

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Федеральное государственное автономное образовательное учреждение
высшего образования**
«Балтийский федеральный университет имени Иммануила Канта»
Образовательно-научный кластер «Институт высоких технологий»
Высшая школа киберфизических систем

КОМПЛЕКТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Шифр: 10.03.01

Направление подготовки:
Информационная безопасность

Направленность (профиль) образовательной программы:
«Организация и технологии защиты информации»

Калининград

НОРМАТИВНОЕ ОСНОВАНИЕ ОТБОРА СОДЕРЖАНИЯ

Формирование комплекта оценочных материалов проводилось в соответствии с

- Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 «Информационная безопасность», утвержденного приказом Минобрнауки России от 17.11.2020 г. № 1427;
- Профессиональный стандарт (ПС) 06.030, «Специалист по защите информации в телекоммуникационных системах и сетях» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н);
- Профессиональный стандарт (ПС) 06.032, «Специалист по безопасности компьютерных систем и сетей» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н);
- Профессиональный стандарт (ПС) 06.033, «Специалист по защите информации в автоматизированных системах» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н);
- Профессиональный стандарт (ПС) 06.034, «Специалист по технической защите информации» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н).

КОЛИЧЕСТВО ТЕСТОВЫХ ЗАДАНИЙ

Код компетенции	Наименование компетенции	Количество заданий
ОПК-2.1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников угроз, их возможных целей, путей реализации и предполагаемого ущерба	20
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	20
ПК-1	Способен к выполнению работ по установке, настройке, обеспечению бесперебойной работы и техническому обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации	20
ПК-5	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	20
ПК-7	Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	20
ПК-8	Способен проводить исследования на побочные электромагнитные излучения и наводки технических средств обработки информации, защищенности акустической речевой информации от утечки по техническим каналам	20
ИТОГО:		120

РАСПРЕДЕЛЕНИЕ ЗАДАНИЙ ПО КОМПЕТЕНЦИЯМ И ДИСЦИПЛИНАМ

Код и наименование компетенции	Индикатор достижения компетенции	Дисциплина / модуль / практика	Семестр
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-2.1.1. Знает принципы построения компьютерных систем и сетей; модели безопасности информационных систем; виды политик безопасности информационных систем; принципы построения средств криптографической защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; возможности используемых и планируемых к использованию средств защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации	Б1.О.07.06. Информационная безопасность корпоративных сетей	7
	ОПК-2.1.2. Умеет анализировать информационных систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты информационных систем; формулировать задания по безопасности информационных систем; выполнять анализ безопасности информационных систем и разрабатывать рекомендации по эксплуатации системы защиты информации		
	ОПК-2.1.3. Владеет навыками проведения анализа функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба		
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Знает методы и средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Б1.О.07.03. Защита информации от утечки по техническим каналам	6
	ОПК-9.2. Умеет выбирать методы и средства криптографической и технической защиты информации для решения задач профессиональной деятельности		
	ОПК-9.3. Имеет навыки практического использования средств криптографической и технической защиты информации для решения задач профессиональной деятельности		
ПК-1. Способен к выполнению работ по установке, настройке, обеспечению бесперебойной работы и техническому обслуживанию программных, программно-аппаратных (в том числе криптографических)	ПК-1.1. Знает состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Б1.В.02.04. Основы построения многоканальных инфокоммуникационных систем и сетей	5
	ПК-1.2. Умеет администрировать работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		

и технических средств и систем защиты информации	ПК-1.3. Владеет навыками применения средств контроля работ по установке, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		
ПК-5. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-5.1. Знает состав рабочей технической документации, действующие нормативные и методические документы	Б1.В.02.01. Метрология, стандартизация и сертификация	4
	ПК-5.2. Умеет применять технологические платформы, сервисы и информационные ресурсы создания технической документации		
	ПК-5.3. Владеет навыками сопровождения технической документации		
ПК-7. Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-7.1. Знает требования стандартов в области информационной безопасности	Б1.В.02.03. Основы электромагнитной совместимости	5
	ПК-7.2. Умеет создавать и вести справочный ресурс для анализа информационной безопасности объектов		
	ПК-7.3. Владеет навыками подготовки технических отчетов по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		
ПК-8. Способен проводить исследования на побочные электромагнитные излучения и наводки технических средств обработки информации, защищенности акустической речевой информации от утечки по техническим каналам	ПК-8.1. Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом «высокочастотного облучения» основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах	Б1.О.06.02. Распространение электромагнитных волн и антенно-фидерные устройства	4
	ПК-8.2. Умеет проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; проводить оценку защищенности информации от утечки за счет побочных электромагнитных излучений и наводок		
	ПК-8.3. Владеет навыками проведения контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; подготовки отчетных материалов по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (протоколов оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок)		

СЦЕНАРИИ ВЫПОЛНЕНИЯ ТЕСТОВЫХ ЗАДАНИЙ

Тип задания	Последовательность действий при выполнении задания
Задание закрытого типа на установление соответствия	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т. д.; список 2 – утверждения, свойства объектов и т. д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответов (например, А1 или Б4)
Задания закрытого типа на установление последовательности	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответов в нужной последовательности без пробелов и знаков препинания (например, БАВ или 213)
Задания комбинированного типа с выбором одного варианта из предложенных и обоснование ответа	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один ответ из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один правильный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа.
Задания комбинированного типа с выбором нескольких вариантов из предложенных и обоснование ответа	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько ответов из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать несколько правильных ответов. 4. Записать последовательность номеров (или букв) выбранных вариантов ответа. 5. Записать аргументы, обосновывающие выбор ответа.
Задания открытого типа с развернутым ответом	1. Внимательно прочитать текст задания и понять суть вопроса. 2. Продумать логику и полноту ответа. 3. Записать ответ, используя четкие компактные формулировки. 4. В случае расчетной задачи, записать решение и ответ.

СИСТЕМА ОЦЕНИВАНИЯ ВЫПОЛНЕНИЯ ТЕСТОВЫХ ЗАДАНИЙ

Задания закрытого типа оцениваются 1 баллом в случае верного ответа, и 0 баллами в случае неверного ответа.

Задания комбинированного типа оцениваются 1 баллом в случае верного ответа и правильного обоснования, которое соответствует критериям, указанным для открытого типа заданий, и 0 баллами в случае неверного ответа.

Задания открытого типа оцениваются в соответствии с критериями:

1. Правильность ответа (отсутствие фактических ошибок).
2. Полнота ответа (раскрытие объема используемых понятий).
3. Обоснованность ответа (наличие аргументов).
4. Логика изложения ответа (грамотная последовательность излагаемого материала).
5. Сопоставимость с эталонным ответом.

ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ И ОБОРУДОВАНИЕ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Код и наименование компетенции	Индикатор достижения компетенции	Дисциплина / модуль / практика	Уровень сложности	Задание	Ключ								
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-2.1.1. Знает принципы построения компьютерных систем и сетей; модели безопасности информационных систем; виды политик безопасности информационных систем; принципы построения средств криптографической защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; возможности используемых и планируемых к использованию средств защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;	Б1.О.07.06. Информационная безопасность корпоративных сетей	Базовый	Установите соответствие между типом угрозы и ее примером в корпоративной сети. <table><tr><td>А. Несанкционированный доступ</td><td>1. Удаленное подключение к серверу без прохождения авторизации</td></tr><tr><td>Б. Нарушение доступности</td><td>2. DDoS-атака на веб-сервер</td></tr><tr><td>В. Искажение информации</td><td>3. Изменение данных в базе клиентов</td></tr><tr><td>Г. Разглашение информации</td><td>4. Перехват и последующая передача конфиденциальной переписки сотрудников</td></tr></table>	А. Несанкционированный доступ	1. Удаленное подключение к серверу без прохождения авторизации	Б. Нарушение доступности	2. DDoS-атака на веб-сервер	В. Искажение информации	3. Изменение данных в базе клиентов	Г. Разглашение информации	4. Перехват и последующая передача конфиденциальной переписки сотрудников	1 2 3 4
			А. Несанкционированный доступ	1. Удаленное подключение к серверу без прохождения авторизации									
			Б. Нарушение доступности	2. DDoS-атака на веб-сервер									
В. Искажение информации	3. Изменение данных в базе клиентов												
Г. Разглашение информации	4. Перехват и последующая передача конфиденциальной переписки сотрудников												
Базовый	Установите соответствие между способом разграничения доступа и его характеристикой. <table><tr><td>А. Ролевой контроль доступа (RBAC)</td><td>1. Доступ определяется на основе атрибутов пользователя, ресурса и среды.</td></tr><tr><td>Б. Дискреционный контроль доступа (DAC)</td><td>2. Доступ предоставляется на основе назначения пользователю определенных ролей.</td></tr><tr><td>В. Мандатный контроль доступа (MAC)</td><td>3. Владелец ресурса определяет, кто имеет к нему доступ.</td></tr><tr><td>Г. Атрибутный контроль доступа (ABAC)</td><td>4. Система определяет доступ на основе меток безопасности и правил.</td></tr></table>	А. Ролевой контроль доступа (RBAC)	1. Доступ определяется на основе атрибутов пользователя, ресурса и среды.	Б. Дискреционный контроль доступа (DAC)	2. Доступ предоставляется на основе назначения пользователю определенных ролей.	В. Мандатный контроль доступа (MAC)	3. Владелец ресурса определяет, кто имеет к нему доступ.	Г. Атрибутный контроль доступа (ABAC)	4. Система определяет доступ на основе меток безопасности и правил.	2 3 4 1			
А. Ролевой контроль доступа (RBAC)	1. Доступ определяется на основе атрибутов пользователя, ресурса и среды.												
Б. Дискреционный контроль доступа (DAC)	2. Доступ предоставляется на основе назначения пользователю определенных ролей.												
В. Мандатный контроль доступа (MAC)	3. Владелец ресурса определяет, кто имеет к нему доступ.												
Г. Атрибутный контроль доступа (ABAC)	4. Система определяет доступ на основе меток безопасности и правил.												
Повышенный	Какая из перечисленных причин является основной движущей силой роста уязвимостей в современных компьютерных системах, несмотря на постоянное совершенствование мер защиты? А. Недостаток квалифицированных специалистов в области ИБ.	Б. Рост уязвимостей тесно связан с экспоненциальным бурным развитием информационных технологий, что приводит к появлению новых, ранее											

	организационные меры по защите информации.			Б. Быстрое развитие технологий, появление новых протоколов и сервисов, сложность аппаратного и программного обеспечения. В. Увеличение числа пользователей, работающих с конфиденциальной информацией. Г. Противоречивость и сложность законодательной базы, регулирующей вопросы информационной безопасности.	неизвестных уязвимостей и способов их эксплуатации.
			Повышенный	Определите, какой из перечисленных подходов является системным для обеспечения информационной безопасности корпоративной сети. А. Установка антивирусного программного обеспечения на все рабочие станции; Б. Применение сертифицированных технических средств защиты, таких как межсетевые экраны, средства антивирусной защиты и др. В. Применение организационных, технических и правовых мер, охватывающих все уровни и компоненты корпоративной сети, с учетом жизненного цикла информации. Г. Регулярное проведение обучения по основам ИБ всего персонала без исключения.	В. Системный подход предполагает целостное рассмотрение ИБ, а не отдельных разрозненных мер. Подход к построению защищенных компьютерных сетей, основанный на учете всех исходных требований, существующих угроз и влияющих на безопасность факторов при комплексном использовании наиболее эффективных мер, методов и средств защиты.
			Повышенный	В контексте концепции многоуровневой защиты ресурсов корпоративных сетей, какой уровень является наиболее близким к пользователю корпоративной сети и защищает непосредственно рабочие станции и другие пользовательские устройства? А. Уровень сетевой инфраструктуры. Б. Уровень приложений. В. Уровень конечных точек. Г. Уровень центра обработки данных.	В. Уровень конечных точек фокусируется на защите устройств, которыми непосредственно пользуются работники, что делает его последним рубежом обороны.

			Высокий	Дайте ответ на поставленный вопрос. Что такое виртуальная частная сеть (VPN) и какие ее основные особенности?	VPN – это технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную сеть, обеспечивающую безопасность циркулирующих данных. Особенности: - виртуальная сеть формируется на основе каналов связи открытой сети; - термин «виртуальная» подчеркивает, что каналы связи виртуальной сети моделируются с помощью каналов связи реальной; - открытая сеть может служить основой для одновременного сосуществования множества виртуальных сетей, количество которых определяется пропускной способностью открытых каналов связи.
--	--	--	---------	---	---

			Высокий	В каких сценариях применяются однонаправленные шлюзы и какой основной принцип безопасности они реализуют?	Однонаправленные шлюзы являются крайне важной мерой защиты для критической информационной инфраструктуры. Они применяются для предотвращения несанкционированного доступа к критически важным сетям и системам (например, АСУ ТП) из внешних сетей, гарантируя, что данные могут передаваться только в одном направлении – из сегмента с более низким уровнем конфиденциальности (критичности) в сегмент с более высоким уровнем конфиденциальности (критичности)							
ОПК-2.1.2. Умеет анализировать информационных систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты информационных систем; формулировать задания по	Б1.О.07.06. Информационная безопасность корпоративных сетей	Базовый	Установите соответствие между типом межсетевого экрана и соответствующим уровнем модели OSI. <table><tr><td>А. Пакетный фильтр</td><td>1. Сетевой уровень</td></tr><tr><td>Б. Шлюз приложений, прокси-сервер</td><td>2. Многоуровневый</td></tr><tr><td>В. Инспектор состояния (Stateful Inspection Firewall)</td><td>3. Сетевой и транспортный уровни</td></tr><tr><td>Г. Межсетевой экран следующего поколения (NGFW)</td><td>4. Прикладной уровень</td></tr></table>	А. Пакетный фильтр	1. Сетевой уровень	Б. Шлюз приложений, прокси-сервер	2. Многоуровневый	В. Инспектор состояния (Stateful Inspection Firewall)	3. Сетевой и транспортный уровни	Г. Межсетевой экран следующего поколения (NGFW)	4. Прикладной уровень	1 4 3 2
		А. Пакетный фильтр	1. Сетевой уровень									
Б. Шлюз приложений, прокси-сервер	2. Многоуровневый											
В. Инспектор состояния (Stateful Inspection Firewall)	3. Сетевой и транспортный уровни											
Г. Межсетевой экран следующего поколения (NGFW)	4. Прикладной уровень											
		Повышенный	Что понимается под «моделью защищаемых ресурсов» при анализе функциональных процессов корпоративной сети?	В.								

	безопасности информационных систем; выполнять анализ безопасности информационных систем и разрабатывать рекомендации по эксплуатации системы защиты информации			А. Схематическое изображение сетевой топологии. Б. Список всех пользователей и их прав доступа. В. Детальное описание всех активов, данных, сервисов и систем, которые необходимо защищать, с указанием их ценности и критичности. Г. Конфигурационные файлы всех серверов и коммутаторов в сети, а также АРМ пользователей.	Формирование модели защищаемых ресурсов - идентификация и анализ защищаемых ресурсов, в качестве которых рассматривается все, что представляет ценность в корпоративной сети или автоматизированной системе. Понимание того, что защищать, является основой для определения того, как организовывать и строить защиту ресурсов.
			Повышенный	Что является основной целью «модели нарушителя» при анализе угроз информационной безопасности? А. Описание всех существующих типов вредоносного ПО. Б. Описание потенциальных субъектов угроз, их мотивов, возможностей и методов действий. В. Классификация всех возможных векторов атак. Г. Анализ технических характеристик средств защиты.	Б. Формирование модели уязвимостей и модели нарушителя - выявление уязвимостей и потенциальных нарушителей, которые делают возможной реализацию угроз. Понимание противника помогает эффективнее формировать модель контрмер.
			Повышенный	Концепция контроля доступа в компьютерную систему предполагает применение ряда механизмов. Какой из них	Б.

				обеспечивает определение того, кто пытается получить доступ? А. Авторизация. Б. Идентификация. В. Аутентификация. Г. Разграничение доступа.	Идентификация – первый шаг получения доступа к системе, когда субъект предъявляет идентификатор (например, логин, смарт-карту и т.п.), сообщая тем самым, кем он является.
			Повышенный	Какие основные функции выполняет диспетчер доступа к корпоративным ресурсам? А. Шифрование трафика при межсетевом взаимодействии и защита корпоративной сети от DDoS-атак. Б. Управление сетевой адресацией с использованием сервисов DHCP, DNS. В. Проверка учетных данных, авторизация, а также ведение журнала событий доступа. Г. Мониторинг доступности и производительности сетевых устройств, реагирование на аномалии.	В. Диспетчер доступа является центральным звеном, контролирующим, кто и к чему может получить доступ.
			Высокий	Опишите, как можно проанализировать процесс передачи конфиденциальных данных от клиентского приложения на сервер в корпоративной сети с целью выявления возможных источников угроз. Перечислите как минимум три типа потенциальных угроз и пути их реализации.	Анализ включает исследование следующих аспектов: 1. Процесс передачи: Использование какого протокола (HTTP, HTTPS, FTP, SCP и т.д.)? Где происходит шифрование (на уровне приложения, на транспортном уровне)? 2. Точки входа/выхода сетевого трафика: Какие устройства

					(межсетевые экраны, прокси-серверы, VPN-шлюзы) обрабатывают этот трафик? 3. Аутентификация и авторизация: Как клиент и сервер аутентифицируются? Как проверяются права доступа? Угроза: Перехват данных (случайный или намеренный). Путь реализации: Использование незащищенного протокола (HTTP вместо HTTPS), отсутствие шифрования на промежуточных узлах, атаки “человек посередине” в незащищенных сетях. Угроза: Несанкционированный доступ к данным на сервере. Путь реализации: Слабая аутентификация клиента, уязвимости в серверном ПО, доступ к данным по украденным учетным записям, недостаточная авторизация.
--	--	--	--	--	--

					Угроза: Искажение данных во время передачи. Путь реализации: Отсутствие механизмов проверки целостности данных (например, цифровых подписей, контрольных сумм), атаки типа “Man-in-the-Middle” с подменой данных.								
	ОПК-2.1.3. Владеет навыками проведения анализа функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Б1.О.07.06. Информационная безопасность корпоративных сетей	Базовый	Установите соответствие между моделью атаки и ее описанием. <table><tr><td>А. Атака типа «Человек посередине» (Man-in-the-Middle, MitM)</td><td>1. Отправка большого количества запросов на сервер с целью перегрузить его и сделать недоступным для легитимных пользователей.</td></tr><tr><td>Б. Атака отказа в обслуживании (DoS/DDoS)</td><td>2. Получение доступа к конфиденциальной информации (например, паролям, данным кредитных карт) путем маскировки под доверенное лицо или организацию.</td></tr><tr><td>В. Фишинг</td><td>3. Перехват и, возможно, изменение данных, передаваемых между двумя сторонами, путем «вставки» себя в канал связи.</td></tr><tr><td>Г. Атака методом перебора паролей (Brute-force attack)</td><td>4. Систематическая попытка угадать пароль путем тестирования всех возможных комбинаций символов.</td></tr></table>	А. Атака типа «Человек посередине» (Man-in-the-Middle, MitM)	1. Отправка большого количества запросов на сервер с целью перегрузить его и сделать недоступным для легитимных пользователей.	Б. Атака отказа в обслуживании (DoS/DDoS)	2. Получение доступа к конфиденциальной информации (например, паролям, данным кредитных карт) путем маскировки под доверенное лицо или организацию.	В. Фишинг	3. Перехват и, возможно, изменение данных, передаваемых между двумя сторонами, путем «вставки» себя в канал связи.	Г. Атака методом перебора паролей (Brute-force attack)	4. Систематическая попытка угадать пароль путем тестирования всех возможных комбинаций символов.	3 1 2 4
А. Атака типа «Человек посередине» (Man-in-the-Middle, MitM)	1. Отправка большого количества запросов на сервер с целью перегрузить его и сделать недоступным для легитимных пользователей.												
Б. Атака отказа в обслуживании (DoS/DDoS)	2. Получение доступа к конфиденциальной информации (например, паролям, данным кредитных карт) путем маскировки под доверенное лицо или организацию.												
В. Фишинг	3. Перехват и, возможно, изменение данных, передаваемых между двумя сторонами, путем «вставки» себя в канал связи.												
Г. Атака методом перебора паролей (Brute-force attack)	4. Систематическая попытка угадать пароль путем тестирования всех возможных комбинаций символов.												

			Базовый	Выберите правильную последовательность базовых этапов построения системы информационно-компьютерной безопасности в корпоративной сети. 1. Эксплуатация и сопровождение системы защиты. 2. Определение детальных требований к системе защиты. 3. Выбор и внедрение технических и организационных средств защиты. 4. Анализ и оценка рисков. 5. Аудит и совершенствование системы защиты. 6. Разработка политики информационной безопасности.	4 2 6 3 1 5
			Повышенный	Метод аутентификации на основе одноразового пароля (ОТР) обеспечивает: А. Постоянную аутентификацию пользователя. Б. Уменьшение риска перехвата и повторного использования пароля. В. Полную защиту от социальной инженерии. Г. Автоматическое обновление паролей.	Б. Одноразовый пароль действителен только для одной сессии или короткого промежутка времени, что значительно снижает риски, связанные с его компрометацией.
			Повышенный	Помимо фильтрации трафика, какие функции посредничества может выполнять межсетевой экран для повышения безопасности? (Выберите несколько вариантов). А. Шифрование трафика между внутренними узлами. Б. Трансляция сетевых адресов (NAT). В. Автоматическая установка обновлений безопасности на всех серверах корпоративной сети. Г. Оптимизация пропускной способности канала связи. Д. Кэширование данных. Е. Аудит и регистрация событий.	Б, Е Трансляция сетевых адресов (NAT) позволяет скрывать топологию внутренней защищаемой корпоративной сети, уменьшает поверхность атаки, не раскрывая реальные IP-адреса внутренних устройств. Функция аудита и регистрации событий позволяет обеспечивать

					подотчетность и полный контроль информационных потоков при межсетевом взаимодействии.
			Повышенный	Какие методы используются злоумышленником на этапе сбора информации о целевой корпоративной информационной системе? (Выберите несколько вариантов). А. Сканирование открытых портов и служб. Б. Перебор паролей пользователей. В. Анализ заголовков электронной почты. Г. Проверка наличия обновлений безопасности на веб-сайте компании. Д. Горизонтальное перемещение, распространение внутри сети.	А, В, Г Сканирование портов (А) выявляет открытые службы. Анализ заголовков писем (В) может дать информацию о внутренней структуре сети и используемых серверах. Изучение публичной информации о веб-сайте (Г) помогает понять используемые технологии и их версии. Перебор паролей (Б) — это метод получения доступа, а не сбора информации об инфраструктуре, горизонтальное перемещение (Д) - тактика, которую используют злоумышленники после получения первоначального доступа к инфраструктуре

			Высокий	Дайте определение «модели угроз» в контексте корпоративных сетей.	Модель угроз – документ (список угроз), описывающий потенциальные источники угроз, их цели, способы реализации и последствия для защищаемых ресурсов корпоративной сети.
			Высокий	Перечислите 2 основных способа защиты от потери информации в корпоративных сетях.	1) Регулярное резервное копирование информации 2) Внесение информационной и функциональной избыточности (дублирование информации и элементов компьютерной системы (репликация данных, кластеризация серверов, технологии RAID)).

Код и наименование компетенции	Индикатор достижения компетенции	Дисциплина / модуль / практика	Уровень сложности	Задание	Ключ
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Знает методы и средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Б1.О.07.03. Защита информации от утечки по техническим каналам	Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какая организация осуществляет сертификацию технических средств защиты информации не криптографическими методами? 1. ФСТЭК РФ 2. ФСБ РФ 3. СВР РФ	1 – В соответствии с постановлением Правительства РФ № 608 от 26.06.1995 – «Положение о сертификации СЗИ» и

				4. МО РФ 5. МВД РФ	с Приказом ФСТЭК России № 55 от 03.04.2018
			Базовый	Дайте ответ на поставленный вопрос. Что называется техническим каналом утечки информации ?	ТКУИ называется совокупность источника информации, физической среды, по которой распространяется информационный сигнал и технических средств перехвата информации.
			Повышенный	Дайте ответ на поставленный вопрос. Что называется специальной проверкой?	Специальная проверка – это комплекс технических мероприятий, направленных на выявление и изъятие закладных устройств в технических средствах и системах.
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. В каком диапазоне длин волн человек способен воспринимать акустические колебания при помощи своих органов слуха? 1) 5 Гц – 20 Гц; 2) 20 Гц – 400 Гц; 3) 400 Гц – 20 000 Гц; 4) 20 000 Гц – 2 МГц.	3 – В соответствии с физиологическими особенностями организма человека.
			Повышенный	Дайте ответ на поставленный вопрос. Что называется контролируемой зоной?	Контролируемая зона – это пространство (территория, здание, часть здания ...), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных

					средств.
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Как называется процесс изменения параметров зондирующего сигнала в зависимости от характеристик информационного сигнала? 1) поляризация; 2) модуляция; 3) фрагментация; 4) дискретизация.	2 – Любой процесс изменения параметров высокочастотного сигнала (зондирующего) по закону низкочастотного сигнала называется модуляцией.
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какое техническое средство будет использовать злоумышленник, если он хочет снять информацию через оконное стекло выделенного помещения? 1) параболический микрофон; 2) трубчатый микрофон; 3) лазерное средство разведки; 4) направленную антенну сканирующего приемника.	3 – Лазерный луч, отражаясь от вибрирующей поверхности окна, будет модулироваться низкочастотными акустическими колебаниями.
	ОПК-9.2. Умеет выбирать методы и средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Б1.О.07.03. Защита информации от утечки по техническим каналам	Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какая организация осуществляет сертификацию технических средств защиты информации криптографическими методами? 1. ФСТЭК РФ 2. ФСБ РФ 3. СВР РФ 4. МО РФ 5. МВД РФ	2 – В соответствии с ФЗ 03.04.1995 № 40 «О ФСБ РФ», и с указом Президента РФ № 9603 от 11.08.2003 «Вопросы ФСБ РФ»
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какое звуковое давление соответствует условному значению нулевого уровня?	1- Это давление соответствует физиологическому порогу слышимости человека.

				1) $2 \cdot 10^{-5}$ Па; 2) $5 \cdot 10^{-5}$ Па; 3) $2 \cdot 10^{-12}$ Па; 4) $10 \cdot 2^{-5}$ Па.	
			Повышенный	Дайте ответ на поставленный вопрос. Что называется специальным обследованием?	Специальное обследование – это комплекс технических мероприятий, направленных на выявление и изъятие закладных устройств в защищаемых выделенных помещениях.
			Повышенный	Дайте ответ на поставленный вопрос. Что называется специальным исследованием?	Специальное исследование – это комплекс технических мероприятий, направленных на выявление возможных технических каналов утечки информации и выдачи рекомендаций по приведению защиты информации в соответствии с нормативными документами.
			Повышенный	Дайте ответ на поставленный вопрос. Что называется распределенной случайной антенной?	Распределенная случайная антенна – это любая токопроводящая коммуникация (провода, металлические трубы и т.п.), выходящая за пределы контролируемой зоны.
			Высокий	Дайте ответ на поставленный вопрос. Что называется сосредоточенной случайной антенной?	Сосредоточенная случайная антенна – это техническое средство,

					имеющее выход за пределы контролируемой зоны посредством проводных (гальванических) коммуникаций.
ОПК-9.3. Имеет навыки практического использования средств криптографической и технической защиты информации для решения задач профессиональной деятельности	Б1.О.07.03. Защита информации от утечки по техническим каналам	Базовый	Дайте ответ на поставленный вопрос. Что называется опасной зоной R1?		Опасной зоной R1 называется область пространства вокруг технических средств приема, передачи, обработки, хранения и отображения информации (ТСПИ), в которой наводки на случайных сосредоточенных антеннах выше допустимого нормированного уровня.
			Дайте ответ на поставленный вопрос. Что называется опасной зоной R2?		Опасной зоной R2 называется область пространства вокруг технических средств приема, передачи, обработки, хранения и отображения информации (ТСПИ), в которой отношение сигнал/шум побочных электромагнитных излучений ТСПИ превышает допустимое нормированное значение.
			Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа.		3 – Виброакустический канал предполагает утечку информации

				Где распространяется опасный сигнал в случае виброакустического канала утечки информации? 1) в вакууме; 2) в телефонных линиях; 3) в твердых телах; 4) по каналу Wi-Fi.	посредством вибрации структурных составляющих среды, то есть распространения упругой волны в твердом теле.
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какие технические средства чаще всего используют злоумышленники для снятия информации по виброакустическому каналу утечки? 1) инфракрасные приемники; 2) направленные антенны; 3) стетоскопы; 4) анализаторы спектра.	3 – Стетоскопы – это приборы, оснащенные датчиками давления, срабатывающими на изменения плотности среды (вибрации).
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какие датчики расположены в узлах плоской фазированной акустической решетки? 1) датчики УФ излучения; 2) емкостные датчики движения; 3) приемники ИК излучения; 4) микрофоны.	4 – Микрофоны являются датчиками, срабатывающими на изменения плотности среды (распространение акустической волны в воздухе).
			Высокий	Дайте ответ на поставленный вопрос. В чем заключается микрофонный эффект?	Микрофонный эффект – это возникновение в электрических цепях радиоэлектронной аппаратуры электрических сигналов, обусловленных механическими воздействиями (акустическим полем, вибрациями, сотрясениями). Он обусловлен незначительными изменениями параметров элементов

					схем (емкости, индуктивности, сопротивления) вследствие этого воздействия.
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Как называется сигнал, который можно представить непрерывной функцией непрерывного аргумента? 1) дискретный; 2) импульсный; 3) цифровой; 4) аналоговый.	4 – Непрерывным образом может изменяться только аналоговый сигнал, соответственно, функция времени, описывающая этот сигнал, тоже будет непрерывной.

Код и наименование компетенции	Индикатор достижения компетенции	Дисциплина / модуль / практика	Уровень сложности	Задание	Ключ				
ПК-1. Способен к выполнению работ по установке, настройке, обеспечению бесперебойной работы и техническому обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации	ПК-1.1. Знает состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Б1.В.02.04. Основы построения многоканальных инфокоммуникационных систем и сетей	Базовый	Скорость передачи основного цифрового канала: <table><tr><td>1. 1544 кбит/с</td></tr><tr><td>2. 2048 кбит/с</td></tr><tr><td>3. 64000 бит/с</td></tr><tr><td>4. 1544 бит/с</td></tr></table>	1. 1544 кбит/с	2. 2048 кбит/с	3. 64000 бит/с	4. 1544 бит/с	3 - ОЦК — это типовой цифровой канал передачи, который используется в цифровых системах связи. Он служит основой для построения иерархий цифровых систем передачи, например, плезиохронной цифровой иерархии (PDH). Такая скорость выбрана не случайно: 64 кбит/с достаточно для передачи сигнала тональной частоты, продискретизированного с частотой 4 кГц и проквантованного по 256 уровням.
			1. 1544 кбит/с						
2. 2048 кбит/с									
3. 64000 бит/с									
4. 1544 бит/с									
Базовый	4-й уровень плезиохронной цифровой иерархии(ПЦИ) в Европе соответствует скорости: <table><tr><td>1. 98 Мбит/с</td></tr><tr><td>2. 139,264 Мбит/сек</td></tr><tr><td>3. 274,176 Мбит/с</td></tr><tr><td>4. 564,992 Мбит/с</td></tr></table>	1. 98 Мбит/с	2. 139,264 Мбит/сек	3. 274,176 Мбит/с	4. 564,992 Мбит/с	2 -Четвёртый уровень плезиохронной цифровой иерархии (ПЦИ) в Европе соответствует скорости 139,264 Мбит/с			
1. 98 Мбит/с									
2. 139,264 Мбит/сек									
3. 274,176 Мбит/с									
4. 564,992 Мбит/с									

					В европейской системе ПЦИ используются следующие скорости по уровням иерархии: • 1-й уровень — 2,048 Мбит/с; • 2-й уровень — 8,448 Мбит/с; • 3-й уровень — 34,368 Мбит/с; • 4-й уровень — 139,264 Мбит/с				
			Повышенный	Процесс выравнивания скоростей цифровых потоков называется: <table><tr><td>1. Стробирование</td></tr><tr><td>2. Кросс-мультиплексирование</td></tr><tr><td>3. Свертывание</td></tr><tr><td>4. Стаффинг</td></tr></table>	1. Стробирование	2. Кросс-мультиплексирование	3. Свертывание	4. Стаффинг	4- Процесс выравнивания скоростей цифровых потоков называется методом стаффинга (stuffing — вставка). Суть метода заключается в том, что в буферных запоминающих устройствах (ЗУ) из входящего потока исключается повторно считанный «лишний» бит или вводится символ вместо пропущенного бита. Одновременно информация об этих операциях передаётся по служебному каналу, входящему в групповой поток. На приёмной стороне на основе этой информации биты информации исключаются или вставляются, и исходная скорость цифрового потока восстанавливается
1. Стробирование									
2. Кросс-мультиплексирование									
3. Свертывание									
4. Стаффинг									
			Повышенный	Информация об изъятых и о вставленных битах в цикле ПЦИ: <table><tr><td>1. Передается по служебным каналам</td></tr><tr><td>2. «Защита» во фреймах</td></tr><tr><td>3. Находится в тайм-слотах</td></tr><tr><td>4. Фиксируется в данных о полезной нагрузке</td></tr></table>	1. Передается по служебным каналам	2. «Защита» во фреймах	3. Находится в тайм-слотах	4. Фиксируется в данных о полезной нагрузке	1 - Информация об изъятых и вставленных битах в цикле ПЦИ (плезиохронной цифровой иерархии, PDH) передаётся по служебным каналам управления, которые формируются отдельными
1. Передается по служебным каналам									
2. «Защита» во фреймах									
3. Находится в тайм-слотах									
4. Фиксируется в данных о полезной нагрузке									

					битами в структуре фрейма в рамках общего потока управления.
			Повышенный	Длительность цикла ПЦИ составляет:	3 - Длительность цикла в плезиохронной цифровой иерархии (ПЦИ, PDH) составляет 125 микросекунд . Этот параметр соответствует интервалу дискретизации канала с частотой 8 кГц, которая используется при кодировании речевого сигнала тональной частоты.
				1. 84 мкс	
				2. 122 мкс	
				3. 125 мкс	
			Высокий	4. 264 мкс	
				Где на линии связи устанавливают терминальные мультиплексоры?	3 - Терминальные мультиплексоры устанавливают на концах линии связи. Они располагаются на конечных станциях и выполняют следующие функции: • на передающей стороне преобразуют сигналы, затем мультиплексируют их в один сигнал для дальнейшей передачи; • на принимающей стороне демультиплексируют сигнал и направляют его к соответствующему оборудованию.
				1. Устанавливают в разрыв линии связи.	
				2. Устанавливают в разрыв и на окончаниях линии связи	
				3. На окончаниях линии связи	
			Высокий	В отличие от терминальных, мультиплексоры ввода/вывода позволяют выполнять:	4 - В отличие от терминальных мультиплексоров, мультиплексоры ввода/вывода (ADM — Add/Drop Multiplexer) позволяют выполнять дополнительные функции, связанные с транспортировкой потоков и резервированием в сети. Основные возможности мультиплексоров ввода/вывода: • Сквозная коммутация выходных потоков в обоих направлениях. Это
				1. Задачи коммутации	
				2. Задачи концентрации цифрового потока	
				3. Задачи регенерации цифровых сигналов	
			Высокий	4. Сквозную коммутацию выходных потоков в обоих направлениях	

					означает, что данные могут передаваться через мультиплексор в разных направлениях, что важно для организации сложных топологий сети, например кольца.
ПК-1.2. Умеет администрировать работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Б1.В.02.04. Основы построения многоканальных инфокоммуникационных систем и сетей	Базовый	Какие ошибки импульсных сигналов на приеме позволяет оценивать метод глаз- диаграммы? 1. амплитудные 2. частотные 3. временные 4. фазовые	13	
		Повышенный	Что обуславливает возникновение искажений при декодировании ИКМ сигналов? 1. Недостаточный динамический диапазон 2. Недостаточное число уровней квантования 3. Недостаточный уровень сигнал/шум	2 - Искажения при декодировании сигналов с импульсно-кодовой модуляцией (ИКМ) могут возникать по нескольким причинам, связанным с особенностями процесса преобразования сигналов, характеристиками канала связи и техническими ограничениями систем. Основные причины искажений: 1. Ошибка квантования — разница между уровнем входного аналогового напряжения и ближайшим уровнем квантования, используемым ИКМ-кодером для его представления. Эта ошибка почти всегда присутствует, поэтому сигнал на выходе ИКМ-декодера отличается от оригинального. Если	

					ошибка квантования не слишком велика, она может восприниматься как наложившееся на сигнал шипение (шум квантования).				
			Повышенный	Какая типология позволяет процедуру самовосстановление при отказах на соседних линиях на сети SDH(СЦИ)? <table><tr><td>1.Линейная типа «точка-точка»</td></tr><tr><td>2.Линейная типа «ввода-вывода»</td></tr><tr><td>3.«Звезда»</td></tr><tr><td>4.«Кольцо»</td></tr></table>	1.Линейная типа «точка-точка»	2.Линейная типа «ввода-вывода»	3.«Звезда»	4.«Кольцо»	4. Кольцевые структуры — типология сети SDH, которая позволяет осуществлять самовосстановление при отказах на соединительных линиях. В таких структурах применяются мультиплексоры ввода-вывода, и они создают резервный путь, по которому передаются сигналы в случае повреждения основной линии
1.Линейная типа «точка-точка»									
2.Линейная типа «ввода-вывода»									
3.«Звезда»									
4.«Кольцо»									
			Повышенный	К недостатками полупроводниковых лазерных усилителей относят: <table><tr><td>Потери большей части светового потока перед активной областью и уменьшение КПД усилителя</td></tr><tr><td>Высокие требования к погрешностям усиления</td></tr><tr><td>Зависимость от направления поляризации, которое является неконтролируемым фактором в одномодовом волокне</td></tr><tr><td>Случайный перенос энергии оптической волны на волну с другой частотой</td></tr></table>	Потери большей части светового потока перед активной областью и уменьшение КПД усилителя	Высокие требования к погрешностям усиления	Зависимость от направления поляризации, которое является неконтролируемым фактором в одномодовом волокне	Случайный перенос энергии оптической волны на волну с другой частотой	12
Потери большей части светового потока перед активной областью и уменьшение КПД усилителя									
Высокие требования к погрешностям усиления									
Зависимость от направления поляризации, которое является неконтролируемым фактором в одномодовом волокне									
Случайный перенос энергии оптической волны на волну с другой частотой									
			Повышенный	Оптическая секция (ОС, или OS) — это: <table><tr><td>1.Участок синхронного линейного тракта между оконечными пунктами или между оконечным пунктом и пунктом ввода/вывода сигналов</td></tr><tr><td>2.Участок синхронного линейного тракта между регенератором и пунктом ввода/вывода сигналов</td></tr></table>	1.Участок синхронного линейного тракта между оконечными пунктами или между оконечным пунктом и пунктом ввода/вывода сигналов	2.Участок синхронного линейного тракта между регенератором и пунктом ввода/вывода сигналов	3 - Также оптическую секцию можно определить как всё, что образует оптический тракт как физическую среду передачи между выходом оптического источника одного оборудования и входом оптического детектора следующего оборудования		
1.Участок синхронного линейного тракта между оконечными пунктами или между оконечным пунктом и пунктом ввода/вывода сигналов									
2.Участок синхронного линейного тракта между регенератором и пунктом ввода/вывода сигналов									

				3.Участок от точки электронно-оптического до точки опто-электронно преобразований сигнала	(согласно рекомендации МСЭ-Т G.972			
				4.Участок синхронного линейного тракта между регенератором и соседним оконечным пунктом или между двумя соседними регенераторами				
			Высокий	При расчете бюджета потерь в оптической линии PON необходимо проверить для каждой цепи, чтобы общая величина потерь не превышала..... <table><tr><td>1.чувствительность приемника</td></tr><tr><td>2.мощность передатчика</td></tr><tr><td>3.динамический диапазон системы</td></tr></table>	1.чувствительность приемника	2.мощность передатчика	3.динамический диапазон системы	3 - При расчёте бюджета потерь в оптической линии PON необходимо проверить, чтобы общая величина потерь (включая эксплуатационный запас) не превышала динамический диапазон системы. Динамический диапазон PON — это диапазон допустимых значений, в котором система может работать без потери качества сигнала. Он определяется как разность между минимальной выходной мощностью передатчика OLT и допустимой мощностью на входе приёмника ONU.
1.чувствительность приемника								
2.мощность передатчика								
3.динамический диапазон системы								
ПК-1.3. Владеет навыками применения средств контроля работ по установке, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических	Б1.В.02.04. Основы построения многоканальных инфокоммуникационных систем и сетей	Базовый	Как изменится скорости передачи информации при переходе с использованием 8-и разрядного кодирования с равномерным квантованием к 12-и разрядному кодированию? <table><tr><td>1. Увеличится в 1,5 раза</td></tr><tr><td>2. Уменьшится в 1,5 раза</td></tr><tr><td>3. Не изменится</td></tr></table>	1. Увеличится в 1,5 раза	2. Уменьшится в 1,5 раза	3. Не изменится	1 – учитывая необходимость оценки характеристик защищенности при равномерном квантовании и количестве шагов, определяемом 12-и и 8-и разрядным кодированием. Очевидно, что использование 8-и разрядного кодирования при равномерном квантовании не отвечает поставленным требованиям, а использование 12-и разрядного кодирования потребует увеличения скорости передачи (или уменьшения объема	
1. Увеличится в 1,5 раза								
2. Уменьшится в 1,5 раза								
3. Не изменится								

средств защиты информации				передаваемой информации) в 12/8 = 1,5 раза.			
		Базовый	Для нормальной работы кодера на его вход должно подаваться неизменное значение сигнала в течение цикла его обработки, что достигается при подаче на вход кодера сигналов..... <table><tr><td>1. АИМ-2</td></tr><tr><td>1. АИМ-1</td></tr><tr><td>3. ИКМ</td></tr></table>	1. АИМ-2	1. АИМ-1	3. ИКМ	1 - Для нормальной работы кодера на его вход должно подаваться неизменное значение сигнала в течение цикла его обработки, что достигается при подаче на вход кодера сигналов постоянного уровня (статических сигналов). Это означает, что входной сигнал должен оставаться неизменным на протяжении всего периода обработки кодером — то есть его амплитуда, форма и другие параметры не должны меняться от начала до конца цикла кодирования, что достигается АИМ-2.
		1. АИМ-2					
1. АИМ-1							
3. ИКМ							
Повышенный	Повышение помехоустойчивости кодирования в канале с шумом достигается введением дополнительной <table><tr><td>1. избыточности</td></tr><tr><td>2. неопределенности</td></tr><tr><td>3. равнозначности</td></tr><tr><td>4. производительности</td></tr></table>	1. избыточности	2. неопределенности	3. равнозначности	4. производительности	1 - В теории кодирования для повышения помехоустойчивости (способности корректно принимать данные при наличии шумов в канале) применяют методы,вводящие избыточность в передаваемое сообщение. Это означает добавление дополнительных битов или символов, которые: • позволяют обнаруживать ошибки; • дают возможность исправлять ошибки без повторной передачи; • повышают надёжность доставки данных.	
1. избыточности							
2. неопределенности							
3. равнозначности							
4. производительности							
	Повышенный	При статистическом кодировании более вероятные сообщения представляются кодовыми словами	1 - При статистическом кодировании более вероятные сообщения представляются				

				1. более короткими 2. более длинными 3. равными 4. произвольными	кодowymi словами меньшей длины. Это ключевой принцип эффективного статистического кодирования (например, кода Хаффмана): • часто встречающиеся символы/сообщения кодируются короткими кодами; • редкие символы/сообщения — более длинными кодами. Такой подход минимизирует среднюю длину кодового слова и обеспечивает оптимальное сжатие данных
				Повышенный Какое количество канальных интервалов используется в цикле ПЦИ: 1.16 2.24 3.30 4.32	4 - Цикл потока Е1 (2048 кбит/с) в плезіохронной цифровой иерархии (ПЦИ) состоит из 32 канальных интервалов, нумеруемых от 0 до 31.
				Высокий Какой алгоритм проверки ошибок используется в синхронной цифровой иерархии? 1. CRC -4 2. ВІР 3. CRC- 16	2 - В синхронной цифровой иерархии (SDH — Synchronous Digital Hierarchy) для проверки ошибок используется код ВІР- (Bit-interleaving Parity — чётность чередующихся бит). Этот метод применяется для обнаружения ошибок на уровне виртуального контейнера (VC)
				Высокий Какой вид канального кодирования используется в плезіохронной цифровой иерархии? 1. CRC -4 2. ВІР	1 - Один из распространённых подходов — применение кодов циклического избыточного контроля (CRC). В европейской

				3. CRC- 16	ветви PDH для проверки базового сигнала E1 рекомендацией ITU-T G.704 определена стандартная функция CRC-4.
--	--	--	--	------------	--

Код и наименование компетенции	Индикатор достижения компетенции	Дисциплина / модуль / практика	Уровень сложности	Задание	Ключ
ПК-5. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-5.1. Знает состав рабочей технической документации, действующие нормативные и методические документы	Б1.В.02.01. Метрология, стандартизация и сертификация	Базовый	При выборе средства измерения температуры производственного помещения 20 ± 3 °C предел допускаемой погрешности измерения следует принять 1) 1,5°C; 2) 3,0°C; 3) 0,5°C; 4) 6,0°C.	1 (Почему не другие варианты? – 0,5 °C — излишне строго (превышает требования для большинства производственных задач). – 3,0 °C и 6,0 °C — недопустимы, так как погрешность превышает допустимое отклонение (± 3 °C), что делает измерения недостоверными.
			Базовый	Источником погрешности не является... 1) примененное средство измерений; 2) примененный метод измерений; 3) отклонение условий выполнения измерений от нормальных; 4) возможное отклонение измеряемой величины.	4 Погрешность — это отклонение результата измерения от истинного значения измеряемой величины. Отклонение измеряемой величины от результата измерения — это само понятие погрешности, а не её источник
			Повышенный	При суммировании составляющих погрешностей измерений принимается допущение, что все составляющие погрешности...	2 При суммировании составляющих погрешностей

				1) имеют нормальное распределение; 2) рассматриваются как случайные величины; 3) суммируются только систематические погрешности; 4) не коррелированы .	измерений принимается допущение, что все составляющие погрешности рассматриваются как случайные величины. Это связано с тем, что погрешности средств измерений в общем случае являются случайными величинами, и для их суммирования необходимо учитывать соответствующие законы распределения.
			Повышенный	Реальная погрешность измерения оценивается ... 1) погрешностью примененного метода; 2) реальную погрешность до выполнения измерений оценить нельзя; 3) суммированием составляющих погрешностей возможных источников; 4) погрешностью средства измерения.	3 Источники погрешностей могут включать: - несовершенство применяемых методов и средств измерений; - непостоянство влияющих на результат измерения физических величин; - индивидуальные особенности экспериментатора; - внешние и внутренние помехи, климатические условия; - порог чувствительности измерительного прибора.

			Повышенный	В основе определения допускаемой погрешности измерения лежит принцип: 1) пренебрежимо малые влияния погрешности измерения на результат измерения; 2) случайности значения отсчёта; 3) погрешности СИ значительно больше других составляющих; 4) реальная погрешность измерений всегда имеет предел.	4 В основе определения допускаемой погрешности измерения лежит принцип существования предела реальной погрешности измерения. Это означает, что любая погрешность имеет конечные границы, которые устанавливаются на основе анализа различных факторов: характеристик средства измерения, метода измерения, условий проведения измерений и других составляющих. На основе этих данных определяется максимально допустимая величина погрешности, которая не должна превышать определённого значения в рамках заданной точности измерений.
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. При измерении физической величины прибором погрешность, возникающая при отклонении температуры среды от нормальной следует назвать как ...	2,3 Погрешность измерения физической величины прибором, возникающую при отклонении температуры среды от нормальной следует рассматривать

				1) относительная; 2) инструментальная; 3) субъективная; 4) методическая.	как: субъективную, инструментальную
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Погрешность измерения размера тонкостенной детали под действием измерительной силы при его контроле является... 1) дополнительная; 2) инструментальная; 3) грубая; 4) методическая	2 Другие варианты ответов (методическая, дополнительная, грубая погрешность) в этом случае не подходят. Методическая погрешность связана с несовершенством метода измерения, дополнительная — с влиянием внешних факторов, не учтённых в стандартной процедуре, а грубая погрешность — с явными ошибками при проведении измерений. Инструментальная погрешность — это составляющая погрешности измерения, которая зависит от погрешностей применяемых средств измерений. В данном случае она связана с влиянием измерительной силы на деталь, что может приводить к её деформации (прогибу) под действием нагрузки.

					Величина такой погрешности определяется по формулам сопротивления материалов, с учётом схемы базирования детали и величины измерительной силы.
ПК-5.2. Умеет применять технологические платформы, сервисы и информационные ресурсы создания технической документации	Б1.В.02.01. Метрология, стандартизация и сертификация	Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Правильность измерений характеризуется... 1) близостью к нулю случайных погрешностей; 2) близостью к нулю систематических погрешностей; 3) отсутствием субъективных погрешностей.		2 Это качественная характеристика измерения, которая определяется тем, насколько близка к нулю величина постоянной или фиксированной изменяющейся при многократных измерениях погрешности (систематической погрешности). Эта характеристика зависит, как правило, от точности средств измерений.
			Повышенный Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Вольтметр с пределами измерений 0...250 В класса точности 0,2 показывает 200 В. Предел допустимой абсолютной погрешности измерения вольтметра равен 1) 0,2 В; 2) 0,5 В; 3) 0,3 В; 4) 0,4 В.		2 $250 * 0,2 / 100 = 0,5$

			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Для измерения температуры до 2500°С следует применить... 1) фотоэлектрический цветовой пирометр; 2) термопары; 3) термоэлектрический термометр ; 4) термометр сопротивления.	2,3 Термопара — устройств о для измерения температуры, основанное на термоэлектрическом эффекте. Состоит из двух проводников разнородных металлов, соединённых на одном конце (измерительном «горячем» спае). Другой конец подключён к схеме обработки сигнала
			Повышенный	Дайте ответ на поставленный вопрос. Стандартизация, участие в которой открыто для национальных органов по стандартизации стран только одного географического, политического или экономического региона – это ...	Региональная стандартизация.
			Повышенный	Дайте ответ на поставленный вопрос. Документ, устанавливающий технические требования, которым должна удовлетворять продукция или услуга, а также процедуры, с помощью которых можно установить, соблюдены ли данные требования – это ...	Технические условия
			Высокий	Дайте ответ на поставленный вопрос. Основные требования к организации производства и оборота продукции на рынке, к методам выполнения различного рода работ, а также методам контроля этих требований в технологических процессах устанавливают	Стандарты на процессы (работы)
	ПК-5.3. Владеет навыками сопровождения	Б1.В.02.01. Метрология,	Базовый	Дайте ответ на поставленный вопрос.	Документ, который принят и устанавливает обязатель

	технической документации	стандартизация и сертификация		Технический регламент (в соответствии с ФЗ «О техническом регулировании») представляет собой...	ные для применения и исполнения требования к объектам технического регулирования.
			Базовый	Дайте ответ на поставленный вопрос. Документ, удостоверяющий соответствие объекта требованиям технических регламентов	Сертификат соответствия
			Повышенный	Дайте ответ на поставленный вопрос. Срок действия сертификата соответствия согласно Федеральному закону «О техническом регулировании» устанавливается...	3 года
			Повышенный	Дайте ответ на поставленный вопрос. Обязательной сертификации подлежат услуги...	-предприятия пищевой промышленности и общественного питания должны соответствовать принципам ХАССП; -гостиницы должны быть сертифицированы для получения категории; -предприятия строительной отрасли обязаны подтвердить уровень качества услуг для получения допусков СРО
			Повышенный	Дайте ответ на поставленный вопрос. Совокупность правил выполнения работ по сертификации, её участников, и условий функционирования в целом называется...	Система сертификации
			Высокий	Дайте ответ на поставленный вопрос. Обязательной сертификации подлежат:	В России обязательной сертификации подлежит продукция, которая

					может быть опасной для жизни и здоровья
			Высокий	Дайте ответ на поставленный вопрос. Процесс измерения представляет собой...	Процесс, заключающийся в сравнении опытным путём измеряемой физической величины с её единицей, принятой за основу для получения количественной информации о характеристиках объектов, явлений или процессов.

Код и наименование компетенции	Индикатор достижения компетенции	Дисциплина / модуль / практика	Уровень сложности	Задание	Ключ
ПК-7. Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-7.1. Знает требования стандартов в области информационной безопасности	Б1.В.02.03. Основы электромагнитной совместимости	Базовый	Что такое электромагнитная совместимость (ЭМС)? 1) Отсутствие любых электромагнитных полей вокруг устройства 2) Процесс экранирования всех узлов прибора 3) Способность устройства работать только в идеальных условиях 4) Способность технического средства функционировать с заданным качеством в электромагнитной обстановке, не создавая недопустимых помех другим устройствам	4) – ЭМС — это способность оборудования работать эффективно в реальной электромагнитной среде, не создавая помех другим и не подвергаясь недопустимому влиянию с их стороны
			Базовый	Какие виды помех выделяют по характеру возникновения? 1) Гармонические 2) Естественные и искусственные 3) Низкочастотные и высокочастотные 4) Синфазные и дифференциальные	2) – По происхождению помехи делятся на естественные (атмосферные, космические) и искусственные (индустриальные, от других устройств)

			Повышенный	Согласно стандартам ЭМС, помехи подразделяются на: 1) Кондуктивные и излучаемые 2) Статические и динамические 3) Только излучаемые 4) Только кондуктивные	1) – По способу распространения помехи делятся на кондуктивные (распространяющиеся по проводам) и излучаемые (распространяющиеся через пространство в виде электромагнитного поля)
			Повышенный	Какой элемент чаще всего является источником кондуктивных помех в импульсных источниках питания? 1) Выпрямительный диод 2) Высокочастотный трансформатор 3) Входной предохранитель 4) Ключевые транзисторы 5) Сетевой разъем	2), 4) – Ключевые транзисторы и трансформаторы коммутируют большие токи на высокой частоте, создавая импульсные помехи в цепях питания
			Повышенный	Как называются помехи, распространяющиеся по проводам за счёт разности потенциалов между сигнальным и обратным проводом? 1) Дифференциальные 2) Естественные 3) Общие 4) Синфазные	1) – Дифференциальная помеха действует между двумя проводами линии (сигнал-земля или фаза-ноль) и приложена последовательно полезному сигналу
			Высокий	Какая проблема электромагнитной совместимости характерна для высокоскоростных цифровых устройств? 1) Дребезг контактов 2) Излучение на гармониках тактовой частоты до нескольких сотен МГц 3) Перегрев транзисторов 4) Синфазные помехи на частоте 50 Гц	2) – Короткие фронты импульсов создают широкий спектр гармоник, которые могут излучаться даже цепями, не предназначенными для ВЧ
			Высокий	Рекомендация по уменьшению излучения от печатной платы: 1) Минимизировать площадь контуров обратного тока 2) Использовать только одностороннюю плату	1) – Чем меньше площадь петли обратного тока, тем меньше излучение согласно закону

				3) Увеличить расстояние между слоями 4) Применять самые толстые проводники	электромагнитной индукции
	ПК-7.2. Умеет создавать и вести справочный ресурс для анализа информационной безопасности объектов	Б1.В.02.03. Основы электромагнитной совместимости	Базовый	Что такое помехоустойчивость технического средства? 1) Высокое сопротивление изоляции 2) Обязательное наличие заземления 3) Способность устройства не создавать помехи 4) Способность работать без ухудшения качества при воздействии электромагнитной помехи заданного уровня	4) – Помехоустойчивость — свойство устройства сохранять работоспособность при воздействии внешних электромагнитных возмущений
			Повышенный	Синфазная помеха — это: 1) Помеха, вызванная только атмосферными разрядами 2) Помеха, действующая одинаково относительно земли на всех проводах линии 3) Помеха между корпусом и землёй 4) Помеха между фазным и нулевым проводом	2) – Синфазная помеха — это напряжение, присутствующее одинаково на всех сигнальных проводах по отношению к общему заземлению
			Повышенный	Какой канал связи для помех является основным на частотах выше 30 МГц? 1) Гальванический 2) Емкостный 3) Индуктивный 4) Электромагнитное излучение	4) – На ВЧ преобладает излучение электромагнитного поля, длина волны соизмерима с размерами проводников, и помехи распространяются как радиоволны
			Повышенный	Какое явление описывает передачу помехи через паразитную ёмкость между двумя проводниками? 1) Гальваническая связь 2) Емкостная связь 3) Импедансная связь 4) Индуктивная связь	2) – Емкостная связь обусловлена наличием паразитной ёмкости, через которую переменное напряжение одного проводника наводит ток в другом
			Повышенный	Что такое предельно допустимый уровень помехи? 1) Максимальный уровень помехи, при котором устройство ещё работает 2) Мощность собственного шума устройства	3) – Предельный уровень — это норматив, устанавливаемый стандартами. Превышение означает

				3) Нормированное значение напряжения или напряжённости поля, которое не должно превышать в заданных условиях 4) Уровень, при котором устройство отключается защитой	несоответствие требованиям ЭМС
			Высокий	Что из перечисленного не относится к методам обеспечения ЭМС на системном уровне? 1) Правильное разделение цепей питания аналоговой и цифровой частей 2) Увеличение тактовой частоты процессора без изменения схемотехники 3) Фильтрация на входах/выходах кабелей 4) Функциональное разделение блоков с разным уровнем помех	2) – Простое повышение тактовой частоты без оптимизации разводки и фильтрации ухудшает ЭМС, увеличивая эмиссию помех
	ПК-7.3. Владеет навыками подготовки технических отчетов по информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Б1.В.02.03. Основы электромагнитной совместимости	Базовый	Основное назначение ферритового фильтра (ферритовой защёлки) на кабеле: 1) Защита от статического электричества 2) Подавление синфазных помех на частотах выше 10 МГц 3) Увеличение прочности кабеля 4) Уменьшение сопротивления кабеля	2) – Феррит создаёт высокое сопротивление для синфазных ВЧ токов, не влияя на полезные дифференциальные сигналы
			Базовый	Какой вид экранирования наиболее эффективен против магнитных полей низкой частоты (50 Гц)? 1) Алюминиевая фольга 2) Медная сетка 3) Пермаллой или толстая сталь 4) Полимерное покрытие	3) – Для экранирования низкочастотных магнитных полей требуются материалы с высокой магнитной проницаемостью
			Повышенный	Принцип работы экрана электростатического поля основан на: 1) Замыкании силовых линий на корпус и отводе тока на землю 2) Изменении частоты падающей электромагнитной волны 3) Отражении электромагнитной волны 4) Поглощении энергии электромагнитных волн	1) – Проводящий экран замыкает на себя электростатическое поле, и заряд стекает на землю, не проникая внутрь
			Повышенный	Какой стандарт регламентирует устойчивость к электростатическому разряду? 1) IEC 61000-4-2	1) – IEC 61000-4-2 описывает методы испытаний и уровни

				2) CISPR 22 3) IEC 61000-3-2 4) IEC 61000-4-4	устойчивости к электростатическим разрядам.
			Повышенный	Для измерения помех, излучаемых шлейфом кабеля, без разрыва цепи применяют: 1) Токовые клещи 2) Измерительные антенны 3) Датчик Холла 4) Анализатор спектра	1) – Токовые клещи измеряют синфазный ток на кабелях без гальванического контакта
			Высокий	Что такое «перекрестные помехи» на печатной плате? 1) Помехи по цепи питания 2) Наводка сигнала с одной дорожки на другую из-за взаимной ёмкости и индуктивности 3) Синфазные помехи 4) Помеха от радиопередатчиков	2) – Перекрёстные помехи возникают между близко расположенными параллельными проводниками через ёмкостную и/или индуктивную связь
			Высокий	Для уменьшения перекрестных помех между сигнальными линиями следует: 1) Увеличить длину параллельного прохождения 2) Увеличить расстояние между линиями 3) ввести заземлённый проводник между ними 4) Повысить частоту сигнала 5) Снизить напряжение питания	2), 3) – Увеличение расстояния и добавление заземлённого проводника снижают паразитную связь между сигнальными линиями

Код и наименование компетенции	Индикатор достижения компетенции	Дисциплина / модуль / практика	Уровень сложности	Задание	Ключ
ПК-8. Способен проводить исследования на побочные электромагнитные излучения и наводки технических средств обработки	ПК-8.1. Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации	Б1.О.06.02. Распространение электромагнитных волн и антенно-фидерные устройства	Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Декаметровым волнам соответствуют какие границы диапазона длин волн? 1) 1000 - 100 м; 2) 100 - 10 м; 1) 10 - 1 км; 1) 10 - 1 м;	2 – В соответствии с Регламентом радиосвязи

информации, защищенности акустической речевой информации от утечки по техническим каналам	ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом «высокочастотного облучения» основных технических средств и систем и за счет возможно внедренных электронных		Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какой слой атмосферы над поверхностью Земли самый нижний? 1) Тропосфера; 2) Стратосфера; 3) Ионосфера; 4) Мезосфера;	1 – Нижняя граница тропосферы находится на поверхности Земли
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. В каком радиочастотном диапазоне земная поверхность по своим свойствам близка к проводнику? 1) УКВ; 2) КВ; 3) СВ; 4) ДВ;	4 – С уменьшением частоты колебаний отношение тока проводимости к току смещения растет
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Чем определяются потери мощности сигнала на приеме при распространении радиоволны в свободном пространстве? 1) Сферическими расхождениями фронта волны; 2) Рассеянием на неоднородностях среды; 3) Поглощением в среде; 4) Дифракцией при распространении;	1 – Свободное пространство соответствует однородной среде без поглощения (например, вакуум)
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Как называются радиоволны, распространяющиеся вдоль земной поверхности и частично огибающие выпуклость земного шара из-за дифракции? 1) Ионосферными; 2) Прямыми; 3) Земными; 4) Тропосферными;	3 – Основная часть энергии волны распространяется в приповерхностном слое Земли в атмосфере с характерным поперечным размером, малым по сравнению с расстоянием вдоль слоя от передатчика до приемника
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа.	2 – Для диапазонов СВ и ДВ расчет надо вести в приближении низко

	устройств перехвата информации в основных технических средствах и системах			С помощью каких формул можно рассчитать напряженность поля радиоволны в диапазонах СВ и ДВ в зоне приближения плоской Земли? 1) Интерференционной трактовки влияния Земли на отражение падающей волны; 2) Шулейкина-Ван-дер-Поля; 3) Для распространения в свободном пространстве; 4) Введенского;	поднятых антенн над поверхностью Земли
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. На каких длинах волн надо учитывать поглощение энергии радиоволн в гидрометеорах? 1) более 6 см; 2) менее 5 см; 3) менее 15 см; 4) более 20 см;	2 – Эффективное рассеяние дают неоднородности атмосферы, размеры которых много больше длины волны и радиуса первой зоны Френеля
	ПК-8.2. Умеет проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; проводить оценку защищенности информации от утечки за счет побочных электромагнитных излучений и наводок	Б1.О.06.02. Распространение электромагнитных волн и антенно-фидерные устройства	Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. При каком из процессов происходит самое значительное уменьшение уровня сигнала? 1) Дефокусировка волнового пучка; 2) Отражение от Земли; 3) Рефракция радиоволн; в плавно неоднородной среде 4) Рассеяние радиоволн на неоднородностях электронной концентрации;	1 – Быстро протекающий процесс резкой перестройки волнового фронта приводит к значительному уменьшению амплитуды колебаний
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. В каком радиочастотном диапазоне земная поверхность по своим свойствам близка к диэлектрику? 1) УКВ; 2) КВ; 3) СВ; 4) ДВ;	1 - С уменьшением частоты колебаний отношение тока проводимости к току смещения растёт
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. В каком диапазоне наблюдается дальнее тропосферное распространение радиоволн? 1) УКВ;	1 - Эффективное рассеяние дают неоднородности атмосферы, размеры которых много больше

				2) КВ; 3) СВ; 4) ДВ;	длины волны и радиуса первой зоны Френеля
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какую функцию выполняет объемный резонатор в цепях сверхвысоких частот? 1) Активного распределенного сопротивления; 2) Резонансной колебательной системы с распределенными параметрами; 3) Емкостного распределенного сопротивления; 4) Индуктивного распределенного сопротивления;	2 – На эквивалентной схеме резонатору соответствует колебательный контур
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какова структура поля электромагнитной волны от системы токов в дальней зоне? 1) поперечная волна; 2) продольная волна; 3) всегда линейная поляризация; 4) всегда есть фазовый центр излучения у системы токов;	1 – Интегрирование уравнения Гельмгольца, например методом функций Грина, дает этот результат
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. При дальнем тропосферном распространении уровень поля в точке приема в какой сезон года больше? 1) Зимой; 2) Весной; 3) Летом; 4) Осенью;	3 – Летом значения функции ионизации нейтральной атмосферы ультрафиолетовым и рентгеновским и излучением Солнца наиболее высокие. Поэтому интенсивность рассеяния радиоволн наибольшая.
	ПК-8.3. Владеет навыками проведения контроля защищенности информации от утечки за счет побочных электромагнитных	Б1.О.06.02. Распространение электромагнитных волн и антенно-фидерные устройства	Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Сколько составляет приблизительно длительность кругосветного эха? 1) 1,3 с; 2) 0,13 с; 3) 1,3 мс; 4) 13 с;	2 – Получается делением длины дуги большого круга шара с радиусом Земли на скорость света

	излучений и наводок; подготовки отчетных материалов по результатам контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок (протоколов оценки защищенности информации от утечки за счет побочных электромагнитных излучений и наводок)		Базовый	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. На каких высотах над поверхностью Земли располагается F₂ слой ионосферы? 1) 60...80; 2) 80...90; 3) 90...120; 4) 250...450;	4 – Высота положения максимума F ₂ слоя ионосферы зависит от геофизических условий
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какая конфигурация электрического тока и электромагнитного поля в направляющей системе при распространении Т волны? 1) С только продольным током; 2) С продольной составляющей у электрического поля волны; 3) С продольной составляющей у магнитного поля волны; 4) С только поперечным током;	1 – Поперечная электромагнитная волна без частотной дисперсии
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какая конфигурация электрического тока и электромагнитного поля в направляющей системе при распространении Н волны? 1) С только продольным током; 2) С продольной составляющей у электрического поля волны; 3) С продольной составляющей у магнитного поля волны; 4) С только поперечным током;	3 - Электромагнитная волна с продольной составляющей магнитного поля и частотной дисперсией
			Повышенный	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Какая конфигурация электрического тока и электромагнитного поля в направляющей системе при распространении Е волны? 1) С только продольным током; 2) С продольной составляющей у электрического поля волны; 3) С продольной составляющей у магнитного поля волны; 4) С только поперечным током;	2 - Электромагнитная волна с продольной составляющей электрического поля и частотной дисперсией

			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. По какому закону дифракционная компонента поля земной волны затухает с расстоянием в зоне тени? 1) Линейному; 2) Квадратичному; 3) Экспоненциальному; 4) Гармоническому;	3 – Дифракционная формула Фока для поля земной волны
			Высокий	Прочитайте текст и выберите правильный ответ и запишите аргумент, обосновывающий выбор ответа. Как правильно прорезать щель, слабо возмущающую поле в волноводе прямоугольного сечения, по которому распространяется волна H_{10}? 1) узкая поперечная щель в середине узкой стенки волновода; 2) узкая продольная щель в середине широкой стенки волновода; 3) узкая поперечная щель в середине широкой стенки волновода; 4) Узкая продольная щель в середине узкой стенки волновода;	2 – Щель должна слабо нарушать токи в стенке волновода