
12	Лабораторная работа № 13 **Тема: «Проведение специальных исследований по каналу ПЭМИН электронно-лучевого монитора (VGA интерфейса) с использованием ПАК «Сигурд»»** Ознакомление с параметрами ПЭМИН VGA интерфейса и его исследование при помощи САИС «Сигурд».	1,5	Компьютерные симуляции
12	Лабораторная работа № 14 **Тема: «Исследование клавиатуры с интерфейсом PS с использованием САИС «Сигурд»»** Ознакомление с параметрами ПЭМИН интерфейса PS/2 и его исследование при помощи САИС «Сигурд	1,5	Компьютерные симуляции
12	Лабораторная работа № 15 **Тема: «Оценка защищенности объектов информатизации от утечки информации по каналам ПЭМИН с использованием САИС «Сигурд»»** Изучить методику проведения аттестационных испытаний и оценки эффективности принятых мер защиты информации от утечки по каналу ПЭМИН	4,5	
	Итого 6 семестр	**12**	**7,5**
	Итого	**25,5**	**15**

7.4 Наименование практических занятий

№ Темы	**Наименование работы**	**Объем часов**	**Форма проведения**
	6 семестр		
10	Практическое занятие №1. **Тема: «Разработка пространственной модели объекта информационной защиты. Описание угроз утечки информации по техническим каналам».**	1,5	групповое решение задач
11	Практическое занятие №2 **Тема: «Разработка системы виброакустической защиты»**	1,5	групповое решение задач
12	Практическое занятие №3 Тема: **«Разработка системы защиты от утечек за счет побочных электромагнитных излучений и наводок»**	1,5	групповое решение задач

13	Практическое занятие №4 Тема: **«Разработка системы защиты технических средств связи от утечек за счет электроакустических преобразований»**	1,5	групповое решение задач
14	Практическое занятие № 5 **Тема: «Расчет максимально возможного количества элементов комплекса ТСЗИ, подключаемых к блоку питания и управления, подбор кабеля»**	1,5	групповое решение задач
15	Практическое занятие №6 **«Обеспечение оперативного контроля исправности, режима работы и контроля состава комплекса»**	4,5	
	Итого 6 семестр	**12**	**7,5**
	Итого	**12**	**7,5**

7.5 Технологическая карта самостоятельной работы обучающегося

Технологическая карта

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
5 семестр						
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13	Изучение литературы по темам1-9	Конспект	▪ собеседование	69,255	7,695	76,95
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13	Подготовка к лекциям	Конспект	▪ собеседование	2,43	0,27	2,7
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13	подготовка к лабораторным работам	Отчет	▪ отчет письменный	1,215	0,135	1,35
			Итого за 5 семестр	**72,9**	**8,1**	**81**
6 семестр						
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13	Изучение литературы по темам10-17	Конспект	▪ собеседование	93,96	10,44	104,4
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13	Подготовка к лекциям	Конспект	▪ собеседование	1,08	0,12	1,2
ПК-1, ПК-4,	подготовка к практической	Отчет	▪ отчет письмен	2,16	0,24	2,4

ПК-5, ПК-12, ПК-13	и лабораторной работе		ный			
Итого за 6 семестр				**97,2**	**10,8**	**108**
Итого				**170,1**	**18,9**	**189**

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Фонд оценочных средств, позволяющий оценить уровень сформированности компетенций, размещен в УМК дисциплины «Техническая защита информации» на кафедре системы управления, информационные технологии и представлен следующими компонентами:

Код оцениваемой компетенции	**Этап формирования компетенции (№ темы)**	**Средства и технологии оценки**	**Тип контроля (текущий/ промежуточный)**	**Вид контроля (текущий/промежуточный)**	**Наименование оценочного средства**
5 семестр					
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	4, 6, 7, 8, 9	Отчёт письменный	текущий	письменный	Темы индивидуальных заданий для лабораторных занятий
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	1-9	собеседование	текущий	устный	Вопросы для собеседования
		Собеседо-вание	промежуточный	устный	Вопросы к экзамену
					Вопросы для проверки уровня знаний
					Вопросы (задания) для проверки умений и навыков
6 семестр					

ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	10-15	Отчёт письменный	текущий	письменный	Темы индивидуальных заданий для лабораторных занятий
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	10-15	Отчёт письменный	текущий	письменный	Темы индивидуальных заданий для практических занятий
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	10-15	собеседование	текущий	устный	Вопросы для собеседования
ПК-1, ПК-4, ПК-5, ПК-12, ПК-13, ОПК-7	1-15	Курсовая работа	промежу-точный	письменный	Оценочные средства для курсового проекта
		Собеседо-вание	промежуточный	устный	Вопросы к экзамену
					Вопросы для проверки уровня знаний
					Вопросы (задания) для проверки умений и навыков

8.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Уровни сформированности компетенций	**Индикаторы**	**Дескрипторы**			
		2 балла	**3 балла**	**4 балла**	**5 баллов**
(для каждой компетенци	**ПК-1**				

и)					
Базовый	**Знать:** работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Отсутствуют знания работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Частичные знания работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Имеются знания работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
	Уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Отсутствие умения выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Частично умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
	Владеть: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Не владеет способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Частично владеет способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Владеет способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
	ПК-4				
	Знать: работу по реализации политики информационной безопасности, применять комплексный подход к	Отсутствуют знания работы по реализации политики информационной безопасности, применять комплексный подход к	Частичные знания работы по реализации политики информационной безопасности, применять комплексный подход к	Имеются знания работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению	

	обеспечению информационной безопасности объекта защиты	обеспечению информационной безопасности объекта защиты	обеспечению информационной безопасности объекта защиты	информационной безопасности объекта защиты	
	Уметь: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Отсутствие умения участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Частично умеет участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Умеет участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Владеть: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Не владеет способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Частично владеет способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Владеет способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	ПК-5				
	Знать: организацию и сопровождение аттестации объекта информатизации по требованиям безопасности информации	Отсутствуют знания организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	Частичные знания организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	Имеются знания организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации	
	Уметь:	Отсутствие умения	Частично умеет	Умеет принимать участие в	

	принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
	Владеть: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Не владеет способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Частично владеет способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Владеет способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
	ПК-12				
	Знать: экспериментальные исследования системы защиты информации	Отсутствуют знания экспериментальные исследования системы защиты информации	Частичные знания экспериментальные исследования системы защиты информации	Имеются знания экспериментальные исследования системы защиты информации	
	Уметь: принимать участие в проведении экспериментальных исследований системы защиты информации	Отсутствие умения принимать участие в проведении экспериментальных исследований системы защиты информации	Частично умеет принимать участие в проведении экспериментальных исследований системы защиты информации	Умеет принимать участие в проведении экспериментальных исследований системы защиты информации	
	Владеть: способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Не владеет способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Частично владеет способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Владеет способностью принимать участие в проведении экспериментальных исследований системы защиты информации	
	ПК-13				

	Знать: участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Отсутствуют знания участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Частичные знания участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Имеются знания участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Уметь: принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Отсутствие умения принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Частично умеет принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Умеет принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Владеть: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	Не владеет способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	Частично владеет способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	Владеет способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	
	ОПК-7				
	Знать: информационные ресурсы, подлежащие	Отсутствуют знания информационные ресурсы, подлежащие	Частичные знания информационные ресурсы, подлежащие	Имеются знания информационные ресурсы, подлежащие защите, угрозы	

	защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Уметь: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Отсутствие умения определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Частично умеет определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Умеет определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Владеть: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.	Не владеет способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.	Частично владеет способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.	Владеет способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.	

Повышенный	ПК-1				
	Знать: работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				Знает работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	Уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				Показывает умение выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	Владеть: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				Владеет способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	ПК -4				
	Знать: работу по реализации политики информационной безопасности, применять комплексный подход к				Знает работу по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационн

	обеспечению информационной безопасности объекта защиты				ой безопасности объекта защиты
	Уметь: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты				Показывает умение участвовать в работах по реализации политики информационн ой безопасности, применять комплексный подход к обеспечению информационн ой безопасности объекта защиты
	Владеть: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты				Владеет способностью участвовать в работах по реализации политики информационн ой безопасности, применять комплексный подход к обеспечению информационн ой безопасности объекта защиты
	ПК-5				
	Знать: организацию и сопровождение аттестации объекта информатизации по требованиям безопасности информации				Знает организацию и сопровождение аттестации объекта информатизаци и по требованиям безопасности информации
	Уметь: принимать участие в организации и сопровождении аттестации объекта				Показывает умение принимать участие в организации и сопровождении аттестации объекта

	информатизации по требованиям безопасности информации				информатизации по требованиям безопасности информации
	Владеть: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				Владеет способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
	ПК-12				
	Знать: экспериментальные исследования системы защиты информации				Знает экспериментальные исследования системы защиты информации
	Уметь: принимать участие в проведении экспериментальных исследований системы защиты информации				Показывает умение принимать участие в проведении экспериментальных исследований системы защиты информации
	Владеть: способностью принимать участие в проведении экспериментальных исследований системы защиты информации				Владеет способностью принимать участие в проведении экспериментальных исследований системы защиты информации
	ПК-13				
	Знать: участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению				Знает участие в формировании, организовывать и поддерживать выполнение комплекса мер по

	информационной безопасности, управлять процессом их реализации				обеспечению информационной безопасности, управлять процессом их реализации	
	Уметь: принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				Показывает умение принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Владеть: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.				Владеет способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.	
	ОПК-7					
	Знать: информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей				Знает информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей	

	функционирования объекта защиты				функционирования объекта защиты	
	Уметь: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				Показывает умение определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Владеть: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.				Владеет способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.	

В рамках рейтинговой системы успеваемость студентов по дисциплине оцениваются знания, умения навыки в ходе текущего контроля и промежуточной аттестации.

Текущий контроль
Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
	5 семестр		
1.	Выполнение лабораторных работ 1-3	6 неделя	25

2.	Выполнение лабораторных работ 4-9	14 неделя	30
	Итого за 5 семестр		**55**
	6 семестр		
3.	Выполнение лабораторных работ 10-12	6 неделя	25
4.	Выполнение практических занятий 1-6	12 неделя	30
	Итого за 6 семестр		**55**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Промежуточная аттестация в форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. В случае если рейтинговый балл студента по дисциплине по итогам семестра равен 60, то программой автоматически добавляется 32 премиальных балла и выставляется оценка «отлично». Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**$20 \leq S_{экз} \leq 40$**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

Итоговая оценка по дисциплине, изучаемой в семестре, определяется по сумме баллов, набранных за работу в течение семестра, и баллов, полученных при сдаче экзамена:

Шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	***Оценка по 5-балльной системе***
88 – 100	*Отлично*
72 – 87	*Хорошо*
53 – 71	*Удовлетворительно*
<53	*Неудовлетворительно*

Промежуточная аттестация в форме **курсовой работы.** Максимальная сумма балов по **курсовой работе** устанавливается в **100** балов и переводится в оценку по 5-бальной системе в соответствии со шкалой:

Шкала соответствия рейтингового балла 5-бальной системе

Рейтинговый балл	Оценка по 5-балльной системе
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
<53	*Неудовлетворительно*

8.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этап формирования компетенций

Вопросы к экзамену (5 семестр)
Вопросы для проверки уровня обученности:

Знать:

1. Нормативно - правовые основы информационной безопасности в РФ.
2. Основные понятия в области технической защиты информации.
3. Структура технического канала утечки информации.
4. Типы носителей информации в технических каналах связи.
5. Классификация технических каналов утечки информации.
6. Понятие информационного сигнала. Модуляция сигналов.
7. Опасные сигналы и их источники.
8. Основные показатели технического канала утечки информации.
9. Основные понятия в области акустики.
10. Классификация акустических каналов утечки информации.
11. Критерии оценки эффективности защиты акустической (речевой) информации.
12. Физические основы возникновения ТК АЭП в ВТСС.
13. Порядок проведения специальных исследований ВТСС на утечку по каналу АЭП.
14. Общий порядок проведения измерений по каналу АЭП.
15. Средства пассивной защиты информации по каналу АЭП.
16. Средства активной защиты информации по каналу АЭП.

Уметь, владеть:

1. Методика проведения специальных исследований в области акустики и виброакустики.
2. Средства акустической разведки.
3. Методы и средства пассивной защиты акустической речевой информации.
4. Методы и средства активной защиты акустической речевой информации.
5. Подавление диктофонов.
6. Перехват побочных электромагнитных излучений ТСПИ средствами разведки ПЭМИН.
7. Паразитные связи и наводки.
8. Средства перехвата радиосигналов.
9. Пассивные и активные методы защиты.

Вопросы к экзамену (6 семестр)

Вопросы для проверки уровня обученности:

Знать:

1. Структура технического канала утечки информации за счет ПЭМИН.
2. Заземление.
3. Фильтрация опасных сигналов.

4. Зашумление.
5. Низкочастотные и высокочастотные излучения технических средств.
6. Паразитные связи и наводки.
7. Средства перехвата радиосигналов.
8. Пассивные и активные методы защиты.
9. Индикаторы электромагнитных излучений. Радиочастотометры.
10. Сканирующие приемники.
11. Автоматизированные поисковые комплексы.
12. Оценка защищенности помещений от утечки речевой информации по акустическому и виброакустическому каналам и по каналу электроакустических преобразований.
13. Оценка защищенности информации от утечки за счет ПЭМИН.

Уметь, владеть:

1. Индикаторы электромагнитных излучений.
2. Радиочастотометры.
3. Сканирующие приемники.
4. Автоматизированные поисковые комплексы.
5. Досмотровая техника.
6. Специальные проверки технических средств и систем.
7. Методы оценки опасности угроз.
8. Способностью проводить эксперименты по заданной методике.
9. Способностью проводить обработку результатов, оценку погрешности и достоверности результатов.
10. Способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.

Тематика курсовых работ

1. Инженерно-техническая защита выделенного помещения №1.
2. Инженерно-техническая защита выделенного помещения №2.
3. Инженерно-техническая защита выделенного помещения №3.
4. Инженерно-техническая защита выделенного помещения №4.
5. Инженерно-техническая защита выделенного помещения №5.
6. Инженерно-техническая защита выделенного помещения №6.
7. Инженерно-техническая защита выделенного помещения №7.
8. Инженерно-техническая защита выделенного помещения №8.
9. Инженерно-техническая защита выделенного помещения №9.
10. Инженерно-техническая защита выделенного помещения №10.
11. Инженерно-техническая защита выделенного помещения №11.
12. Инженерно-техническая защита выделенного помещения №12.
13. Инженерно-техническая защита выделенного помещения №13.
14. Инженерно-техническая защита выделенного помещения №14.
15. Инженерно-техническая защита выделенного помещения №15.
16. Инженерно-техническая защита выделенного помещения №16.
17. Инженерно-техническая защита выделенного помещения №17.
18. Инженерно-техническая защита выделенного помещения №18.
19. Инженерно-техническая защита выделенного помещения №19.
20. Инженерно-техническая защита выделенного помещения №20.
21.

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Процедура проведения экзамена осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ. В экзаменационный билет включаются 2 теоретических вопроса. Для подготовки по билету отводится 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются последовательность, рациональность выполнения, точность расчетов, правильность выполнения чертежей и рисунков.

Для выполнения курсовой работы по дисциплине необходимо получить индивидуальное задание, ознакомиться с исходными данными, изучить основную литературу. При проверке задания оцениваются понимание студента темы и содержание работы.

При защите курсовой работы оцениваются: практическая и научная значимость работы, оценка работы рецензентом и ответы на вопросы, а также учитывается качество оформления проекта (пояснительная записка и приложения, если они есть).

Текущая аттестация студентов проводится преподавателями, ведущими лабораторные по дисциплине, в следующих формах: отчет письменный, собеседование, курсовая работа.

Допуск к защите отчетов по лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. Максимальное количество баллов студент получает, если оформление отчета соответсвует установленным требованиям, а отчет полностью раскрывает суть работы. Основанием для снижением оценки являются:

- частично не соовествует установленным требованиям;
- в отчете непольностью раскрывается суть работы.

Отчет может быть отправлен на доработку в следующих случаях:

- полностью не соовествует установленным требованиям;
- не раскрыта суть работы.

Процедура проведения собеседования проводится в следующей форме: студенту выдается вопрос для собеседования, он готовит ответ (в письменной или устной форме) и отчитывается преподавателю по заданному вопросу. При подготовке к ответу студенту предоставляется право пользования справочными материалами. При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- точность вычислений;
- знание технологий, использованных при выполнении задания.

Критерии оценивания ответов на вопросы собеседования, отчёта, курсовой работы приведены в Фонде оценочных средств по дисциплине «Техническая защита информации».

9 Методические указания для обучающихся по освоению дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с практическими занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
1.	изучение литературы по темам 1-15	1,2	1,2	1-4	1-2
2.	проработка лекционного материала	1,2	1,2	1-4	1-2
3.	подготовка к лабораторным и практическим работам	1,2	1,2	1-4	1-2
4.	Выполнение курсовой работы	1,2	1,2	1-4	1-2

11. Учебно-методическое и информационное обеспечение дисциплины

10.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.

10.1.1. Перечень основной литературы:

1. Технические средства и методы защиты информации: учеб.пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва: Горячая линия-Телеком, 2016. – 616 с.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. М.: НПЦ «Аналитика», 2017.

10.1.2. Перечень дополнительной литературы:

1. Разработка системы технической защиты информации: учебное пособие [Электронный ресурс]/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стер. – М.: Флинта, 2014. – URL:http://biblioclub.ru/index.php?page=book&id=93349

2. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие/ А. Ф. Чипига- М.: Гелиос АРВ, 2013.

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине:

1. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине Техническая защита информации.
2. Методические указания по выполнению лабораторных работ по дисциплине Техническая защита информации.
3. Методические указания по выполнению практических занятий по дисциплине Техническая защита информации.
4. Методические указания по выполнению курсовой работы по дисциплине Техническая защита информации.

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

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.

4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

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

Информационные технологии:

- Персональные компьютеры, объединенные в локальную сеть и имеющие выход в Интернет;
- Мультимедиа лекции

Информационные справочные системы:

- www.consultant.ru
- www.garant.ru

Перечень программного обеспечения и информационно-справочных систем:

Базовый пакет программ Microsoft Office Standard 2013. Бессрочная лицензия. Дата окончания срока поддержки (обновления) 11.04.2023г., Microsoft Windows Профессиональная. Бессрочная лицензия.

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

1. Учебная аудитория для проведения занятий лекционного типа: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер преподавателя, проектор , доска магнитно-маркерная

Подключение к сети «Интернет», выход в корпоративную сеть университета

2. Учебная аудитория для проведения занятий семинарского типа (практических работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер, проектор, доска магнитно-маркерная

Подключение к сети «Интернет», выход в корпоративную сеть университета

3. Учебная аудитория для проведения занятий семинарского типа (лабораторных работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер, проектор, доска магнитно-маркерная

Подключение к сети «Интернет», выход в корпоративную сеть университета

4. Учебная аудитория для групповых и индивидуальных консультаций: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: проектор, экран настенный, саб, персональный компьютер

5. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: проектор, экран настенный, саб, персональный компьютер.

6. Учебная аудитория для выполнения курсовых проектов: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер, проектор, доска магнитно-маркерная

Подключение к сети «Интернет», выход в корпоративную сеть университета