

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Грובה Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова
Дата подписания: 17.06.2026 15:38:47
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего
образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
Т.А. Грובה
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Защита информации от утечки по техническим каналам
название дисциплины (модуля)

Направление подготовки	10.03.01 «Информационная безопасность»
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	6

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Защита информации от утечки по техническим каналам студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

2. ФОС является приложением к программе дисциплины (модуля) «Защита информации от утечки по техническим каналам в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик (и) Рачков В.Е., доцент кафедры

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Петренко В.И., заведующий кафедрой

Члены комиссии: Жук А.П., профессор кафедры

Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «СГУ-Инфоком»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Защита информации от утечки по техническим каналам».

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция: ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</i>				
Результаты обучения по дисциплине (модулю): <i>Индикатор: ИД-2 Эффективно применяет знания теории и методики курса при раскрытии компьютерных преступлений, при работе с конфиденциальной информацией и государственной тайной, при работе с организационно-правовым обеспечением, при работе с ЭП, при защите авторского права, при проведении экспертизы преступлений в сфере компьютерной информации; применять нормативно-правовые акты при защите информации; оценивать состояние организационной защиты информации на объекте.</i>	-фрагментарно осуществляет организацию защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -выбирает без должной аргументации мероприятия защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -не участвует в организации защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	-фрагментарно осуществляет организацию защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -выбирает без должной аргументации мероприятия защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -участвует в организации защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации,	-осуществляет организацию защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -выбирает мероприятия защиты информации ограниченного доступа в целом выбирает мероприятия защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -частично участвует в организации	- осуществляет организацию защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -выбирает мероприятия защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

		Федеральной службы по техническому и экспортному контролю;	защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	-участвует в организации защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ИД-3 _{ОПК-6} Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Не способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Плохо способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Хорошо способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

				му и экспортному контролю.
Компетенция: ОПК-9 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-1 Понимает базовые принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	- с трудом оперирует знаниями средств криптографической и технической защиты информации по техническим каналам; - слабо оценивает средства криптографической и технической защиты информации по техническим каналам; - фрагментарно анализирует средства криптографической и технической защиты информации по техническим каналам;	- в основном оперирует знаниями средств криптографической и технической защиты информации по техническим каналам; - слабо оценивает средства криптографической и технической защиты информации по техническим каналам; - фрагментарно анализирует средства криптографической и технической защиты информации по техническим каналам;	- в целом оперирует знаниями средств криптографической и технической защиты информации по техническим каналам; - фрагментарно оценивает средства криптографической и технической защиты информации по техническим каналам; - анализирует средства криптографической и технической защиты информации по техническим каналам;	- оперирует знаниями средств криптографической и технической защиты информации по техническим каналам; - оценивает средства криптографической и технической защиты информации по техническим каналам; - анализирует средства криптографической и технической защиты информации по техническим каналам;
Результаты обучения по дисциплине (модулю): Индикатор: ИД-2 Использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	- слабо осуществляет выбор средств криптографической и технической защиты информации для решения задач профессиональной деятельности; - фрагментарно выделяет средства криптографической и технической защиты информации для решения задач профессиональной деятельности; - с трудом использует средства криптографической и	- в целом осуществляет выбор средств криптографической и технической защиты информации для решения задач профессиональной деятельности; - фрагментарно выделяет средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	- в целом осуществляет выбор средств криптографической и технической защиты информации для решения задач профессиональной деятельности; - фрагментарно выделяет средства	- осуществляет выбор средств криптографической и технической защиты информации для решения задач профессиональной деятельности; - выделяет средства

	технической защиты информации для решения задач профессиональной деятельности.	- с трудом использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	криптографической и технической защиты информации для решения задач профессиональной деятельности; - использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	криптографической и технической защиты информации для решения задач профессиональной деятельности; - использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.
Результаты обучения по дисциплине (модулю): <i>Индикатор: ИД-3 Выбирает оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности</i>	- не выделяет оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	- с трудом выделяет оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	- в основном выделяет оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	- выделяет оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения ОФО семестр 5	
1.		Государственная система защиты информации. Основные направления защиты информации.	ОПК-6
2.		Цели и задачи защиты информации от утечки информации по техническим каналам.	ОПК-6
3.		Объекты технической защиты информации.	ОПК-6
4.		Нормативные документы по технической защите информации.	ОПК-6
5.		Объект информатизации (определение и характеристика).	ОПК-6
6.		Характеристика основных технических средств и систем (ОТСС).	ОПК-6
7.		Характеристика вспомогательных технических средств и систем (ВТСС).	ОПК-6

8.		Структура и состав технического канала утечки информации.	ОПК-6
9.		Классификация технических каналов утечки информации.	ОПК-6
10.		Основные показатели технических каналов утечки информации.	ОПК-6
11.		Концепция технической защиты информации.	ОПК-6

12.		Общие принципы технической защиты информации.	ОПК-6
13.		Принципы построения системы защиты информации.	ОПК-6
14.		Классификация направлений и методов защиты.	ОПК-6
15.		Характеристика методов скрытия информации.	ОПК-6
16.		Понятия информации.	ОПК-6
17.		Свойства информации, как предмета технической защиты.	ОПК-6
18.		Характеристика информационных технологий как предмет защиты.	ОПК-6
19.		Характеристика информационных процессов в автоматизированных информационных системах.	ОПК-6
20.		Структура и схема информационного процесса передачи информации.	ОПК-6
21.		Виды информации в автоматизированных информационных системах.	ОПК-6
22.		Машинное представление информации.	ОПК-6
23.		Физическое представление информации в автоматизированных информационных системах.	ОПК-6
24.		Виды сообщений в информационно-телекоммуникационных системах.	ОПК-6

25.		Классификация сигналов.	ОПК-6
26.		Сравнительная характеристика аналоговых и дискретных сигналов.	ОПК-6
27.		Временное и спектральное представление сигналов.	ОПК-6
28.		Принципы записи информации на носители в виде физических полей.	ОПК-6
29.		Виды модуляции. Характеристика аналоговых видов модуляции.	ОПК-6
30.		Виды модуляции. Характеристика импульсных видов модуляции (манипуляции).	ОПК-6
31.		Принципы передачи и считывания информации с носителей в виде физических полей.	ОПК-6
32.		Особенности современных автоматизированных информационных системах как объектов защиты.	ОПК-6
33.		Уязвимость основных структурно-функциональных элементов распределенных АИС	ОПК-6
34.		Определения угроз безопасности информации АИС и субъектов информационных отношений.	ОПК-6
35.		Источники угроз безопасности АИС, их классификация.	ОПК-6
36.		Основные непреднамеренные искусственные угрозы АИС.	ОПК-6
37.		1. Основные преднамеренные искусственные угрозы АИС.	ОПК-6
38.		2. Доступ к информации, условия разведывательного контакта.	ОПК-6
39.		Способы и каналы несанкционированного доступа к информации	ОПК-6

40.		Опасные случайные сигналы и их источники.	ОПК-6
41.		Классификация акустоэлектрических преобразователей	ОПК-6
42.		Акустоэлектрические преобразователи как источники опасных сигналов.	ОПК-6
43.		Паразитные связи и наводки как источники опасных сигналов.	ОПК-6
44.		Низкочастотные и высокочастотные излучения технических средств.	ОПК-6
45.		Классификация и характеристика видов технической разведки	ОПК-6
46.		Классификация и характеристика технических средств разведки.	ОПК-6
47.		Возможности (показатели) технической разведки и ее средств.	ОПК-6
48.		Общая характеристика радиоэлектронных технических каналов утечки информации.	ОПК-6
49.		Классификация радиоэлектронных технических каналов утечки информации.	ОПК-6
50.		Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений.	ОПК-6
51.		Структура и характеристика электромагнитного технического канала утечки информации.	ОПК-6
52.		Характеристика сигналов ПЭМИ от средств вычислительной техники.	ОПК-6
53.		Условия возникновения электромагнитного канала утечки информации. Характеристика опасной зоной 2 (R2).	ОПК-6
54.		Перехват побочных электромагнитных излучений СВТ средствами разведки ПЭМИН.	ОПК-6

		Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений.	
55.		Структура и характеристика электрического технического канала утечки информации.	ОПК-6
56.		Условия возникновения электрического канала утечки информации. Характеристика опасных зон 1 (r1).	ОПК-6
57.		Перехват наведенных информационных сигналов средствами разведки ПЭМИН.	ОПК-6
58.		Технический канал утечки информации, создаваемый путем высокочастотного облучения ТСПИ.	ОПК-6
59.		Классификация аппаратных закладок, внедряемых в средства вычислительной техники.	ОПК-6
60.		Технический канал утечки информации, создаваемый путем внедрения в ТСПИ электронных устройств негласного получения информации.	ОПК-6
61.		Характеристика электронных устройств перехвата информации, внедряемых в средства вычислительной техники.	ОПК-6
62.		Аппаратные кейлоггеры.	ОПК-6
63.		Способы перехвата информации, обрабатываемой ТСПИ.	ОПК-6
64.		Общая характеристика речевого сигнала. Линейные характеристики акустического поля.	ОПК-6
65.		Общая характеристика речевого сигнала. Энергетические характеристики акустического поля.	ОПК-6

66.		Общая характеристика речевого сигнала. Фонетические характеристики речи.	ОПК-6
67.		Выделенные помещения.	ОПК-6
68.		Классификация способов перехвата акустической (речевой) информации.	ОПК-6
69.		Схема и характеристика прямого акустического канала перехвата речевой информации.	ОПК-6
70.		Схемы каналов перехвата речевой информации с использованием микрофонов и диктофонов.	ОПК-6
71.		Схемы каналов перехвата речевой информации с использованием закладных устройств передачи информации по каналам связи.	ОПК-6
72.		Схема перехвата речевой информации с использованием устройств типа «телефонное ухо» с передачей информации по телефонной линии на низкой частоте.	ОПК-6
73.		Принципы построения акустических закладок.	ОПК-6
74.		Эндовибраторы.	ОПК-6
75.		Акустовибрационные технические каналы утечки информации.	ОПК-6
76.		Схемы каналов перехвата речевой информации с использованием стетоскопов.	ОПК-6
77.		Акустооптические (лазерные) технические каналы утечки информации.	ОПК-6
78.		Принцип действия лазерной акустической системы разведки.	ОПК-6

79.		Акустоэлектрический (параметрический) технический канал утечки информации	ОПК-6
80.			ОПК-6
81.	a	Выберите один или несколько ответов: Технические каналы утечки информации являются техническими системами: a) с пространственно распределенными структурными элементами; b) с временно распределенными структурными элементами; c) с пространственно сосредоточенными структурными элементами; d) с временно сосредоточенными структурными элементами	ОПК-6
82.	a	Выберите один или несколько ответов: В составных технических каналах утечки информации преобразование одного носителя сигнала в другой осуществляется за счет: a) физических эффектов–преобразователей энергии; b) физических эффектов-проводников; c) физических явлений электромагнитной природы; d) физических эффектов-модификаторов; e) физических эффектов–преобразователей объектов	ОПК-6
83.	b	Выберите один или несколько ответов: К составным каналам утечки информации из перечисленных относятся: a) акустический канал; b) акустоэлектрический канал; c) электрический канал по цепям электропитания; d) электрический канал по цепям заземления; e) канал утечки за счет побочных электромагнитных излучений	ОПК-6
84.	c	Выберите один или несколько ответов: Составной технический канал утечки информации помимо элементов,	ОПК-6

		присущих простому каналу утечки информации, содержит: a) источник (генератор) сигнала; b) источник (генератор) помех; c) преобразователь одного вида сигнала в другой; d) приемник сигнала.	
85.	a	Выберите один или несколько ответов: Принцип обнаружения закладных устройств при помощи индикатора поля основан: a) на выявлении факта превышения уровня электромагнитного поля в точке приема; b) на прослушивании сигналов радиомикрофонов с амплитудной модуляцией; c) на измерении интенсивности сигнала в точке приема с помощью радиотестера; d) на основе эффекта акустической завязки.	ОПК-6
86.	d	Выберите один или несколько ответов: Режим акустозавязки индикатора поля позволяет при обнаружении радиозакладки услышать характерный ### отрицательной акустической обратной связи a) шум; b) гул; c) писк; d) свист.	ОПК-6

87.	с	Выберите один или несколько ответов: Наибольшими преимуществами по сравнению с остальными типами индикаторов поля (ИП) обладают: а) малогабаритные ИП; б) камуфлированные ИП; с) поисковые ИП; д) пороговые ИП.	ОПК-6
88.	с	Выберите один или несколько ответов: При облучении нелинейным локатором МОМ-диода в его приемнике наблюдается: а) сильный сигнал на второй и слабый сигнал на третьей гармонике; б) слабый сигнал на второй и слабый сигнал на третьей гармонике; с) слабый сигнал на второй и сильный сигнал на третьей гармонике; д) сильный сигнал на второй и сильный сигнал на третьей гармонике.	ОПК-6
89.	б	Выберите один или несколько ответов: Современный нелинейный локатор 4 поколения серии NR 900 E содержит: а) передающую и приемную антенны, два передатчика, три приемника, пульт управления и индикации; б) антенную систему, передатчик, два приемника, пульт управления и индикации; с) антенную систему, передатчик, приемник, пульт управления и индикации; д) приемопередающую антенну, приемопередатчик, пульт управления и индикации.	ОПК-6

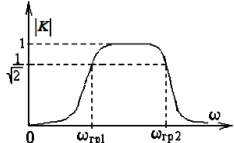
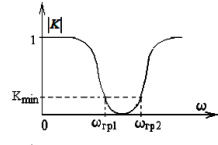
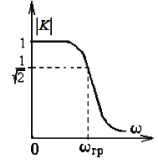
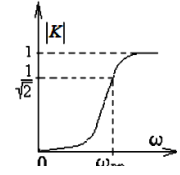
90.	a	Выберите один или несколько ответов: Перенос информации с помощью физических полей возможен за счет их способности сохранять ### занесенную информацию достаточно длительное время: a) в своей структуре; b) в своем образе; c) в своем пространстве; d) в окружающем пространстве.	ОПК-6
91.	a	Выберите один или несколько ответов: Носителем электромагнитного поля является: a) фотон; b) заряд; c) ток; d) электрон.	ОПК-6
92.	c	Выберите один или несколько ответов: Электромагнитные волны являются: a) переменными; b) продольными; c) поперечными; d) продольно-поперечными.	ОПК-6
93.	d	Выберите один или несколько ответов: К характеристике акустического поля, не влияющей на перенос информации, относится a) интенсивность акустических колебаний; b) мощность звука;	ОПК-6

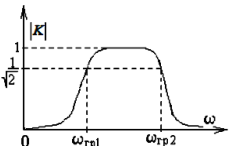
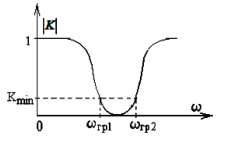
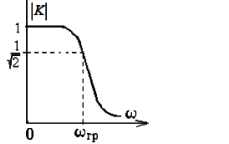
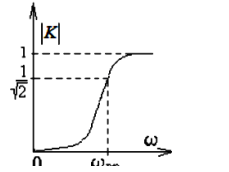
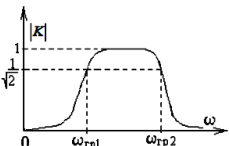
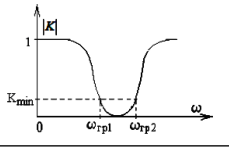
		с) звуковое давление; d) акустическое сопротивление среды	
94.	e	Выберите один или несколько ответов: Акустическое поле является: a) переменным; b) продольным; c) поперечным; d) продольно-поперечным; e) силовым.	ОПК-6
95.	c	Выберите один или несколько ответов: Составной технический канал утечки информации помимо элементов, присущих простому каналу утечки информации, содержит: e) источник (генератор) сигнала; f) источник (генератор) помех; g) преобразователь одного вида сигнала в другой; h) приемник сигнала.	ОПК-6
96.	a d	Выберите один или несколько ответов: К основным характеристикам переносных флюороскопов и рентгенотелевизионных установок относятся: a) проникающая способность; b) чувствительность; c) избирательность; d) разрешение.	ОПК-6

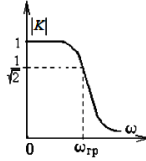
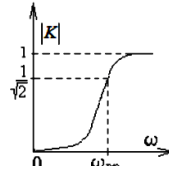
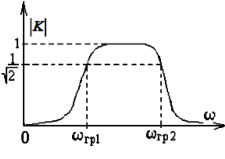
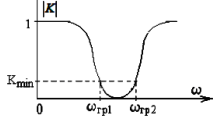
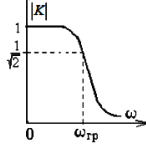
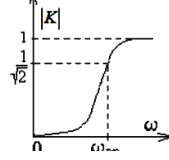
97.	a b	Выберите один или несколько ответов: Наиболее узкая полоса пропускания в сканирующем приемнике достигается при приеме сигналов a) AM-LSB; b) AM-USB; c) NFM; d) AM.	ОПК-6
98.	a	Выберите один или несколько ответов: Наилучшая чувствительность сканирующего приемника при приеме сигналов достигается: a) NFM; b) AM; c) SSB; d) WFM.	ОПК-6
99.	a	Выберите один или несколько ответов: К демаскирующим признакам акустических закладок типа телефонного уха не относится: a) наличие в телефонной линии радиоизлучения с модуляцией радиосигнала акустическим сигналом; b) падение напряжения в телефонной линии при положенной трубке; c) наличие тока утечки в телефонной линии при отключенном телефоне; d) подавление (не прохождение) одного-двух вызывных звонков при наборе телефонного аппарата.	ОПК-6

100.	a	Выберите один или несколько ответов: Демаскирующим признаком акустической радиозакладки является: a) наличие в ближней зоне модулированного сигнала; b) наличие в линии электропитания высокочастотного сигнала; c) наличие в помещении мощного высокочастотного излучения; d) наличие в помещении переизлученного радиосигнала.	ОПК-6
101.	b	Выберите один или несколько ответов: Приемники нелинейных локаторов при точности определения местонахождения полупроводниковых элементов в несколько см. обеспечивают дальность их обнаружения порядка: a) 5-20 метров; b) 0,5-2 метров c) 0,2-0,5 метров; d) 5-10 метров.	ОПК-6
102.	a	Выберите один или несколько ответов: Какой вариант в полном объеме характеризует понятие угрозы безопасности информации? a) ...понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств. b) ...потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам. c) ...возможность реализации воздействия на информацию, обрабатываемую в АИС, приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность	ОПК-6

		воздействия на компоненты АИС, приводящего к их утрате, уничтожению или сбою функционирования. d) ...потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.	
103.	a	Выберите один или несколько ответов: Какой структурно-функциональный элемент информационной системы не может быть подвержен формальному администрированию при реализации мер защиты информации? a) Сеть общего пользования. b) Рабочие станции организации. c) Сетевые устройства. d) Сервер организации.	ОПК-6
104.	a	Выберите один или несколько ответов: Обязательной аттестации подлежат объекты информатизации, предназначенные для: a) обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. b) обработки информации, представляющей коммерческую тайну. c) обработки информации, представляющей персональные данные. d) обработки информации служебного характера.	ОПК-6
105.	a b c	Выберите один или несколько ответов: Программно-аппаратные и технические средств защиты информации как правило реализуют следующие режимы работы: a) режим обнаружения; b) режим идентификации; c) режим анализа и измерения характеристик сигналов; d) режим нейтрализации.	ОПК-6

106.	a	Выберите один или несколько ответов: Технология проектирования систем радиомониторинга базируется: a) на временном или спектральном анализе принимаемых сигналов; b) на возможности обнаружения и приема (регистрация) сигнала; c) на реализации обработки (анализ) принятых сигналов; d) на возможности восстановления информации, содержащейся в принятых сигналах, и ее анализе.	ОПК-6
107.	b	Выберите один или несколько ответов: Укажите рисунок, отражающий амплитудно-частотную характеристику режекторного фильтра. a)  b)  c)  d) 	ОПК-6
108.	a	Выберите один или несколько ответов: Укажите рисунок, отражающий амплитудно-частотную характеристику полосового фильтра.	ОПК-6

		a)  b)  c)  d) 	
109.	с	Выберите один или несколько ответов: Укажите рисунок, отражающий амплитудно-частотную характеристику фильтра нижних частот. a)  b) 	ОПК-6

		 c)  d)	
110.	d	Выберите один или несколько ответов: Укажите рисунок, отражающий амплитудно-частотную характеристику фильтра верхних частот.  a)  b)  c)  d)	ОПК-6

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется, если студент показал глубокое, прочное и аргументированное освоение программного учебного материала, при этом поставленный вопрос раскрыт последовательно, четко и логически стройно, в полном исчерпывающем объеме, основные категории, понятия и термины учебного курса формулировались правильно, не допущено при ответе ошибок

Оценка «хорошо» выставляется, если студент показал твердое знание программного учебного материала, при этом поставленный вопрос раскрыт грамотно и по существу, в достаточно полном объеме, основные категории, понятия и термины учебного курса формулировались правильно, допущены при ответе отдельные неточности или одна ошибка;

Оценка «удовлетворительно» выставляется, если студент показал знание только основной части учебного материала без его частных деталей, при этом поставленный вопрос раскрыт с нарушением логической последовательности, не в полном объеме, были допущены неточные формулировки основных категорий, понятий и терминов учебного курса, а также ошибки (не более двух) или ряд незначительных неточностей, не исказивших существенно суть ответа;

Оценка «неудовлетворительно» выставляется, студенту, который не знает значительной части программного материала, допускает грубые ошибки (более двух), существенно исказившие его суть. Оценка неудовлетворительно выставляется также, если отсутствует письменный ответ на вопрос, либо студент отказался его сдавать.