

**КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность: 10.05.01 Компьютерная безопасность

Специализация: «Разработка защищенного программного обеспечения»

Формы обучения: очная

Объем дисциплины:

в зачетных единицах: 3 з.е.

в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

Оценочные материалы по дисциплине **Физические основы защиты информации**

обсуждены и рекомендованы к утверждению решением кафедры гуманитарных дисциплин и иностранных языков от 21 марта 2025 г., протокол № 7

одобрены Научно-методическим советом Казанского кооперативного института (филиала) от «2» апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Паспорт оценочных материалов по дисциплине
2. Оценочные материалы по дисциплине:
 - 2.1. Оценочные материалы для проведения текущего контроля.
 - 2.2. Оценочные материалы для проведения промежуточной аттестации.

Обновление оценочных материалов дисциплины

Целью оценочных материалов по дисциплине (модулю) (далее –ОМ) является комплексная оценка результатов обучения по дисциплине Физические основы защиты информации и установление уровня сформированности компетенций обучающегося.

ОМ предназначены для проведения текущего контроля успеваемости и промежуточной аттестации.

ОМ включают оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации.

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины Физические основы защиты информации.

1. Паспорт оценочных материалов по дисциплине «Физические основы защиты информации»

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства ¹	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
ПК-3.4 Способен анализировать уязвимости и угрозы информационной безопасности в компьютерных системах и сетях	ПК-3.4.1 Анализирует компьютерную систему с целью определения уровня защищённости и доверия	Знать: основные концепции и стандарты информационной безопасности, типы угроз и уязвимостей компьютерных систем, а также методы их выявления и классификации, методологии и инструменты для оценки уровня защищённости и доверия компьютерных систем. Уметь: идентифицировать компоненты компьютерной системы, подлежащие анализу, проводить анализ рисков для компьютерной системы, выявлять уязвимости и определять потенциальные угрозы, использовать специализированные инструменты и программное обеспечение для сканирования, тестирования и анализа безопасности компьютерных систем.	Тема 1. Поля объектов и проблема защиты информации. Тема 2. Поля объектов и проблема защиты информации. Основные свойства и параметры волн различной природы и различных частотных диапазонов при распространении в идеальных и реальных средах, способы и устройства возбуждения и приема волн Тема 3. Электрические, магнитные и электромагнитные поля объектов. Электромагнитные волны, их характеристики, свойства и особенности распространения в различных средах Тема 4. Модели управления доступом к информации. Модели поддержания целостности информации. Тема 5. Электрические, магнитные и электромагнитные поля объектов.	Реферат (Тема 1-8) Тест (тема 1-8) Домашние задания по практическим занятиям (тема 1-8)	Тест (П 1-10 тестового задания)

		Владеть: навыками применения методов и инструментов анализа защищённости компьютерных систем, навыками выявления, оценки и классификации угроз и уязвимостей компьютерных систем, навыками разработки и реализации рекомендаций по повышению уровня защищённости и доверия компьютерных систем.	Принципы экранирования статических и динамических полей Тема 6. Упругие волны, их характеристики. Основы акустики речи и слуха. Тема 7. Упругие волны, их характеристики. Специфика акустики помещений, Звукоизоляция. Тема 8. Упругие волны, их характеристики. Инфразвук, ультразвук.		
	ПК-3.4.2 Демонстрирует умение проводить анализ безопасности компоненты программно-аппаратных средств защиты информации в компьютерных системах	Знать: основные подходы и методики анализа безопасности компонентов программных и программно-аппаратных средств защиты информации, типовые виды атак и сценарии компрометации компонент защитных механизмов, методы верификации и аттестации средств защиты информации, современные средства и технологии мониторинга и аудита безопасности компонент защиты информации. Уметь: проводить детальное исследование функциональности и архитектуры компонент программных и аппаратных средств защиты информации,	Тема 1. Поля объектов и проблема защиты информации. Тема 2. Поля объектов и проблема защиты информации. Основные свойства и параметры волн различной природы и различных частотных диапазонов при распространении в идеальных и реальных средах, способы и устройства возбуждения и приема волн Тема 3. Электрические, магнитные и электромагнитные поля объектов. Электромагнитные волны, их характеристики, свойства и особенности распространения в различных средах Тема 4. Модели управления доступом к информации.	Реферат (Тема 1-8) Тест (тема 1-8) Домашние задания по практическим занятиям (тема 1-8)	Тест (П 11-20 тестового задания)

		выявлять возможные уязвимости и слабые места в компонентах защитной инфраструктуры, оценивать эффективность используемых средств защиты и степень соответствия установленным требованиям и стандартам. Владеть: навыками практической работы с современными инструментами и методами анализа безопасности программных и аппаратных решений, способностью разрабатывать рекомендации по устранению выявленных недостатков и оптимизации настроек существующих средств защиты, методиками документального оформления результатов анализа и оценивания степени риска для автоматизированных систем обработки информации.	Модели поддержания целостности информации. Тема 5. Электрические, магнитные и электромагнитные поля объектов. Принципы экранирования статических и динамических полей Тема 6. Упругие волны, их характеристики. Основы акустики речи и слуха. Тема 7. Упругие волны, их характеристики. Специфика акустики помещений, Звукоизоляция. Тема 8. Упругие волны, их характеристики. Инфразвук, ультразвук.		
	ПК-3.4.3. Формирует предложения по устранению выявленных уязвимостей	Знать: основные подходы и принципы устранения уязвимостей программного и аппаратного обеспечения, рекомендации по выбору оптимальных способов нейтрализации выявленных слабых мест, законодательные требования и регламенты,	Тема 1. Поля объектов и проблема защиты информации. Тема 2. Поля объектов и проблема защиты информации. Основные свойства и параметры волн различной природы и различных частотных диапазонов при распространении в	Реферат (Тема 1-8) Тест (тема 1-8) Домашние задания по практическим занятиям (тема 1-8)	Тест (П 21-30 тестового задания)

		регламентирующие процесс исправления дефектов и повышение уровня защищенности информационных ресурсов. Уметь: анализировать выявленные уязвимости и оценивать их критичность для функционирования системы, определять наиболее эффективные пути ликвидации выявленных проблем и предотвращения возможных инцидентов, составлять аргументированные предложения по модернизации существующей системы защиты. Владеть: навыками разработки конкретных мероприятий по устранению выявленных уязвимостей, умениями формулировать конкретные рекомендации и технические задания на устранение найденных дефектов, наличием опыта управления проектами по улучшению уровня защиты ИТ-инфраструктуры организаций.	идеальных и реальных средах, способы и устройства возбуждения и приема волн Тема 3. Электрические, магнитные и электромагнитные поля объектов. Электромагнитные волны, их характеристики, свойства и особенности распространения в различных средах Тема 4. Модели управления доступом к информации. Модели поддержания целостности информации. Тема 5. Электрические, магнитные и электромагнитные поля объектов. Принципы экранирования статических и динамических полей Тема 6. Упругие волны, их характеристики. Основы акустики речи и слуха. Тема 7. Упругие волны, их характеристики. Специфика акустики помещений, Звукоизоляция. Тема 8. Упругие волны, их характеристики. Инфразвук, ультразвук.	
--	--	--	--	--

2. Оценочные материалы по дисциплине «Физические основы защиты информации»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема 1. Поля объектов и проблема защиты информации

1. Классификация и анализ современных хранилищ конфиденциальной информации: от баз данных до облачных архивов. (Сравнительный анализ рисков и мер защиты)
2. Уязвимости технических средств обработки информации: компьютеры, серверы и мобильные устройства как объекты защиты. (Анализ каналов утечки и методов противодействия)
3. Обеспечение безопасности помещений и территорий с ограниченным доступом: физические и технические аспекты.
4. Архитектура защищенных информационных систем: принципы построения и управления.
5. Проблема защиты информации в распределенных системах и больших данных (Big Data).
6. Мобильные устройства как ключевой объект защиты в современной корпоративной среде.
7. Методы и средства защиты серверного оборудования в дата-центрах.
8. Анализ угроз безопасности информации на уровне сетевой инфраструктуры.
9. Роль организационных мер в защите помещений с циркуляцией конфиденциальной информации.
10. Сравнительный анализ отечественных и зарубежных требований к защите информационных систем.
11. Защита информации в системах "умный дом" и "интернета вещей" (IoT).

Тема 2. Поля объектов и проблема защиты информации. Основные свойства и параметры волн

1. Система информационной безопасности как комплексная дисциплина: структура и основные компоненты.
2. Таксономия угроз информационной безопасности: современная классификация и примеры.
3. Сферы защиты информации: анализ правовой, технической и организационной составляющих.
4. Физические основы распространения волн различной природы в контексте задач защиты информации.
5. Способы и устройства возбуждения и приема электромагнитных волн для целей разведки и защиты.
6. Особенности распространения волн в реальных средах (городская

- застройка, помещения) и их влияние на безопасность.
7. Объекты защиты: от материальных предметов до виртуальных явлений в киберпространстве.
 8. Частотные диапазоны волн и их использование в технических каналах утечки информации.
 9. Моделирование угроз на основе анализа параметров и свойств различных типов волн.
 10. Роль человеческого фактора как объекта и субъекта защиты в современной системе ИБ.

Тема 3. Электрические, магнитные и электромагнитные поля объектов

1. Физическая природа и характеристики электрических и магнитных полей технических средств.
2. Электромагнитные волны: основные характеристики, свойства и механизмы распространения.
3. Особенности распространения электромагнитных полей в различных средах (вакуум, атмосфера, строительные материалы).
4. Визуализация полей: понятие и практическое значение силовых линий электрического поля.
5. Электрический потенциал как ключевая характеристика и его роль в образовании наводок.
6. Методы расчета и измерения параметров электромагнитных полей вокруг технических средств.
7. Побочные электромагнитные излучения и наводки (ПЭМИН) как основной канал утечки информации.
8. Сравнительный анализ характеристик статических и динамических электрических полей.
9. Влияние геометрии и материалов объекта на структуру создаваемого им электромагнитного поля.
10. Практическое применение знаний о полях для поиска и ликвидации каналов утечки информации.

Тема 4. Модели управления доступом и поддержания целостности информации

1. Эволюция моделей управления доступом: от мандатной модели до моделей на основе ролей (RBAC).
2. Дискреционное управление доступом (DAC): принципы, преимущества и недостатки.
3. Мандатное управление доступом (MAC): строгая политика безопасности и ее реализация.
4. Модели поддержания целостности информации: от модели Белла-ЛаПадулы до Кларка-Вильсона.
5. Криптографические методы контроля целостности: хеш-функции и их стойкость.

6. Имитовставка (MAC - Message Authentication Code) как средство обеспечения целостности и аутентичности.
7. Электронная цифровая подпись (ЭЦП): правовые основы, алгоритмы и области применения.
8. Контрольные суммы и избыточное кодирование в системах обнаружения и исправления ошибок.
9. Технологии резервного копирования и создания полных копий данных для обеспечения доступности и целостности.
10. Практическая реализация моделей целостности в современных операционных системах и СУБД.
11. Сравнительный анализ алгоритмов хеширования (MD5, SHA-1, SHA-2, SHA-3) с точки зрения стойкости и производительности.

Тема 5. Принципы экранирования статических и динамических полей

1. Физические принципы экранирования электрических, магнитных и электромагнитных полей.
2. Источники электромагнитных полей (ЭМП) в современной техносфере и их характеристика.
3. Нормирование электромагнитных полей: санитарно-гигиенические аспекты и требования ГОСТ 12.1.002-84.
4. Методы и средства защиты от электромагнитных излучений: пассивные и активные способы.
5. Особенности экранирования статических (постоянных) магнитных полей.
6. Экранирование динамических (переменных) полей и высокочастотных излучений.
7. Материалы для электромагнитного экранирования и их эффективность в различных частотных диапазонах.
8. Конструктивные методы защиты технических средств от ПЭМИН.
9. Расчет и проектирование экранированных помещений (клеток Фарадея).
10. Практическое применение экранирования в защищенной аппаратуре и критически важных объектах.
11. Актуальность требований ГОСТ 12.1.002-84 в условиях современной электромагнитной обстановки.

Тема 6. Упругие волны, их характеристики. Основы акустики речи и слуха

1. Физика упругих волн: общая классификация и фундаментальные характеристики.
2. Особенности распространения упругих волн в твердых телах: продольные и поперечные волны.
3. Практическое применение упругих волн в технике и технологиях (дефектоскопия, медицина, геолокация).
4. Акустика речи: физиологические и физические основы формирования

речевого сигнала.

5. Психоакустика и механизмы слухового восприятия человека.
6. Модели речевого сигнала и их использование в системах записи, передачи и распознавания речи.
7. Частотный и динамический диапазон речевого сигнала и слухового восприятия.
8. Акустические каналы утечки речевой информации и методы их перехвата.
9. Использование ультразвука для скрытной передачи данных (акустический кибершпионаж).
10. Методы защиты речевой информации от утечки по акустическому каналу.

Тема 7. Упругие волны, их характеристики. Специфика акустики помещений

1. Специфика распространения звука в замкнутых пространствах: эффект комнаты и реверберация.
2. Критическое расстояние в акустике помещений: определение, расчет и практическое значение.
3. Правило третей и другие принципы оптимального размещения источников звука и микрофонов.
4. Спектральные искажения звукового сигнала в помещении и их влияние на разборчивость речи.
5. Методы и материалы звукоизоляции ограждающих конструкций.
6. Звукопоглощение и акустическая обработка помещений для защиты конфиденциальных переговоров.
7. Расчет времени реверберации и его оптимизация для задач обеспечения акустической безопасности.
8. Использование активных систем шумоподавления в защищаемых помещениях.
9. Акустический дизайн переговорных комнат и залов совещаний с точки зрения защиты информации.
10. Современные стандарты и требования к акустической безопасности помещений.

Тема 8. Упругие волны, их характеристики. Инфразвук, ультразвук. Обзор DLP-систем

1. Инфразвук и ультразвук: физические свойства, особенности генерации и распространения.
2. Практическое применение инфразвука и ультразвука в науке, технике и медицине.
3. Воздействие инфразвука и ультразвука на человека и технические системы.
4. Классификация уязвимостей информационных систем: таксономия CWE, OWASP Top 10.

5. Разбор реального примера уязвимости (на выбор: Heartbleed, Shellshock, EternalBlue) и методика ее эксплуатации.
6. Методология гипотетического дефекта (Hypothetical Defect Methodology) в прогнозировании уязвимостей.
7. Системы предотвращения утечек информации (DLP): архитектура, принципы работы и обзор рынка.
8. Сравнительный анализ ведущих DLP-систем (Symantec, McAfee, Digital Guardian, InfoWatch).
9. Методы обнаружения и блокирования утечек по сетевым, почтовым и периферийным каналам.
10. Интеграция DLP-систем в комплексную систему безопасности организации.
11. Юридические и этические аспекты использования DLP-систем для мониторинга сотрудников.

Критерии оценки выполнения рефератов по учебной дисциплине

Оценка «отлично» выставляется студенту, если тема реферата раскрыта в полной мере и все требования по написанию реферата соблюдены.

Оценка «хорошо» выставляется студенту, если недостаточно раскрыта тема реферата, но все требования по написанию реферата соблюдены.

Оценка «удовлетворительно» выставляется студенту, если недостаточно раскрыта тема реферата, не все требования по написанию реферата соблюдены, присутствуют ошибки и неточности в работе.

Оценка «неудовлетворительно» выставляется студенту, если отсутствует реферат.

Рекомендации по написанию реферата:

Реферат — письменная работа, выполняемая обучающимся в течение определенного срока.

Реферат — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу.

Реферат отвечает на вопрос — что содержится в данной публикации (публикациях). Реферат — не механический пересказ работы, а изложение ее сущности.

Кроме реферирования прочитанной литературы, от обучающегося требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата предлагает преподаватель или сам обучающийся, в последнем случае она должна быть согласована с преподавателем.

В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или

описания.

Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.

Структура реферата:

1. Титульный лист.
2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы.
4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифрой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал.
5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении.
6. Приложение может включать графики, таблицы, расчеты.
7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания.

Этапы работы над рефератом.

Работу над рефератом можно условно подразделить на три этапа:

1. Подготовительный этап, включающий изучение предмета исследования;
 2. Изложение результатов изучения в виде связного текста;
 3. Устное сообщение по теме реферата.
1. Подготовительный этап работы.

Формулировка темы. Подготовительная работа над рефератом начинается с формулировки темы. Тема в концентрированном виде выражает содержание будущего текста, фиксируя как предмет исследования, так и его ожидаемый результат. Для того чтобы работа над рефератом была успешной, необходимо, чтобы тема заключала в себе проблему, скрытый вопрос (даже если наука уже давно дала ответ на этот вопрос, студент, только знакомящийся с соответствующей областью знаний, будет вынужден искать ответ заново, что даст толчок к развитию проблемного, исследовательского мышления).

Поиск источников. Грамотно сформулированная тема зафиксировала предмет изучения; задача обучающегося — найти информацию, относящуюся к данному предмету и разрешить поставленную проблему. Выполнение этой задачи начинается с поиска источников. На этом этапе необходимо вспомнить,

как работать с энциклопедиями и энциклопедическими словарями.

Работа с источниками. Работу с источниками надо начинать с ознакомительного чтения, т. е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции — это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Создание конспектов для написания реферата.

Подготовительный этап работы завершается созданием конспектов, фиксирующих основные тезисы и аргументы. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы).

По завершении предварительного этапа можно переходить непосредственно к созданию текста реферата.

2. Создание текста.

Общие требования к тексту.

Текст реферата должен подчиняться определенным требованиям: он должен раскрывать тему, обладать связностью и цельностью.

Раскрытие темы предполагает, что в тексте реферата излагается относящийся к теме материал и предлагаются пути решения содержащейся в теме проблемы; связность текста предполагает смысловую соотносительность отдельных компонентов, а цельность - смысловую законченность текста.

С точки зрения связности все тексты делятся на тексты-констатации и тексты-рассуждения. Тексты-констатации содержат результаты ознакомления с предметом и фиксируют устойчивые и несомненные суждения. В текстах-

рассуждениях одни мысли извлекаются из других, некоторые ставятся под сомнение, дается им оценка, выдвигаются различные предположения.

План реферата.

Универсальный план реферата – введение, основной текст и заключение.

Требования к введению.

Во введении аргументируется актуальность исследования, - т. е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками; перечисляются положения, которые должны быть обоснованы. Введение может также содержать обзор источников или экспериментальных данных, уточнение исходных понятий и терминов, сведения о методах исследования. Во введении обязательно формулируются цель и задачи реферата.

Объем введения - в среднем около 10% от общего объема реферата.

Основная часть реферата.

Основная часть реферата раскрывает содержание темы. Она наиболее значительна по объему, наиболее значима и ответственна. В ней обосновываются основные тезисы реферата, приводятся развернутые аргументы, предполагаются гипотезы, касающиеся существа обсуждаемого вопроса. Важно проследить, чтобы основная часть не имела форму монолога. Аргументируя собственную позицию, можно и должно анализировать, и оценивать позиции различных исследователей, с чем-то соглашаться, чему-то возражать, кого-то опровергать. Текст основной части делится на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала: классификации (эмпирические исследования), типологии (теоретические исследования), периодизации (исторические исследования).

Заключение.

Заключение — последняя часть научного текста. В ней краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования. Здесь же могут намечаться и дальнейшие перспективы развития темы. Небольшое по объему сообщение также не может обойтись без заключительной части - пусть это будут две-три фразы. Но в них должен подводиться итог проделанной работы.

Список использованной литературы.

Реферат любого уровня сложности обязательно сопровождается списком используемой литературы. Названия книг в списке располагают по алфавиту с указанием выходных данных использованных книг.

Требования, предъявляемые к оформлению реферата

Объемы рефератов – от 10-18 машинописных страниц. Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 35 мм. слева и 15 мм. справа, рекомендуется шрифт 12-14, интервал - 1,5. Все листы реферата должны быть пронумерованы. Каждый вопрос в тексте должен иметь заголовок в точном соответствии с наименованием в плане-оглавлении. При написании и оформлении реферата следует избегать типичных ошибок, например, таких:

– поверхностное изложение основных теоретических вопросов выбранной темы, когда автор не понимает, какие проблемы в тексте являются главными, а какие второстепенными,

– в некоторых случаях проблемы, рассматриваемые в разделах, не раскрывают основных аспектов выбранной для реферата темы,

– дословное переписывание книг, статей, заимствования рефератов из интернета и т. д.

При проверке реферата преподавателем оцениваются:

1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.

2. Характеристика реализации цели и задач исследования (новизна и актуальность поставленных в реферате проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).

3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).

4. Качество и ценность полученных результатов (степень завершенности реферативного исследования, спорность или однозначность выводов).

5. Использование литературных источников.

6. Культура письменного изложения материала.

7. Культура оформления материалов работы.

Комплект типовых домашних заданий по практическим занятиям

Тема 1. Объектно- ориентированный подход к программированию.

Тема 1. Поля объектов и проблема защиты информации

Задание 1.1: Инвентаризация информационных активов организации

Цель: Составить реестр объектов защиты и оценить их уязвимость

- Проведите аудит типовой организации (на примере учебного заведения или офиса)
- Классифицируйте объекты защиты:
 - Информационные системы и базы данных
 - Технические средства (серверы, компьютеры, сетевые устройства)
 - Мобильные устройства и носители информации
 - Помещения с ограниченным доступом
- Для каждого объекта определите:
 - Категорию конфиденциальности

- Потенциальные угрозы
- Существующие меры защиты
- **Отчет:** таблица инвентаризации, диаграмма рисков, рекомендации

Задание 1.2: Разработка модели угроз для хранилища данных

Цель: Построить комплексную модель угроз для системы хранения информации

- Выберите объект исследования (архив документов, база данных, облачное хранилище)
- Проведите анализ по методике OCTAVE или STRIDE:
 - Идентификация активов и уязвимостей
 - Оценка вероятности и воздействия угроз
 - Расчет уровня риска
- Разработайте матрицу угроз и карту рисков
- Предложите меры по минимизации выявленных рисков
- **Отчет:** модель угроз, матрица рисков, план мероприятий

Задание 1.3: Проектирование системы физической защиты помещений

Цель: Разработать комплекс мер физической защиты для помещения с конфиденциальной информацией

- Выберите тип помещения (серверная, переговорная, архив)
- Разработайте проект системы защиты:
 - Контроль доступа (турникеты, СКУД)
 - Видеонаблюдение и сигнализация
 - Защита от проникновения
 - Противопожарные меры
- Рассчитайте стоимость реализации проекта
- Оцените эффективность предлагаемых решений
- **Отчет:** план помещения, спецификация оборудования, расчет эффективности

Тема 2. Основные свойства и параметры волн

Задание 2.1: Экспериментальное исследование распространения электромагнитных волн

Цель: Изучить характеристики ЭМ-волн в различных средах

- Соберите измерительный комплекс на основе:
 - Генератора сигналов
 - Приемной антенны
 - Осциллографа или анализатора спектра
- Проведите серию экспериментов:
 - Измерение затухания сигнала в свободном пространстве
 - Исследование прохождения через различные материалы
 - Анализ влияния препятствий на распространение волн
- Постройте графики зависимости уровня сигнала от расстояния
- **Отчет:** схемы установок, протоколы измерений, графики, выводы

Задание 2.2: Расчет параметров антенных систем

Цель: Освоить методику расчета основных характеристик антенн

- Для заданного типа антенны (диполь, петлевая, патч-антенна):
 - Рассчитайте диаграмму направленности
 - Определите коэффициент усиления
 - Вычислите входное сопротивление
 - Оцените эффективную площадь
- Проведите моделирование в специализированном ПО (MMANA, NEC2)
- Сравните расчетные и экспериментальные данные
- **Отчет:** расчетные формулы, результаты моделирования, анализ погрешностей

Задание 2.3: Анализ волновых процессов в реальных условиях

Цель: Исследовать особенности распространения волн в городской среде

- Выберите участок городской застройки для исследования
- Проведите натурные измерения:
 - Уровня сигнала от стационарных передатчиков
 - Многолучевого распространения
 - Замираний сигнала
- Постройте карту покрытия и выявите "мертвые" зоны
- Проанализируйте влияние городской инфраструктуры на распространение волн
- **Отчет:** карты измерений, анализ факторов влияния, рекомендации

Тема 3. Электрические, магнитные и электромагнитные поля

Задание 3.1: Измерение и анализ электромагнитной обстановки

Цель: Провести комплексные измерения параметров ЭМП в рабочем помещении

- Используя измеритель напряженности поля, выполните:
 - Картографирование ЭМП на рабочих местах
 - Измерение фоновых уровней излучения
 - Анализ спектрального состава полей
- Выявите источники повышенного излучения
- Сравните результаты с санитарными нормами
- Разработайте рекомендации по нормализации ЭМ-обстановки
- **Отчет:** карты изолиний, протоколы измерений, анализ соответствия нормам

Задание 3.2: Исследование паразитных излучений технических средств

Цель: Обнаружить и проанализировать побочные электромагнитные излучения

- Выберите объекты исследования (компьютер, монитор, источник питания)
- Настройте измерительную аппаратуру для регистрации ПЭМИН:
 - Определите рабочие частоты оборудования
 - Настройте приемную антенну
 - Проведите измерения в различных режимах работы

- Оцените возможность восстановления информации по паразитным излучениям
- Предложите методы подавления выявленных излучений
- **Отчет:** спектрограммы, анализ рисков, рекомендации по защите

Задание 3.3: Расчет электрических полей в сложных конфигурациях

Цель: Освоить методы расчета электростатических полей

- Для заданной системы проводников:
 - Рассчитайте распределение потенциала
 - Постройте картину силовых линий
 - Определите напряженность поля в характерных точках
- Используйте методы:
 - Аналитический расчет для простых конфигураций
 - Численное моделирование (метод конечных элементов)
- Проведите верификацию результатов экспериментально
- **Отчет:** расчетные схемы, распределения полей, сравнение методов

Тема 4. Модели управления доступом и целостности информации

Задание 4.1: Разработка системы контроля целостности на основе хеш-функций

Цель: Создать программный комплекс для контроля целостности файлов

- Реализуйте на Python/Java систему, выполняющую:
 - Вычисление хеш-сумм (SHA-256, SHA-3) для файлов
 - Сравнение с эталонными значениями
 - Ведение журнала проверок
 - Уведомление о нарушениях целостности
- Протестируйте систему на различных типах файлов
- Оцените производительность и надежность
- **Отчет:** исходный код, тестовые сценарии, анализ результатов

Задание 4.2: Реализация модели управления доступом

Цель: Разработать систему управления доступом на основе ролевой модели (RBAC)

- Создайте прототип системы, включающий:
 - Базу данных пользователей и ролей
 - Матрицу прав доступа
 - Механизм аутентификации и авторизации
 - Журнал аудита действий
- Реализуйте сценарии:
 - Назначение и изменение ролей
 - Проверка прав доступа
 - Эскалация привилегий
- **Отчет:** архитектура системы, схемы взаимодействия, тестовые примеры

Задание 4.3: Создание системы электронной цифровой подписи

Цель: Реализовать алгоритмы ЭЦП и провести их анализ

- Разработайте программную реализацию:
 - Генерации ключевой пары (RSA, ECDSA)

- Формирования электронной подписи
 - Проверки подлинности подписи
- Проведите криптоанализ:
 - Оценку стойкости алгоритмов
 - Анализ уязвимостей реализации
 - Тестирование на различных наборах данных
- **Отчет:** алгоритмы реализации, результаты тестирования, рекомендации

Тема 5. Принципы экранирования полей

Задание 5.1: Расчет эффективности экранирования электромагнитных полей

Цель: Освоить методику расчета коэффициента экранирования

- Для заданных условий:
 - Рассчитайте коэффициент экранирования для различных материалов
 - Определите оптимальную толщину экрана
 - Оцените влияние частоты на эффективность экранирования
- Проведите сравнительный анализ материалов:
 - Медь, алюминий, сталь
 - Специализированные сплавы
 - Многослойные структуры
- Разработайте рекомендации по выбору экранирующих материалов
- **Отчет:** расчетные формулы, сравнительные таблицы, графики зависимостей

Задание 5.2: Проектирование экранированного корпуса для электронного устройства

Цель: Разработать конструкцию экранированного корпуса

- Выберите тип устройства (источник питания, контроллер, измерительный прибор)
- Выполните проектирование:
 - Разработка 3D-модели корпуса
 - Расчет мест ввода/вывода сигналов
 - Конструкция разъемов и органов управления
 - Система вентиляции и теплоотвода
- Рассчитайте ожидаемую эффективность экранирования
- Оцените стоимость изготовления
- **Отчет:** чертежи корпуса, расчеты, спецификация материалов

Задание 5.3: Экспериментальное исследование эффективности экранирования

Цель: Проверить теоретические расчеты на практике

- Изготовьте тестовые образцы экранов:
 - Однослойные экраны из различных материалов
 - Многослойные структуры
 - Экраны с перфорацией
- Проведите измерения коэффициента экранирования:

- В различных частотных диапазонах
 - При разных ориентациях экрана
 - С различными источниками поля
- Сравните экспериментальные данные с расчетными
- **Отчет:** методика измерений, результаты, анализ расхождений

Тема 6. Упругие волны и акустика речи

Задание 6.1: Анализ речевого сигнала и его параметров

Цель: Исследовать характеристики речевого сигнала

- Запишите речевые samples различных дикторов:
 - Мужские и женские голоса
 - Разные языки и акценты
 - Различные эмоциональные состояния
- Проведите анализ с использованием Audacity/Praat:
 - Спектральный анализ (Фурье-преобразование)
 - Формантный анализ
 - Измерение основных частотных характеристик
 - Анализ динамических параметров
- Выявите индивидуальные особенности речевых сигналов
- **Отчет:** спектрограммы, таблицы параметров, выводы

Задание 6.2: Исследование распространения упругих волн в конструкциях

Цель: Изучить особенности распространения звука в твердых телах

- Соберите экспериментальную установку:
 - Источник колебаний (вибратор, пьезоэлемент)
 - Приемные датчики (акселерометры, пьезодатчики)
 - Регистрирующая аппаратура
- Проведите измерения:
 - Скорости распространения волн в различных материалах
 - Коэффициента затухания
 - Влияния границ раздела сред
- Постройте дисперсионные кривые для исследуемых материалов
- **Отчет:** схемы установок, результаты измерений, анализ данных

Задание 6.3: Разработка системы идентификации диктора

Цель: Создать алгоритм идентификации человека по голосу

- Разработайте программный комплекс, выполняющий:
 - Предобработку речевого сигнала
 - Выделение признаков (MFCC, LPC)
 - Классификацию с использованием машинного обучения
 - Оценку достоверности идентификации
- Проведите тестирование на базе записей различных дикторов
- Оцените точность и надежность системы
- **Отчет:** алгоритмы, результаты тестирования, рекомендации по улучшению

Тема 7. Акустика помещений и звукоизоляция

Задание 7.1: Акустические измерения в помещении

Цель: Определить акустические характеристики учебной аудитории

- Проведите комплекс акустических измерений:
 - Измерение времени реверберации на различных частотах
 - Определение критического расстояния
 - Картографирование акустического поля
 - Анализ фоновых шумов
- Рассчитайте акустические параметры помещения
- Сравните результаты с нормативными требованиями
- **Отчет:** протоколы измерений, расчеты, выводы о качестве акустики

Задание 7.2: Проект акустической обработки помещения

Цель: Разработать меры по улучшению акустических характеристик

- Для выбранного помещения разработайте проект:
 - Расчет требуемого звукопоглощения
 - Подбор акустических материалов
 - Размещение звукопоглощающих конструкций
 - Дизайн-проект акустической обработки
- Рассчитайте ожидаемое улучшение параметров
- Оцените стоимость реализации проекта
- **Отчет:** план помещения, спецификация материалов, расчет эффективности

Задание 7.3: Исследование звукоизолирующих свойств конструкций

Цель: Экспериментально определить звукоизолирующую способность материалов

- Изготовьте тестовые образцы ограждающих конструкций:
 - Однослойные перегородки
 - Многослойные структуры
 - Конструкции с воздушными промежутками
- Проведите измерения индекса звукоизоляции:
 - В различных частотных диапазонах
 - При разных углах падения звука
 - С различными источниками шума
- Постройте частотные характеристики звукоизоляции
- **Отчет:** методика испытаний, результаты, рекомендации по применению

Тема 8. Инфразвук, ультразвук и DLP-системы

Задание 8.1: Исследование воздействия инфразвука и ультразвука

Цель: Изучить особенности инфразвука и ультразвука и их воздействие

- Создайте установку для генерации инфразвука и ультразвука
- Проведите серию экспериментов:
 - Измерение параметров генерируемых сигналов
 - Исследование распространения в различных средах
 - Оценка биологического воздействия (на модельных объектах)

- Анализ возможности использования для скрытой передачи информации
- Разработайте меры защиты от вредного воздействия
- **Отчет:** параметры сигналов, результаты исследований, рекомендации

Задание 8.2: Анализ уязвимостей информационной системы

Цель: Провести комплексный анализ уязвимостей типовой информационной системы

- Выберите объект анализа (веб-приложение, сеть, ОС)
- Проведите сканирование уязвимостей с использованием:
 - Nessus, OpenVAS, Nmap
 - Специализированных скриптов и утилит
- Классифицируйте выявленные уязвимости по степени критичности
- Разработайте план устранения наиболее опасных уязвимостей
- **Отчет:** отчет сканирования, классификация уязвимостей, план мероприятий

Задание 8.3: Разработка концепции DLP-системы для организации

Цель: Создать техническое задание на внедрение DLP-системы

- Проведите анализ бизнес-процессов организации
- Определите требования к DLP-системе:
 - Мониторируемые каналы передачи данных
 - Критерии фильтрации контента
 - Политики безопасности
 - Интеграция с существующей инфраструктурой
- Разработайте архитектуру системы и спецификацию оборудования
- Оцените стоимость внедрения и эксплуатации
- **Отчет:** техническое задание, архитектурная схема, расчет стоимости

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Типовые тесты

Тема 1. Поля объектов и проблема защиты информации

П1. Что относится к основным объектам защиты информации?

- а) только компьютеры и серверы
- б) информационные системы, технические средства, помещения ✓
- в) только базы данных и архивы
- г) только мобильные устройства

П2. Какой параметр НЕ характеризует поле объекта?

- а) напряженность
- б) частота
- в) цвет корпуса оборудования ✓
- г) потенциал

П3. Основная проблема защиты информации в помещениях:

- а) неудобная мебель
- б) отсутствие контроля доступа и несанкционированное проникновение ✓
- в) плохое освещение
- г) недостаток розеток

П4. Что такое технические каналы утечки информации?

- а) способы передачи данных через официальные каналы связи
- б) физические поля и излучения, позволяющие получить информацию ✓
- в) методы резервного копирования данных
- г) системы вентиляции помещений

П5. Какое из перечисленных помещений требует наибольшего уровня защиты?

- а) комната отдыха
- б) архив с конфиденциальными документами ✓
- в) кухня
- г) коридор

П6. Что является источником электромагнитных полей в офисном помещении?

- а) стулья и столы
- б) компьютеры, серверы, сетевое оборудование ✓
- в) книги на полках
- г) картины на стенах

П7. Для защиты мобильных устройств необходимо:

- а) хранить их в сейфе
- б) использовать шифрование и средства аутентификации ✓
- в) носить в кармане
- г) не использовать вообще

П8. Что такое "поле объекта" в контексте защиты информации?

- а) область вокруг объекта, где обнаруживаются его физические поля ✓

- б) место расположения объекта
- в) база данных объекта
- г) документация на объект

П9. Какие технические средства обрабатывают конфиденциальную информацию?

- а) только персональные компьютеры
- б) компьютеры, серверы, маршрутизаторы, системы хранения данных ✓
- в) только принтеры
- г) только мобильные телефоны

Тема 2. Основные свойства и параметры волн

П1. Что характеризует длину волны?

- а) энергию волны
- б) расстояние между точками с одинаковой фазой колебаний ✓
- в) скорость распространения
- г) амплитуду колебаний

П2. Какой параметр определяет энергию волны?

- а) частота
- б) амплитуда ✓
- в) длина волны
- г) фаза

П3. Волны в реальных средах:

- а) не затухают
- б) распространяются без искажений
- в) испытывают затухание и искажения ✓
- г) меняют частоту

П4. Диапазон частот электромагнитных волн для целей защиты информации:

- а) от 0 Гц до 100 ГГц ✓
- б) только звуковые частоты
- в) только оптический диапазон
- г) только радиодиапазон

П5. Что такое фаза волны?

- а) скорость распространения
- б) момент времени в цикле колебаний ✓
- в) максимальное отклонение
- г) количество колебаний в секунду

П6. Резонансная частота - это:

- а) минимальная возможная частота
- б) частота, на которой система колеблется с максимальной амплитудой ✓
- в) частота затухания
- г) постоянная величина для всех систем

П7. Коэффициент затухания показывает:

- а) как быстро волна теряет энергию ✓
- б) скорость волны
- в) частоту волны
- г) направление распространения

П8. Идеальная среда для распространения волн:

- а) не существует ✓
- б) вакуум
- в) вода
- г) металл

П9. Дисперсия волн - это:

- а) зависимость скорости от частоты ✓
- б) затухание волны
- в) отражение волны
- г) поглощение волны

П10. Установите правильную последовательность этапов исследования волн:

- а) генерация → измерение → анализ → выводы ✓
- б) анализ → выводы → генерация → измерение
- в) выводы → измерение → генерация → анализ
- г) генерация → выводы → анализ → измерение

Тема 3. Электрические, магнитные и электромагнитные поля

П1. Электрическое поле создается:

- а) движущимися зарядами
- б) неподвижными зарядами ✓
- в) магнитными полями
- г) гравитационными полями

П2. Линии электрического поля:

- а) всегда замкнуты
- б) начинаются на положительных зарядах и заканчиваются на отрицательных ✓
- в) не имеют направления
- г) параллельны друг другу

П3. Электромагнитная волна представляет собой:

- а) только электрическое поле
- б) только магнитное поле
- в) взаимосвязанные электрическое и магнитное поля ✓
- г) статическое поле

П4. Электрический потенциал измеряется в:

- а) Вольтах ✓
- б) Амперах

- в) Омах
- г) Теслах

П5. Магнитное поле создается:

- а) неподвижными зарядами
- б) движущимися зарядами ✓
- в) электрическими полями
- г) температурой

П6. Напряженность электрического поля измеряется в:

- а) Вольт/метр ✓
- б) Ампер/метр
- в) Вольт
- г) Тесла

П7. Что такое силовые линии магнитного поля?

- а) линии, показывающие направление действия силы на северный полюс ✓
- б) линии равного потенциала
- в) линии тока
- г) линии сопротивления

П8. Электромагнитная индукция - это:

- а) возникновение тока при изменении магнитного поля ✓
- б) создание магнитного поля током
- в) распространение волн
- г) зарядка аккумуляторов

П9. Постоянное магнитное поле создается:

- а) переменным током
- б) постоянными магнитами ✓
- в) только электромагнитами
- г) только в вакууме

Тема 4. Модели управления доступом и целостности информации

П1. Что такое полная копия данных?

- а) сжатая версия данных
- б) точная копия всех данных ✓
- в) только важные данные
- г) зашифрованные данные

П2. Контрольная сумма используется для:

- а) увеличения объема данных
- б) проверки целостности данных ✓
- в) шифрования данных
- г) сжатия данных

П3. Хеш-функция должна быть:

- а) обратимой
- б) детерминированной и стойкой к коллизиям ✓

- в) простой для вычисления
- г) случайной

П4. ЭЦП обеспечивает:

- а) только конфиденциальность
- б) только целостность
- в) аутентификацию и целостность ✓
- г) только доступность

П5. Имитовставка используется для:

- а) проверки подлинности и целостности данных ✓
- б) шифрования данных
- в) сжатия данных
- г) архивирования данных

П6. Какой алгоритм хеширования считается устаревшим?

- а) SHA-256
- б) MD5 ✓
- в) SHA-3
- г) Blake2

П7. Что такое "коллизия" в хеш-функциях?

- а) одинаковый хеш для разных данных ✓
- б) разный хеш для одинаковых данных
- в) ошибка вычисления
- г) потеря данных

П8. ЭЦП основана на:

- а) симметричном шифровании
- б) асимметричном шифровании ✓
- в) хеш-функциях
- г) контрольных суммах

П9. Для проверки целостности файла используется:

- а) сравнение хеш-сумм ✓
- б) сравнение размеров
- в) сравнение дат создания
- г) сравнение имен

П10. Установите правильную последовательность контроля целостности:

- а) вычисление хеша → сравнение с эталоном → действие при несовпадении ✓
- б) действие при несовпадении → вычисление хеша → сравнение
- в) сравнение с эталоном → вычисление хеша → действие
- г) вычисление хеша → действие → сравнение

Тема 5. Принципы экранирования полей

П1. Экранирование необходимо для:

- а) усиления полей
- б) ослабления полей ✓

- в) изменения частоты полей
- г) генерации полей

П2. ГОСТ 12.1.002-84 регулирует:

- а) требования к электромагнитным полям ✓
- б) требования к освещению
- в) температурный режим
- г) уровень шума

П3. Нормирование ЭМП учитывает:

- а) только частоту
- б) только интенсивность
- в) частоту, интенсивность и время воздействия ✓
- г) только время воздействия

П4. Метод защиты от ЭМП:

- а) увеличение мощности излучения
- б) использование экранов ✓
- в) уменьшение расстояния до источника
- г) усиление излучения

П5. Эффективность экранирования зависит от:

- а) только материала экрана
- б) материала, толщины и частоты поля ✓
- в) только толщины экрана
- г) только цвета экрана

П6. Для экранирования магнитных полей низкой частоты используют:

- а) медь
- б) алюминий
- в) ферромагнитные материалы ✓
- г) пластик

П7. Коэффициент экранирования показывает:

- а) во сколько раз ослабляется поле ✓
- б) стоимость экрана
- в) вес экрана
- г) температуру экрана

П8. Многослойные экраны эффективны потому, что:

- а) они тяжелее
- б) они дешевле
- в) сочетают разные механизмы экранирования ✓
- г) они красивее

П9. Экранирование работает за счет:

- а) отражения и поглощения энергии поля ✓
- б) усиления поля
- в) изменения частоты поля
- г) генерации противоположного поля

Тема 6. Упругие волны и акустика речи

П1. Упругие волны распространяются:

- а) только в вакууме
- б) только в газах
- в) в упругих средах ✓
- г) только в жидкостях

П2. Диапазон частот речевого сигнала:

- а) 20 Гц - 20 кГц
- б) 300 Гц - 3,4 кГц ✓
- в) 0 Гц - 100 Гц
- г) 10 кГц - 100 кГц

П3. Основная характеристика слухового восприятия:

- а) цвет
- б) громкость и высота звука ✓
- в) температура
- г) влажность

П4. Практическое применение упругих волн:

- а) только музыка
- б) только речь
- в) дефектоскопия, медицинская диагностика ✓
- г) только строительство

П5. Скорость звука в воздухе при нормальных условиях:

- а) 330 м/с ✓
- б) 1000 м/с
- в) 300000 км/с
- г) 1500 м/с

П6. Форманты в речи - это:

- а) области усиления определенных частот ✓
- б) тихие участки речи
- в) паузы в речи
- г) быстрые изменения громкости

П7. Ультразвук - это звук с частотой:

- а) ниже 20 Гц
- б) выше 20 кГц ✓
- в) точно 1000 Гц
- г) 20 Гц - 20 кГц

П8. Инфразвук может вызывать:

- а) только приятные ощущения
- б) дискомфорт и панику ✓
- в) улучшение слуха
- г) повышение интеллекта

П9. Акустический импеданс зависит от:

- а) плотности и скорости звука в среде ✓
- б) температуры среды
- в) цвета среды
- г) влажности среды

П10. Установите правильную последовательность речеобразования:

- а) легкие → голосовые связки → артикуляция → речь ✓
- б) артикуляция → легкие → голосовые связки → речь
- в) голосовые связки → легкие → речь → артикуляция
- г) речь → легкие → голосовые связки → артикуляция

Тема 7. Акустика помещений и звукоизоляция

П1. Эффект комнаты проявляется в:

- а) изменении тембра звука ✓
- б) изменении цвета стен
- в) повышении температуры
- г) увеличении освещенности

П2. Критическое расстояние - это расстояние, на котором:

- а) прямой звук равен отраженному ✓
- б) звук исчезает
- в) звук усиливается
- г) появляется эхо

П3. Спектральные искажения возникают due to:

- а) неравномерного поглощения частот ✓
- б) равномерного поглощения
- в) отсутствия поглощения
- г) только низких частот

П4. Звукоизоляция зависит от:

- а) только массы конструкции
- б) только герметичности
- в) массы, герметичности и упругости материалов ✓
- г) только цвета материалов

П5. Время реверберации - это:

- а) время затухания звука на 60 дБ ✓
- б) время распространения звука
- в) время настройки оборудования
- г) время записи звука

П6. Звукопоглощающие материалы:

- а) отражают звук
- б) преобразуют звуковую энергию в тепловую ✓
- в) усиливают звук
- г) генерируют звук

П7. Флаттер - это:

- а) быстрое повторение эха ✓
- б) медленное затухание звука
- в) усиление низких частот
- г) ослабление высоких частот

П8. Звукоизоляция окон зависит от:

- а) только толщины стекла
- б) количества стекол и расстояния между ними ✓
- в) только цвета рамы
- г) только размера окна

П9. Резонанс в помещениях возникает когда:

- а) размеры комнаты кратны длине волны ✓
- б) комната пустая
- в) комната заполнена мебелью
- г) включен свет

Тема 8. Инфразвук, ультразвук и DLP-системы

П1. Инфразвук - это колебания с частотой:

- а) ниже 20 Гц ✓
- б) 20 Гц - 20 кГц
- в) выше 20 кГц
- г) точно 1000 Гц

П2. Ультразвук используется для:

- а) только медицинской диагностики
- б) только очистки поверхностей
- в) медицинской диагностики, дефектоскопии ✓
- г) только связи

П3. DLP-система предназначена для:

- а) повышения скорости сети
- б) предотвращения утечек данных ✓
- в) усиления сигнала
- г) архивирования данных

П4. Методология гипотетического дефекта используется для:

- а) поиска существующих уязвимостей
- б) прогнозирования возможных уязвимостей ✓
- в) устранения уязвимостей
- г) документирования уязвимостей

П5. Инфразвук опасен тем, что:

- а) не слышим, но воздействует на организм ✓
- б) слишком громкий
- в) вызывает только удовольствие
- г) улучшает слух

П6. Ультразвуковые датчики работают на принципе:

- а) отражения ультразвуковых волн ✓
- б) поглощения света
- в) излучения тепла
- г) генерации магнитного поля

П7. DLP-система анализирует:

- а) только исходящий трафик
- б) входящий и исходящий трафик ✓
- в) только внутреннюю сеть
- г) только почтовые сообщения

П8. Классификация уязвимостей включает:

- а) только критические уязвимости
- б) уязвимости по степени опасности ✓
- в) только программные уязвимости
- г) только аппаратные уязвимости

П9. Акустический канал утечки информации - это:

- а) перехват речевой информации ✓
- б) перехват сетевого трафика
- в) копирование файлов
- г) фотографирование экрана

П10. Установите правильную последовательность работы DLP-системы:

- а) анализ → обнаружение → блокировка → отчет
- б) блокировка → анализ → обнаружение → отчет
- в) обнаружение → анализ → блокировка → отчет ✓
- г) отчет → анализ → обнаружение → блокировка

Критерии оценивания тестовых заданий для текущего контроля

Максимальное количество баллов за решение одного теста составляет 5 баллов, которые переводятся в академические оценки следующим образом:

- оценка «отлично» (5 баллов) выставляется при условии правильного ответа студента не менее чем на 85% контрольных заданий
- оценка «хорошо» (4 балла) выставляется при условии правильного ответа студента не менее чем на 70% контрольных заданий
- оценка «удовлетворительно» (3 балла) выставляется при условии правильного ответа студента не менее чем на 51% контрольных заданий
- оценка «неудовлетворительно» (1-2 балла) выставляется при условии правильного ответа студента менее чем на 50% контрольных заданий

2.2 Оценочные материалы для проведения промежуточной аттестации

ПК-3.4.1 Анализирует компьютерную систему с целью определения уровня защищённости и доверия

П1. Какой из объектов защиты информации требует наиболее строгого контроля доступа при анализе защищенности системы?

- а) Комнаты отдыха;
- б) Архивы с конфиденциальными документами; [✓]
- в) Коридоры общего пользования;
- г) Кухни и столовые.

Ответ: б) Архивы с конфиденциальными документами

П2. Что является критически важным при анализе электромагнитной обстановки помещения?

- а) Цвет стен и мебели;
- б) Уровень освещенности;
- в) Наличие источников электромагнитных полей и их параметры; [✓]
- г) Температурный режим.

Ответ: в) Наличие источников электромагнитных полей и их параметры

П3. Какой параметр волн является ключевым при оценке их опасности для защищаемой информации?

- а) Цвет излучения;
- б) Частота и интенсивность; [✓]
- в) Направление распространения;
- г) Время суток излучения.

Ответ: б) Частота и интенсивность

П4. При анализе системы управления доступом какой компонент требует первоочередной проверки?

- а) Дизайн интерфейса;
- б) Механизмы аутентификации и авторизации; [✓]
- в) Скорость работы системы;
- г) Цветовая схема.

Ответ: б) Механизмы аутентификации и авторизации

П5. Установите соответствие между объектом защиты и методом анализа его безопасности:

Объект защиты	Метод анализа
1. Помещения	а) Проверка физической защиты и контроля доступа
2. Технические средства	б) Измерение параметров полей и излучений
3. Информационные системы	в) Аудит настроек и политик безопасности

Правильный ответ:

1 – а, 2 – б, 3 – в

П6. Установите соответствие между типом волн и методом их анализа:

Тип волн	Метод анализа
1. Электромагнитные волны	а) Измерение напряженности поля
2. Упругие волны	б) Акустические измерения
3. Электрические поля	в) Измерение потенциала и напряженности

Правильный ответ:

1 – а, 2 – б, 3 – в

П7. Установите правильную последовательность анализа уровня защищенности компьютерной системы:

- а) Идентификация критических активов и данных.
- б) Анализ архитектуры системы и точек входа.
- в) Оценка механизмов контроля доступа.
- г) Тестирование на уязвимости.
- д) Формирование отчета о уровне доверия.

Ответ: АБВГД

П8. Установите правильную последовательность оценки акустической безопасности помещения:

- а) Измерение фонового шума.
- б) Определение времени реверберации.
- в) Анализ звукоизолирующих свойств конструкций.
- г) Выявление акустических каналов утечки информации.
- д) Оценка общего уровня акустической защищенности.

Ответ: АБВГД

П9. Как называется метод анализа, при котором проверяется соответствие системы установленным стандартам и нормативам?

Правильный ответ: Аудит соответствия (Compliance Audit)

П10. Как называется характеристика, определяющая способность системы сохранять защищенность при отказах?

Правильный ответ: Отказоустойчивость (Fault Tolerance) или Надежность (Reliability)

ПК-3.4.2 Демонстрирует умение проводить анализ безопасности компонентов программных и программно-аппаратных средств защиты информации

П11. Какой параметр электрического поля является наиболее важным при анализе его опасности для информации?

- а) Цвет поля;
- б) Напряженность и частота; [✓]
- в) Форма силовых линий;
- г) Время существования.

Ответ: б) Напряженность и частота

П12. При анализе системы контроля целостности данных какой алгоритм считается устаревшим и ненадежным?

- а) SHA-256;
- б) MD5; [✓]
- в) SHA-3;
- г) Blake2.

Ответ: б) MD5

П13. Какой механизм защиты от электромагнитных полей является

наиболее эффективным для высокочастотных излучений?

- а) Увеличение расстояния до источника;
- б) Использование экранов из проводящих материалов; [✓]
- в) Уменьшение мощности излучения;
- г) Изменение цвета оборудования.

Ответ: б) Использование экранов из проводящих материалов

П14. При анализе акустической защиты помещения какой параметр является критически важным?

- а) Цвет стен;
- б) Время реверберации и уровень звукоизоляции; [✓]
- в) Размер помещения;
- г) Количество окон.

Ответ: б) Время реверберации и уровень звукоизоляции

П15. Установите соответствие между компонентом защиты и методом его анализа:

Компонент защиты	Метод анализа
1. Система контроля целостности	а) Проверка алгоритмов хеширования и ЭЦП
2. Механизмы экранирования	б) Измерение коэффициента экранирования
3. Акустическая защита	в) Акустические измерения и анализ

Правильный ответ:

1 – а, 2 – б, 3 – в

П16. Установите соответствие между уязвимостью и методом ее обнаружения:

Уязвимость	Метод обнаружения
1. Слабое экранирование	а) Измерение параметров полей
2. Недостаточная звукоизоляция	б) Акустические измерения
3. Ненадежная целостность данных	в) Анализ алгоритмов хеширования

Правильный ответ:

1 – а, 2 – б, 3 – в

П17. Установите правильную последовательность анализа системы экранирования:

- а) Измерение фоновых уровней полей.
- б) Оценка эффективности экранирования.
- в) Анализ материалов и конструкции экранов.
- г) Выявление недостатков экранирования.
- д) Разработка рекомендаций по улучшению.

Ответ: АБВГД

П18. Установите правильную последовательности тестирования системы контроля целостности:

- а) Проверка алгоритмов хеширования.
- б) Тестирование на различных типах данных.
- в) Анализ стойкости к коллизиям.

- г) Оценка производительности системы.
- д) Формирование выводов о надежности.

Ответ: АБВГД

П19. Как называется метод анализа, при котором проверяется способность системы противостоять конкретным типам атак?

Правильный ответ: Тестирование на проникновение (Penetration Testing) или Оценка уязвимостей (Vulnerability Assessment)

П20. Как называется характеристика, определяющая способность системы обеспечивать целостность данных?

Правильный ответ: Достоверность (Integrity) или Надежность хранения (Storage Reliability)

ПК-3.4.3 Формирует предложения по устранению выявленных уязвимостей

П21. При обнаружении слабого экранирования электромагнитных полей какое решение является наиболее эффективным?

- а) Покраска оборудования в другой цвет;
- б) Установка дополнительных экранов из проводящих материалов; [✓]
- в) Увеличение мощности излучения;
- г) Изменение частоты работы оборудования.

Ответ: б) Установка дополнительных экранов из проводящих материалов

П22. Какое предложение по устранению уязвимости следует внести при обнаружении использования устаревшего алгоритма хеширования MD5?

- а) Продолжить использование MD5;
- б) Перейти на более современный алгоритм (SHA-256, SHA-3); [✓]
- в) Увеличить длину хеша MD5;
- г) Использовать два алгоритма одновременно.

Ответ: б) Перейти на более современный алгоритм (SHA-256, SHA-3)

П23. При выявлении недостаточной звукоизоляции помещения какое улучшение следует предложить?

- а) Установка дополнительных звукопоглощающих материалов; [✓]
- б) Увеличение громкости разговоров;
- в) Покраска стен в другой цвет;
- г) Установка более яркого освещения.

Ответ: а) Установка дополнительных звукопоглощающих материалов

П24. Какое предложение по устранению уязвимости эффективно при обнаружении слабых механизмов аутентификации?

- а) Упрощение процедуры аутентификации;
- б) Внедрение многофакторной аутентификации; [✓]
- в) Отключение аутентификации;
- г) Использование простых паролей.

Ответ: б) Внедрение многофакторной аутентификации

П25. Установите соответствие между выявленной уязвимостью и предлагаемым решением:

Уязвимость	Предлагаемое решение
1. Слабое экранирование ЭМП	а) Установка дополнительных экранов
2. Недостаточная звукоизоляция	б) Модернизация акустической защиты
3. Ненадежные алгоритмы хеширования	в) Замена на современные алгоритмы

Правильный ответ:

1 – а, 2 – б, 3 – в

П26. Установите соответствие между недостатком защиты и мерой по его устранению:

Недостаток защиты	Мера по устранению
1. Высокий уровень фоновых шума	а) Установка шумоподавляющих материалов
2. Недостаточная эффективность экранирования	б) Применение многослойных экранов
3. Слабая аутентификация	в) Внедрение биометрической проверки

Правильный ответ:

1 – а, 2 – б, 3 – в

П27. Установите правильную последовательность устранения выявленных уязвимостей:

- а) Приоритизация уязвимостей по степени опасности.
- б) Разработка плана устранения для каждой уязвимости.
- в) Реализация защитных мер и доработок.
- г) Тестирование эффективности выполненных работ.
- д) Документирование произведенных изменений.

Ответ: АБВГД

П28. Установите правильную последовательность улучшения системы защиты:

- а) Анализ воздействия изменений на работу системы.
- б) Разработка поэтапного плана внедрения улучшений.
- в) Реализация улучшений в тестовой среде.
- г) Мониторинг работы системы после внедрения.
- д) Корректировка улучшений по результатам мониторинга.

Ответ: АБВГД

П29. Как называется документ, описывающий план устранения выявленных уязвимостей с указанием сроков и ответственных?

Правильный ответ: План исправления уязвимостей (Vulnerability Remediation Plan)

П30. Как называется процесс постепенного внедрения улучшений безопасности с минимальным воздействием на работу системы?

Правильный ответ: Поэтапное развертывание (Phased Deployment) или Инкрементальное внедрение

**Критерии оценки для проведения зачета
по дисциплине (тестирование)**

Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок.

Оценка	Уровень сформированности компетенции	Критерии
«Отлично» («зачтено»)	Высокий	Выполнено более 80% заданий предложенного теста
«Хорошо» («зачтено»)	Хороший	Выполнено 60-80% заданий предложенного теста
«Удовлетворительно» («зачтено»)	Достаточный	Выполнено 35-60% заданий предложенного теста
«Неудовлетворительно» («не зачтено»)	Недостаточный	Выполнено менее 35% заданий предложенного теста

Обновление оценочных материалов дисциплины

обсуждено и рекомендовано к утверждению решением кафедры
наименование кафедры _____
от ____ ____ 20__ г., протокол № ____

одобрено Научно-методическим советом _____ от ____ ____ 20__ г.,
протокол № ____