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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ АТАКАМ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Оценочные материалы по дисциплине Системы противодействия компьютерным атакам

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

Целью оценочных материалов по дисциплине (модулю) (далее –ОМ) является комплексная оценка результатов обучения по дисциплине Системы противодействия компьютерным атакам 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 Системы противодействия компьютерным атакам.

1. Паспорт оценочных материалов по дисциплине «Системы противодействия компьютерным атакам»

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-3.5. Способен разрабатывать требования по защите, формированию политик безопасности компьютерных систем и сетей на основе менеджмента, аудита и оценки рисков информационной безопасности	ПК-3.5.1. Принимает решения о необходимости защи-ты информации, содержащейся в ИС	Знать: основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы. Уметь: анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам Владеть: навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.	Тема 1. Системный подход к обеспечению защиты от компьютерных атак. Тема 2. Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности. Тема 3. Методы и средства обнаружения и отражения сетевых атак. Тема 4. Комплексные системы защиты от компьютерных атак	Реферат (Тема 1-4) Тест (тема 1-4) Домашние задания по практическим занятиям (тема 1-4)	Тест (П 1-10 тестового задания)
	ПК-3.5.2. Принимает решения о необходимости защи-ты информации, содержащейся в ИС	Знать: основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы.	Тема 1. Системный подход к обеспечению защиты от компьютерных атак. Тема 2. Средства выявления и локализации уязвимостей компьютерных систем к	Реферат (Тема 1-4) Тест (тема 1-4) Домашние задания по практическим занятиям (тема 1-4)	Тест (П 11-20 тестового задания)

		Уметь: анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам Владеть: навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.	воздействию угроз безопасности. Тема 3. Методы и средства обнаружения и отражения сетевых атак. Тема 4. Комплексные системы защиты от компьютерных атак		
	ПК-3.5.3. Анализирует компьютерную систему с целью определения необходимого уровня защищенности и доверия на основе менеджмента, аудита и оценки рисков информационной безопасности.	Знать: основные принципы построения и механизмы функционирования систем противодействия компьютерным атакам, особы обнаружения и нейтрализации последствий вторжений в компьютерные системы. Уметь: анализировать защищенность компьютерных систем, управлять системами противодействия компьютерным атакам Владеть: навыками выявления и устранения уязвимостей компьютерных систем, настройки систем противодействия компьютерным атакам.	Тема 1. Системный подход к обеспечению защиты от компьютерных атак. Тема 2. Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности. Тема 3. Методы и средства обнаружения и отражения сетевых атак. Тема 4. Комплексные системы защиты от компьютерных атак	Реферат (Тема 1-4) Тест (тема 1-4) Домашние задания по практическим занятиям (тема 1-4)	Тест (П 21-30 тестового задания)

2. Оценочные материалы по дисциплине «Системы противодействия компьютерным атакам»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

ТЕМА 1. СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК

1. Системный подход к защите компьютерных систем: основные принципы и методологии. (Анализ компонентов КС как объектов защиты)
2. Угрозы безопасности компьютерных систем: современная классификация и таксономия. (Внешние и внутренние угрозы, целенаправленные атаки)
3. Методы и методики построения защищенных компьютерных систем: сравнительный анализ. (Проактивный и реактивный подходы)
4. Организационные методы защиты: разработка политик безопасности и регламентов. (Роль организационных мер в комплексной защите)
5. Защита компонентов компьютерной системы: от аппаратного обеспечения до прикладного ПО. (Многоуровневая модель защиты)
6. Модели управления безопасностью компьютерных систем: отечественный и зарубежный опыт.
7. Методики оценки рисков для компьютерных систем: практическое применение.
8. Роль человеческого фактора в системе защиты от компьютерных атак. (Обучение и повышение осведомленности)
9. Инцидент-менеджмент в защищенных компьютерных системах: процедуры реагирования.
10. Построение системы безопасности для критически важных объектов информационной инфраструктуры.
11. Эволюция подходов к защите компьютерных систем: от периметровой защиты к Zero Trust.

ТЕМА 2. СРЕДСТВА ВЫЯВЛЕНИЯ И ЛОКАЛИЗАЦИИ УЯЗВИМОСТЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ

1. Методы и средства оценки защищенности компьютерных систем: автоматизированные и ручные подходы. (Сканеры уязвимостей, пентестинг)
2. Системы контроля доступа к компонентам КС: от дискреционного до мандатного управления. (DAC, MAC, RBAC)
3. Обеспечение безопасности электропитания компьютерных систем: технические и организационные меры. (ИБП, стабилизаторы, генереторы)
4. Методы и средства гарантированного уничтожения информации:

сравнительный анализ технологий. (Физическое уничтожение, криптографическое стирание)
5. Выявление и локализация утечек информации по техническим каналам: ПЭМИН и акустические каналы.
6. Средства мониторинга и аудита безопасности компьютерных систем в реальном времени. (SIEM-системы)
7. Методы противодействия атакам на системы электропитания компьютерной инфраструктуры.
8. Оценка эффективности средств защиты от утечек информации: метрики и критерии.
9. Локализация уязвимостей в распределенных компьютерных системах: особенности и методы.
10. Средства защиты от утечек через периферийные устройства и внешние носители.
11. Интеграция средств выявления уязвимостей в процессы DevOps (DevSecOps).

ТЕМА 3. МЕТОДЫ И СРЕДСТВА ОБНАРУЖЕНИЯ И ОТРАЖЕНИЯ СЕТЕВЫХ АТАК

1. Системы обнаружения и предотвращения сетевых атак (IDS/IPS): архитектура и принципы работы. (Сетевые и хостовые системы)
2. Методы обнаружения вредоносных программ в компьютерных системах: сигнатурный и поведенческий анализ.
3. Контентная фильтрация сетевого трафика: технологии и практическое применение. (DLP, веб-фильтрация)
4. Межсетевое экранирование: эволюция от packet filtering до next-generation firewalls.
5. Средства создания и управления виртуальными частными сетями (VPN): протоколы и безопасность. (IPsec, SSL/TLS VPN)
6. Обнаружение сложных целевых атак (APT): методы и средства.
7. Анализ сетевого трафика для выявления аномальной активности: машинное обучение в IDS.
8. Отражение DDoS-атак: многоуровневая система защиты.
9. Системы глубокого анализа пакетов (Deep Packet Inspection) в современных межсетевых экранах.
10. Обнаружение и нейтрализация сетевых червей и ботнетов.
11. Методы противодействия уклонению от систем обнаружения сетевых атак.

ТЕМА 4. КОМПЛЕКСНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК

1. Доверенные аппаратные среды: архитектура и принципы построения. (Trusted Platform Module, аппаратные модули доверия)
2. Подсистемы безопасности операционных систем: механизмы Mandatory Integrity Control и AppContainer.

3. Защита систем управления базами данных: от контроля доступа до шифрования данных.
4. Комплексные системы защиты локальных и корпоративных сетей: проектирование и внедрение.
5. Системы контроля работы пользователей компьютерных систем: мониторинг и анализ действий.
6. Оснащение центров ГосСОПКА: структура, функции и технические средства.
7. Защита прикладного программного обеспечения на протяжении всего жизненного цикла.
8. Комплексные системы защиты от целевых атак (Advanced Persistent Threats).
9. Интеграция разнородных средств защиты в единый комплекс безопасности.
10. Системы управления информационной безопасностью (SIEM) в корпоративных сетях.
11. Обеспечение безопасности мобильных устройств в корпоративной среде (MDM, MAM).
12. Защита облачных инфраструктур: особенности и комплексные решения.

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 существа.

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 согласованна 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, предъявляемыек 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. Системный подход к обеспечению защиты от компьютерных атак

Задание 1.1: Разработка политики информационной безопасности для организации

Цель: Освоить принципы создания организационных мер защиты

- Разработайте политику ИБ для средней компании (100-200 сотрудников)
- Включите разделы:
  - Правила использования ресурсов
  - Процедуры управления доступом
  - Политика паролей

- Регламент реагирования на инциденты
- **Объем:** 15-20 страниц
- **Критерии:** полнота, соответствие законодательству, практическая применимость

Задание 1.2: Анализ угроз для типовой IT-инфраструктуры
Цель: Научиться проводить оценку угроз безопасности

- Составьте модель угроз для компании (выбор из: банк, интернет-магазин, медицинское учреждение)
- Используйте методику STRIDE или OCTAVE
- Представьте результаты в виде матрицы угроз
- **Отчет:** диаграммы угроз, таблицы рисков, рекомендации

Задание 1.3: Проектирование системы управления доступом
Цель: Разработать систему разграничения прав доступа

- Создайте модель RBAC для организации с 5-7 ролями
- Определите права доступа для каждой роли
- Реализуйте прототип на Python/Java
- **Результат:** схема ролей, матрица доступа, код программы

Задание 1.4: Разработка регламента реагирования на инциденты
Цель: Создать план действий при кибератаках

- Разработайте пошаговый регламент для:
  - Обнаружение атаки
  - Локализация инцидента
  - Устранение последствий
  - Восстановление работы
- **Объем:** 10-15 страниц
- **Критерии:** четкость процедур, полнота coverage, практичность

Задание 1.5: Сравнительный анализ методов защиты
Цель: Изучить различные подходы к защите КС

- Проведите сравнительный анализ 3-4 методологий защиты
- Оцените эффективность для разных типов организаций
- Подготовьте рекомендации по выбору методологии
- **Отчет:** таблица сравнения, выводы, рекомендации

Тема 2. Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности

Задание 2.1: Проведение сканирования уязвимостей
Цель: Освоить инструменты оценки защищенности

- Проведите сканирование тестового стенда с помощью OpenVAS/Nessus
- Проанализируйте результаты сканирования
- Составьте отчет с рекомендациями по устранению уязвимостей
- **Отчет:** результаты сканирования, классификация уязвимостей, план исправлений

Задание 2.2: Аудит системы контроля доступа
Цель: Научиться проверять настройки прав доступа

- Проведите аудит прав доступа в тестовой системе (Windows/Linux)

- Выявите нарушения принципа минимальных привилегий
- Составьте отчет с рекомендациями
- **Отчет:** таблица проверки, выявленные нарушения, рекомендации

Задание 2.3: Проектирование системы гарантированного уничтожения информации

Цель: Разработать процедуры уничтожения данных

- Создайте регламент уничтожения для разных типов носителей
- Исследуйте методы криптографического стирания
- Разработайте технические требования к средствам уничтожения
- **Отчет:** регламент, технические требования, протоколы тестирования

Задание 2.4: Обнаружение утечек по техническим каналам

Цель: Освоить методы выявления ПЭМИН

- Создайте стенд для исследования электромагнитных излучений
- Проведите измерения параметров излучений
- Разработайте рекомендации по защите
- **Отчет:** схемы измерений, результаты, рекомендации по экранированию

Задание 2.5: Анализ защищенности системы электропитания

Цель: Оценить уязвимости системы питания

- Проведите аудит системы электропитания тестового ЦОД
- Выявите single points of failure
- Разработайте схему резервирования
- **Отчет:** схема питания, выявленные уязвимости, план улучшений

Тема 3. Методы и средства обнаружения и отражения сетевых атак

Задание 3.1: Настройка и тестирование IDS/IPS системы

Цель: Освоить развертывание систем обнаружения атак

- Разверните Suricata/Snort на тестовом стенде
- Настройте правила обнаружения атак
- Проведите тестирование эффективности
- **Отчет:** конфигурационные файлы, результаты тестирования, рекомендации

Задание 3.2: Создание системы контентной фильтрации

Цель: Разработать систему фильтрации сетевого трафика

- Настройке Squid Proxy с фильтрацией контента
- Реализуйте категориальную фильтрацию
- Протестируйте эффективность блокировки
- **Отчет:** конфигурация, тестовые сценарии, результаты

Задание 3.3: Построение VPN-туннеля

Цель: Освоить технологии виртуальных частных сетей

- Настройте IPsec VPN между двумя сегментами сети
- Протестируйте производительность и безопасность
- Проведите анализ уязвимостей реализации
- **Отчет:** схемы настройки, результаты тестов, рекомендации по безопасности

Задание 3.4: Анализ вредоносного ПО
Цель: Изучить методы обнаружения malware

- Проанализируйте образцы вредоносных программ в sandbox
- Составьте сигнатуры для обнаружения
- Разработайте правила для IDS
- **Отчет:** анализ образцов, сигнатуры, правила обнаружения

Задание 3.5: Настройка межсетевого экранирования
Цель: Освоить принципы настройки firewall

- Настройте iptables/pfSense для защиты сегмента сети
- Создайте правила для типовых сервисов
- Протестируйте эффективность защиты
- **Отчет:** конфигурация firewall, тестовые сценарии, результаты

Тема 4. Комплексные средства защиты от компьютерных атак

Задание 4.1: Проектирование доверенной аппаратной среды
Цель: Разработать архитектуру защищенной системы

- Спроектируйте систему на основе TPM/HSM
- Разработайте схему безопасной загрузки
- Опишите процедуры аутентификации
- **Отчет:** архитектурная схема, спецификации, процедуры безопасности

Задание 4.2: Аудит подсистемы безопасности ОС
Цель: Проверить настройки безопасности операционной системы

- Проведите аудит безопасности Windows/Linux сервера
- Проверьте соответствие требованиям стандартов
- Составьте отчет о соответствии
- **Отчет:** чек-лист проверки, выявленные проблемы, рекомендации

Задание 4.3: Разработка системы защиты СУБД
Цель: Настроить комплексную защиту базы данных

- Настройте аудит и мониторинг СУБД
- Реализуйте шифрование чувствительных данных
- Настройте разграничение доступа
- **Отчет:** конфигурация СУБД, политики доступа, настройки шифрования

Задание 4.4: Создание системы мониторинга пользователей
Цель: Разработать систему контроля действий пользователей

- Настройте сбор и анализ логов пользовательской активности
- Реализуйте детектирование аномального поведения
- Создайте дашборд для мониторинга
- **Отчет:** архитектура системы, правила детектирования, примеры отчетов

Задание 4.5: Проектирование центра мониторинга безопасности
Цель: Разработать концепцию SOC

- Спроектируйте архитектуру центра мониторинга
- Определите перечень мониторируемых событий
- Разработайте регламенты работы analysts
- **Отчет:** архитектура SOC, матрика событий, регламенты работы

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. Системный подход к обеспечению защиты от компьютерных атак

П1. Что понимается под системным подходом к защите от компьютерных атак?

а) Использование только антивирусного ПО

б) Комплексное применение организационных и технических мер защиты ✓

в) Защита только периметра сети

г) Обеспечение только физической безопасности

П2. Какой компонент компьютерной системы является наиболее уязвимым?

а) Аппаратное обеспечение

б) Человеческий фактор ✓

в) Операционная система

г) Сетевое оборудование

П3. Какие методы относятся к организационной защите компьютерных систем?

а) Установка межсетевого экрана

б) Разработка политик и регламентов безопасности ✓

в) Настройка систем обнаружения вторжений

г) Шифрование данных

П4. Какой принцип является основополагающим при построении защищенных компьютерных систем?

а) Принцип максимальных привилегий

б) Принцип "доверяй, но проверяй"
в) Принцип эшелонированной защиты ✓
г) Принцип минимального контроля

П5. Что включает в себя направление "построение защищенных компьютерных систем"?
а) Только установку антивирусного ПО
б) Проектирование архитектуры безопасности с учетом угроз ✓
в) Только физическую защиту помещений
г) Только резервное копирование данных

П6. Какой метод защиты наиболее эффективен против целевых атак?
а) Установка антивируса
б) Обучение пользователей
в) Комплексное применение различных мер защиты ✓
г) Использование сложных паролей

П7. Что такое "компьютерная система" в контексте защиты информации?
а) Отдельный компьютер
б) Совокупность аппаратных и программных компонентов ✓
в) Только серверное оборудование
г) Только рабочие станции

П8. Какой из перечисленных элементов НЕ относится к организационным методам защиты?
а) Политика паролей
б) Регламент реагирования на инциденты
в) Обучение пользователей
г) Настройка межсетевого экрана ✓

П9. Что является основной целью системного подхода к защите?
а) Снижение стоимости защиты
б) Обеспечение комплексной безопасности ✓
в) Упрощение администрирования
г) Повышение производительности

П10. Какой метод наиболее эффективен для защиты от внутренних угроз?
а) Усиление периметра сети
б) Разделение привилегий и контроль действий пользователей ✓
в) Установка дополнительных серверов
г) Увеличение скорости интернета

Тема 2. Средства выявления и локализации уязвимостей компьютерных систем

П1. Что такое "уязвимость" в контексте компьютерной безопасности?
а) Высокая стоимость оборудования

б) Слабое место в системе, которое может быть использовано для атаки ✓
в) Низкая производительность системы
г) Отсутствие резервного копирования

П2. Какой инструмент используется для автоматического сканирования уязвимостей?

а) Microsoft Word
б) Nessus ✓
в) Adobe Photoshop
г) AutoCAD

П3. Что такое "контроль доступа" в компьютерных системах?

а) Управление температурой в серверной
б) Регулирование прав пользователей на доступ к ресурсам ✓
в) Контроль интернет-трафика
г) Управление электропитанием

П4. Какой метод обеспечивает гарантированное уничтожение информации?

а) Удаление файлов через Корзину
б) Форматирование диска
в) Физическое уничтожение носителей ✓
г) Переименование файлов

П5. Что относится к техническим каналам утечки информации?

а) Социальная инженерия
б) Электромагнитное излучение ✓
в) Кража документов
г) Подкуп сотрудников

П6. Какой параметр наиболее важен для оценки защищенности системы?

а) Цвет корпуса сервера
б) Количество установленных программ
в) Наличие неустраненных уязвимостей ✓
г) Скорость интернет-соединения

П7. Что такое "локализация уязвимости"?

а) Установка дополнительного оборудования
б) Определение точного места уязвимости в системе ✓
в) Перезагрузка системы
г) Обновление антивирусных баз

П8. Какой метод используется для выявления утечек информации?

а) Анализ логов и мониторинг сетевого трафика ✓
б) Увеличение зарплаты сотрудников
в) Покраска стен в другой цвет
г) Установка кондиционеров

П9. Что обеспечивает безопасность электропитания компьютерных систем?

а) Использование ИБП и стабилизаторов ✓
б) Установка дополнительных мониторов
в) Настройка яркости экранов
г) Применение беспроводных клавиатур

П10. Какой из перечисленных методов НЕ относится к выявлению уязвимостей?

а) Пентестинг
б) Аудит безопасности
в) Сканирование уязвимостей
г) Дефрагментация диска ✓

Тема 3. Методы и средства обнаружения и отражения сетевых атак

П1. Что такое IDS в контексте сетевой безопасности?

а) Internet Data Service
б) Intrusion Detection System ✓
в) Internal Disk Storage
г) International Domain System

П2. Какой метод используется для обнаружения сетевых атак?

а) Анализ сетевого трафика и выявление аномалий ✓
б) Изменение паролей пользователей
в) Установка дополнительной оперативной памяти
г) Настройка заставки на рабочий стол

П3. Что такое "контентная фильтрация"?

а) Контроль содержания передаваемых данных ✓
б) Фильтрация воздуха в серверной
в) Очистка воды в системе охлаждения
г) Сортировка мусора в офисе

П4. Какую функцию выполняет межсетевой экран?

а) Контроль и фильтрация сетевого трафика ✓
б) Охлаждение процессоров
в) Обеспечение электропитания
г) Создание резервных копий

П5. Что такое VPN?

а) Virtual Private Network - виртуальная частная сеть ✓
б) Very Powerful Network - очень мощная сеть
в) Visual Programming Network - визуальная программируемая сеть
г) Variable Protocol Network - сеть с переменным протоколом

П6. Какой тип атак обнаруживают системы IDS?

а) Только вирусные атаки
б) Только спам
в) Различные типы сетевых атак ✓
г) Только фишинг

П7. Что такое "вредоносная программа"?

а) Полезное программное обеспечение

б) Программа, наносящая вред компьютерной системе ✓

в) Системная утилита

г) Драйвер устройства

П8. Какой протокол чаще всего используется для создания VPN?

а) HTTP

б) FTP

в) IPsec ✓

г) SMTP

П9. Что такое "межсетевое экранирование"?

а) Разделение сети на сегменты с разным уровнем доверия ✓

б) Установка физических барьеров между компьютерами

в) Покраска сетевого оборудования

г) Настройка экранов мониторов

П10. Какой метод наиболее эффективен для отражения DDoS-атак?

а) Отключение интернета

б) Использование специализированных систем защиты ✓

в) Перезагрузка серверов

г) Увеличение скорости интернета

Тема 4. Комплексные системы защиты от компьютерных атак

П1. Что такое "доверенная аппаратная среда"?

а) Оборудование от проверенных поставщиков

б) Аппаратная платформа с встроенными механизмами безопасности ✓

в) Компьютеры в защищенных помещениях

г) Серверы с большим объемом памяти

П2. Какая подсистема отвечает за безопасность в операционных системах?

а) Подсистема графического интерфейса

б) Подсистема управления памятью

в) Подсистема безопасности ✓

г) Подсистема ввода-вывода

П3. Что обеспечивают комплексные системы защиты корпоративных сетей?

а) Только защиту от вирусов

б) Только контроль доступа в интернет

в) Комплексную защиту всех компонентов сети ✓

г) Только резервное копирование

П4. Какой инструмент используется для контроля работы пользователей?

а) Системы мониторинга и аудита ✓

б) Текстовые редакторы

в) Графические редакторы
г) Системы проектирования

П5. Что такое ГосСОПКА?

а) Государственная система обнаружения и предупреждения компьютерных атак ✓
б) Государственная система обслуживания персональных компьютеров
в) Городская система оповещения о погоде
г) Главная система обработки платежей

П6. Какие средства защиты включают комплексные системы?

а) Только антивирусную защиту
б) Только межсетевые экраны
в) Многоуровневую систему различных средств защиты ✓
г) Только системы резервного копирования

П7. Что обеспечивает безопасность в СУБД?

а) Только быстрый доступ к данным
б) Только хранение больших объемов данных
в) Защиту целостности и конфиденциальности данных ✓
г) Только создание отчетов

П8. Какой компонент является основой доверенной аппаратной среды?

а) Монитор с большей диагональю
б) Клавиатура с подсветкой
в) Аппаратные модули безопасности (TPM) ✓
г) Мышь с дополнительными кнопками

П9. Что контролируют системы мониторинга пользователей?

а) Только время прихода на работу
б) Только использование интернета
в) Различные аспекты деятельности пользователей ✓
г) Только перерывы на обед

П10. Какой принцип лежит в основе комплексных систем защиты?

а) Принцип минимальной достаточности
б) Принцип "чем больше, тем лучше"
в) Принцип многоуровневой защиты ✓
г) Принцип случайного выбора

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-3.5.1. Принимает решения о необходимости защиты информации, содержащейся в ИС

П1. Какой объект защиты является первоочередным в рамках системного подхода к защите от компьютерных атак?
а) Отдельные файлы с данными;
б) Антивирусное программное обеспечение;
в) Компьютерные системы и их компоненты; [✓]
г) Сетевые кабели.
Ответ: в) Компьютерные системы и их компоненты

П2. Какое решение необходимо принять для противодействия угрозе несанкционированного восстановления данных с выведенных из эксплуатации носителей?
а) Внедрение системы гарантированного уничтожения информации; [✓]
б) Установка межсетевого экрана;
в) Настройка контентной фильтрации;
г) Применение средств создания VPN.
Ответ: а) Внедрение системы гарантированного уничтожения информации

П3. Решение о необходимости защиты от утечек информации по техническим каналам принимается при выявлении рисков, связанных с:
а) Прямым сетевым взломом;
б) Побочными электромагнитными излучениями и наводками; [✓]
в) Неправильной настройкой семафоров;
г) Отказом службы печати.
Ответ: б) Побочными электромагнитными излучениями и наводками

П4. Какое решение является основой для регламентации процессов использования и администрирования информационной системы?
а) Применение организационных методов защиты; [✓]
б) Установка последних обновлений ОС;
в) Покупка самого дорогого firewall;
г) Отключение системы от сети.
Ответ: а) Применение организационных методов защиты

П5. Установите соответствие между выявленной угрозой и решением о необходимости применения класса средств защиты:

Угроза	Класс средств защиты
1. Перехват данных, передаваемых между офисами через Интернет.	а) Средства создания VPN
2. Несанкционированное извлечение данных с выведенных из эксплуатации носителей.	б) Средства гарантированного уничтожения информации

3. Доступ в сеть организации с целью кражи конфиденциальных данных.	в) Межсетевое экранирование
4. Утечка информации через микрофон или камеру.	г) Средства выявления утечек по техническим каналам

Правильный ответ:
1 – а, 2 – б, 3 – в, 4 – г

П6. Установите соответствие между компонентом ИС и решением о необходимости его защиты:

Компонент ИС	Решение о защите
1. Канал связи	а) Защита от несанкционированного прослушивания и перехвата (шифрование, VPN).
2. База данных	б) Защита от несанкционированного доступа и манипуляций (СУБД, контроль доступа).
3. Электропитание	в) Защита от сбоев, обеспечивающая доступность системы (ИБП, резервирование).

Правильный ответ:
1 – а, 2 – б, 3 – в

П7. Установите правильную последовательность принятия решений о необходимости защиты информации:
а) Идентификация информационных активов и систем.
б) Анализ потенциальных угроз и уязвимостей.
в) Оценка рисков для каждого актива.
г) Принятие решения о необходимости защиты для активов с неприемлемым уровнем риска.
д) Выбор конкретных средств и методов защиты.
Ответ: АБВГД

П8. Установите правильную последовательность приоритетов для защиты компьютерной системы:
а) Обеспечение доступности системы (электропитание, отказоустойчивость).
б) Защита целостности данных (контроль доступа, СУБД).
в) Защита конфиденциальности (шифрование, VPN).
г) Реализация систем мониторинга и аудита (обнаружение атак).
Ответ: АБВГ

П9. Как называется принцип, требующий предоставления пользователям и системам минимальных прав доступа, необходимых для выполнения их функций?
Правильный ответ: Принцип минимальных привилегий (Principle of Least Privilege)

П10. Как называется комплексный подход, при котором защита строится на всех уровнях компьютерной системы?
Правильный ответ: Системный подход к защите информации.

ПК-3.5.2. Принимает решения о необходимости защиты информации, содержащейся в ИС

П1. Какое средство защиты необходимо выбрать для безопасного

обмена данными между удаленными филиалами компании через Интернет?
а) Система контроля работы пользователей;
б) Средство создания виртуальных частных сетей (VPN); [✓]
в) Доверенная аппаратная среда;
г) Средство гарантированного уничтожения информации.
Ответ: б) Средство создания виртуальных частных сетей (VPN)

П2. Какое средство является наиболее эффективным для предотвращения несанкционированного доступа к ресурсам корпоративной сети извне?
а) Средства создания VPN;
б) Средства выявления утечек информации;
в) Средства межсетевого экранирования; [✓]
г) Системы безопасности СУБД.
Ответ: в) Средства межсетевого экранирования

П3. Какое средство обеспечивает аппаратную основу для безопасного хранения криптографических ключей?
а) Межсетевой экран;
б) Доверенный аппаратный модуль (TPM); [✓]
в) Система контроля доступа;
г) Антивирусное ПО.
Ответ: б) Доверенный аппаратный модуль (TPM)

П4. Какой метод защиты информации направлен на блокировку доступа к запрещенным веб-ресурсам?
а) Межсетевое экранирование;
б) Контентная фильтрация; [✓]
в) Создание VPN;
г) Гарантированное уничтожение.
Ответ: б) Контентная фильтрация

П5. Установите соответствие между целью защиты и выбираемым для ее достижения средством:

Цель защиты	Средство защиты
1. Обнаруживать и пресекать попытки несанкционированного доступа в сети в реальном времени.	а) Система обнаружения вторжений (IDS)
2. Контролировать и регистрировать действия сотрудника за рабочим компьютером.	б) Система контроля работы пользователей
3. Обеспечить безопасность операционной системы на уровне ядра.	в) Подсистема безопасности ОС
4. Защитить прикладное программное обеспечение от уязвимостей.	г) Подсистема безопасности ПО

Правильный ответ:
1 – а, 2 – б, 3 – в, 4 – г

П6. Установите соответствие между методом и средством защиты информации:

Метод защиты	Средство защиты
1. Обнаружение сетевых атак	а) Антивирусное ПО, системы обнаружения вторжений (IDS)
2. Контроль доступа	б) Межсетевые экраны, системы аутентификации
3. Шифрование данных	в) Средства VPN, средства шифрования дисков
4. Резервирование и восстановление	г) Системы бесперебойного питания (ИБП), системы backup

Правильный ответ:
1 – а, 2 – б, 3 – в, 4 – г

П7. Установите правильную последовательность выбора средств защиты для вновь создаваемой компьютерной системы:
а) Определение критичных активов и угроз.
б) Выбор организационных методов защиты.
в) Выбор технических средств защиты (МЭ, СОВ, антивирус).
г) Создание доверенной аппаратной среды (при необходимости).
д) Внедрение систем мониторинга и аудита.
Ответ: АБВГД

П8. Установите правильную последовательность построения эшелонированной защиты (Defense in Depth):
а) Защита периметра (межсетевые экраны).
б) Защита сети (сегментация, IDS).
в) Защита узлов (антивирусы, обновления ОС).
г) Защита приложений (WAF, безопасное кодирование).
д) Защита данных (шифрование, контроль доступа).
Ответ: АБВГД

П9. Как называется методология построения защищенных систем, предполагающая создание нескольких уровней защиты?
Правильный ответ: Эшелонированная защита (Defense in Depth)

П10. Как называется средство, обеспечивающее контроль и регистрацию действий пользователей для выявления инсайдерских угроз?
Правильный ответ: Система контроля работы пользователей (User Activity Monitoring).

ПК-3.5.3. Анализирует компьютерную систему с целью определения необходимого уровня защищенности и доверия на основе менеджмента, аудита и оценки рисков информационной безопасности.

П1. Какой процесс позволяет выявить слабые места компьютерной системы, которые могут быть использованы злоумышленником?
а) Межсетевое экранирование;
б) Аудит и оценка защищенности (сканирование уязвимостей); [✓]
в) Контентная фильтрация;
г) Резервное копирование.

Ответ: б) Аудит и оценка защищенности (сканирование уязвимостей)

П2. Какой подход лежит в основе определения необходимого уровня защищенности на основе анализа потенциального ущерба?

а) Анализ рисков информационной безопасности; [✓]

б) Слепое доверие;

в) Копирование конфигурации соседней организации;

г) Интуитивный метод.

Ответ: а) Анализ рисков информационной безопасности

П3. Уровень доверия к операционной системе определяется на основе анализа:

а) Стоимости лицензии;

б) Наличия и эффективности встроенной подсистемы безопасности; [✓]

в) Популярности среди домашних пользователей;

г) Количества установленных обновлений.

Ответ: б) Наличия и эффективности встроенной подсистемы безопасности

П4. Оснащение центров ГосСОПКА является примером реализации какого уровня управления информационной безопасностью?

а) Локального (уровень рабочей станции);

б) Объектного (уровень отдельной системы);

в) Корпоративного (уровень сети организации);

г) Национального (государственного) уровня. [✓]

Ответ: г) Национального (государственного) уровня

П5. Установите соответствие между этапом анализа и его содержанием:

Этап анализа	Содержание этапа
1. Идентификация активов	а) Определение стоимости и критичности информационных и технических ресурсов.
2. Оценка уязвимостей	б) Выявление недостатков конфигурации, ПО и политик безопасности, которые могут быть использованы.
3. Оценка угроз	в) Анализ потенциальных источников и методов атаки, их мотивации и вероятности реализации.
4. Определение уровня защищенности	г) Сопоставление текущего состояния системы с требованиями стандартов и лучших практик.

Правильный ответ:

1 – а, 2 – б, 3 – в, 4 – г

П6. Установите соответствие между понятием и его описанием в контексте анализа защищенности:

Понятие	Описание
1. Угроза	а) Потенциальная возможность нарушения безопасности системы.
2. Уязвимость	б) Слабость в системе, которая может быть использована для нарушения ее безопасности.
3. Риск	в) Комбинация вероятности реализации угрозы и размера потенциального ущерба.

4. Актив	г) Любой ресурс, представляющий ценность для организации.

Правильный ответ:
1 – а, 2 – б, 3 – в, 4 – г

П7. Установите правильную последовательность этапов анализа рисков для определения необходимого уровня защищенности ИС:
а) Выявление активов и уязвимостей системы.
б) Идентификация и оценка потенциальных угроз.
в) Расчет уровня риска для каждого актива.
г) Выбор и обоснование контрмер (средств защиты).
д) Разработка решений по минимизации принятых рисков.
Ответ: АБВГД

П8. Установите правильную последовательность цикла непрерывного повышения защищенности (PDCA):
а) Планирование (Plan) — разработка политик и мер.
б) Выполнение (Do) — внедрение запланированных мер.
в) Проверка (Check) — мониторинг и аудит эффективности.
г) Действие (Act) — корректирующие и предупреждающие действия.
Ответ: АБВГ

П9. Как называется принцип, при котором анализ защищенности и меры по ее повышению должны повторяться циклически?
Правильный ответ: Цикл непрерывного улучшения (PDCA - Plan-Do-Check-Act)

Р10. Как называется документированная оценка соответствия системы требованиям стандартов безопасности?
Правильный ответ: Аудит информационной безопасности (Security Audit).

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 №____