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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ОПЕРАЦИИ И АТАКИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ СЕТЯХ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

Форма промежуточной аттестации: зачет

2025

Оценочные материалы по дисциплине Операции и атаки в компьютерных системах сетях

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 Операции и атаки в компьютерных системах сетях 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 Операции и атаки в компьютерных системах сетях

1. Паспорт оценочных материалов по дисциплине «Операции и атаки в компьютерных системах сетях»

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-3.6 Способен участвовать в работах по противодействию информационным атакам и операциям, реализуемым в компьютерных системах и сетях	ПК-3.6.1 Выполняет анализ защищенности компьютерных систем и сетей с использованием сканеров безопасности	Знать: принципы и подходы противодействия информационным атакам и операциям в компьютерных системах и сетях, типологию современных кибератак и возможные последствия их осуществления, способы распознавания и предупреждения целенаправленных информационных воздействий. Уметь: осуществлять комплексный анализ текущих угроз и рисков в информационно-технических инфраструктурах организаций, организовывать мероприятия по обнаружению и предупреждению вредоносных воздействий на компьютерные системы и сети, использовать специализированные программные комплексы и инструменты для мониторинга и анализа информационных потоков Владеть: навыками анализа состояния защищённости компьютерных систем и сетевых инфраструктур, способностью разрабатывать стратегии и меры предосторожности против информационных атак, умением оперативно реагировать на признаки нарушения информационной безопасности	Тема 1. Содержание понятия безопасность и его структура. Тема 2. Стандарты информационной безопасности.	Реферат (тема 1,2)	Тест (В1-8)

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
		и обеспечивать устойчивую работу систем и сетей.			
	ПК-3.6.2 Реализует анализ защищенности сетевых сервисов автоматического реагирования на попытки несанкционированного доступа к ресурсам	Знать: основные концепции и принципы кибербезопасности, методы и инструменты анализа защищенности сетевых сервисов, типы угроз и уязвимостей, связанных с сетевыми сервисами., принципы работы систем автоматического реагирования на инциденты, нормативные документы и стандарты в области информационной безопасности. Уметь: проводить анализ защищенности сетевых сервисов с использованием специализированных инструментов, идентифицировать потенциальные уязвимости и угрозы для сетевых сервисов., настраивать системы автоматического реагирования на инциденты, разрабатывать рекомендации по улучшению защищенности сетевых сервисов, оценивать эффективность мер по защите ресурсов. Владеть: инструментами для анализа и тестирования защищенности (например, сканеры уязвимостей, системы обнаружения вторжений), методами мониторинга и анализа событий безопасности, процессами реагирования на инциденты и управления	Тема 3. Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации Тема 4. Модели управления доступом к информаци и. Модели поддержан ия целостност и информации	Реферат (тема 3,4)	Тест (В9-15)

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
		ими, навыками работы с отчетами по инцидентам и анализу их причин.			
	ПК-3.6.3 Структурирует аналитическую информацию для составления отчётов по результатам проверок качества противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях	Знать: стандарты и требования к отчетности в области кибербезопасности, основные методы сбора и анализа данных о безопасности информационных систем, структуру и содержание отчетов по результатам проверок, инструменты визуализации данных и представления аналитической информации. Уметь: собирать, обрабатывать и анализировать данные о безопасности из различных источников, структурировать информацию для создания ясных и понятных отчетов, формулировать выводы и рекомендации на основе проведенного анализа, использовать инструменты для создания визуальных представлений данных (графики, диаграммы). Владеть: техниками написания отчетов, включая использование стандартных шаблонов и форматов, инструментами для анализа данных (например, Excel, BI-системы), навыками презентации аналитической информации для различных аудиторий (технических специалистов, руководства).	Тема 5. Аудит вычислительной системы и архивация. Анализ уязвимости системы. DLP- системы. Системы обнаружения вторжений	Реферат (тема 5)	Тест (В16-25)

2. Оценочные материалы по дисциплине «Операции и атаки в компьютерных системах сетях»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема 1. Содержание понятия безопасность и его структура
1. Определение и структура понятия "безопасность": исторический и современный контексты.
2. Классификация угроз информационной безопасности: виды и источники.
3. Алгоритмы шифрования как средства поддержки информационной безопасности.
4. Структура системы управления информационной безопасностью: элементы и взаимосвязи.
5. Методы оценки рисков в информационной безопасности: подходы и инструменты.
6. Значение политик безопасности для организации: разработка и реализация.
7. Проектирование алгоритмов поддержки информационной безопасности: этапы и методологии.
8. Роль технологий аутентификации и авторизации в обеспечении информационной безопасности.
9. Информационная безопасность в облачных технологиях: вызовы и решения. .
10. Будущее информационной безопасности: новые технологии и вызовы.

Тема 2. Стандарты информационной безопасности
1. Обзор международных стандартов информационной безопасности: ISO/IEC 27001 и ISO/IEC 27002.
2. Стандарт NIST Cybersecurity Framework: принципы и применение.
3. Сравнительный анализ стандартов безопасности данных PCI DSS и HIPAA.
4. Роль стандартов в обеспечении безопасности персональных данных: GDPR и другие регуляции.
5. Стандарты безопасности для облачных услуг: Cloud Security Alliance (CSA) и их лучшие практики.
6. Стандарты информационной безопасности в сфере правительственных и военных организаций: FISMA и DIACAP.
7. Аудит и сертификация в области информационной безопасности: роль стандартов и их значение.
8. Стандарты управления инцидентами в информационной безопасности: NIST SP 800-61.
9. Стандарты безопасности программного обеспечения: OWASP Top Ten и их значение.
10. Будущее стандартов информационной безопасности: тренды и вызовы.

Тема 3. Сценарий Идентификация- Аутентификация- Авторизация и варианты реализации.
1. Понятие идентификации, аутентификации и авторизации: основные различия и взаимосвязи.
2. Методы идентификации пользователей: от традиционных до современных подходов.
3. Аутентификация: способы и технологии, применяемые в информационных системах.
4. Авторизация: модели доступа и управление правами пользователей.
5. Сценарий интеграции идентификации, аутентификации и авторизации в веб-приложениях.
6. Безопасность идентификации и аутентификации: основные угрозы и способы защиты.
7. Биометрические технологии в идентификации и аутентификации: преимущества и недостатки.
8. Использование многофакторной аутентификации: принципы и практика.
9. Сценарии авторизации в облачных сервисах: вызовы и решения.

10. Будущее идентификации, аутентификации и авторизации: тренды и инновации

Тема 4. Модели управления доступом к информации. Модели поддержания целостности информации
1. Обзор моделей управления доступом: RBAC, ABAC и MAC.
2. Роль управления доступом в информационной безопасности: задачи и вызовы.
3. Модель управления доступом на основе ролей (RBAC): применение и примеры.
4. Атрибутно-ориентированное управление доступом (ABAC): принципы и применение.
5. Модель управления доступом на основеMandatory Access Control (MAC): особенности и применение.
6. Поддержка целостности информации: методы и технологии.
7. Модели обеспечения целостности информации в распределенных системах.
8. Интеграция управления доступом и обеспечения целостности: практические аспекты.
9. Аудит и мониторинг доступа: роль в поддержании целостности информации.
10. Будущее моделей управления доступом и целостности информации: тренды и инновации.

Тема 5. Аудит вычислительной системы и архивация. Анализ уязвимости системы. DLP- системы. Системы обнаружения вторжений
1. Аудит вычислительных систем: методы и подходы.
2. Архивация данных: лучшие практики и технологии.
3. Анализ уязвимостей: процесс и инструменты.
4. DLP-системы: принципы работы и применение.
5. Системы обнаружения вторжений (IDS): классификация и механизмы работы.
6. Интеграция аудита и анализа уязвимостей: как повысить безопасность системы.
7. Роль DLP-систем в защите конфиденциальной информации: вызовы и решения.
8. Сравнительный анализ систем обнаружения вторжений: IDS против IPS.
9. Аудит соблюдения стандартов безопасности: методология и важность.
10. Будущее аудита и защиты информации: новые тренды и инновации.

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) тре-

буют 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 практических заданий

Тест 1. Тема. Содержание понятия безопасность и его структура. Проектирование алгоритмов поддержки информационной безопасности.

1. Что такое информационная безопасность?

А) Защита информации от несанкционированного доступа +

Б) Процесс управления данными

В) Поддержка компьютерного оборудования
Г) Создание программного обеспечения

2. Какой из следующих элементов не является частью структуры информационной безопасности?
А) Конфиденциальность
Б) Целостность
В) Доступность
Г) Производительность +

3. Какой из следующих аспектов относится к целостности информации?
А) Защита от несанкционированного доступа
Б) Обеспечение точности и полноты данных +
В) Ограничение доступа к данным
Г) Устойчивость к физическим повреждениям

4. Какой из перечисленных методов используется для обеспечения конфиденциальности информации?
А) Шифрование +
Б) Резервное копирование
В) Аудит безопасности
Г) Мониторинг действий пользователей

5. Что включает в себя проектирование алгоритмов поддержки информационной безопасности?
А) Определение требований к программному обеспечению
Б) Разработка и тестирование алгоритмов защиты
В) Оценка рисков и уязвимостей
Г) Все перечисленное +

6. Какой из следующих процессов не относится к управлению рисками в информационной безопасности?
А) Идентификация угроз
Б) Оценка уязвимостей
В) Обновление программного обеспечения +
Г) Разработка стратегии защиты

7. Что такое риск в контексте информационной безопасности?
А) Вероятность утраты информации +
Б) Стоимость защиты информации
В) Уровень доступа к данным
Г) Количество инцидентов безопасности

8. Какой принцип безопасности подразумевает минимизацию прав доступа пользователей?
А) Принцип конфиденциальности
Б) Принцип наименьших привилегий +
В) Принцип целостности
Г) Принцип доступности

9. Какой из следующих методов обеспечивает защиту данных от потери?
А) Шифрование
Б) Архивация +

В) Аудит
Г) Аутентификация

10. Какой стандарт обычно используется для оценки систем управления информационной безопасностью?
А) ISO 9001
Б) ISO 27001 +
В) ISO 14001
Г) ISO 50001

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

Тест 2. Тема. Стандарты информационной безопасности

1. Что такое стандарты информационной безопасности?
А) Нормативные документы, определяющие требования к безопасности информации +
Б) Программное обеспечение для защиты данных
В) Процедуры резервного копирования данных
Г) Методики обучения сотрудников

2. Какой из следующих стандартов относится к управлению информационной безопасностью?
А) ISO 9001
Б) ISO 27001 +
В) ISO 14001
Г) ISO 50001

3. Какой стандарт определяет требования к системам управления информационной безопасностью (СУИБ)?
А) ISO 9001
Б) ISO 27001 +
В) ISO 20000
Г) ISO 31000

4. Какой стандарт фокусируется на управлении рисками в области информационной безопасности?
А) ISO 27005 +
Б) ISO 27002
В) ISO 9001
Г) ISO 14001

5. Какой из следующих стандартов содержит рекомендации по лучшим практикам в области управления безопасностью информации?

А) ISO 27002 +
Б) ISO 20000
В) ISO 50001
Г) ISO 14001

6. Какой стандарт касается защиты персональных данных?
А) ISO 27018 +
Б) ISO 27001
В) ISO 9001
Г) ISO 31000

7. Что подразумевает сертификация по стандарту ISO 27001?
А) Оценка качества продукции
Б) Подтверждение соответствия требованиям управления информационной безопасностью +
В) Проверка финансовой отчетности
Г) Аудит экологической безопасности

8. Какой стандарт применяется для обеспечения безопасности платежной информации?
А) PCI DSS +
Б) ISO 27001
В) ISO 14001
Г) ISO 20000

9. Какой стандарт определяет требования к управлению безопасностью в облачных вычислениях?
А) ISO 27017 +
Б) ISO 27001
В) ISO 9001
Г) ISO 31000

10. Какой из следующих стандартов фокусируется на управлении информационными технологиями и их безопасностью?
А) COBIT+
Б) ISO 14001
В) ISO 50001
Г) ISO 9001

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

Тест №3 Тема. Сценарий Идентификация- Аутентификация- Авторизация и варианты реализации.

1. Что такое идентификация в контексте информационной безопасности?
А) Проверка личности пользователя +
Б) Процесс определения прав доступа
В) Установка пароля для доступа
Г) Процесс регистрации пользователя

2. Какой из следующих процессов следует за идентификацией?
А) Аутентификация +
Б) Авторизация
В) Шифрование
Г) Мониторинг

3. Что подразумевает аутентификация?
А) Определение, кто является пользователем
Б) Проверка, является ли пользователь тем, за кого он себя выдает +
В) Установка уровней доступа
Г) Оценка рисков системы

4. Какой из следующих методов не является методом аутентификации?
А) Пароль
Б) Биометрические данные +
В) Токен
Г) Шифрование

5. Что такое авторизация?
А) Процесс проверки личности пользователя
Б) Определение прав доступа пользователя к ресурсам +
В) Установка пароля для доступа
Г) Обновление учетной записи пользователя

6. Какой из следующих методов можно использовать для авторизации?
А) Ролевое управление доступом (RBAC) +
Б) Шифрование
В) Аутентификация по отпечатку пальца
Г) Мониторинг активности пользователей

7. Какой из следующих подходов к аутентификации считается наиболее безопасным?
А) Использование пароля
Б) Двухфакторная аутентификация (2FA) +
В) Одинаковые пароли для разных сервисов
Г) Аутентификация по IP-адресу

8. Что такое "единоразовые пароли" (One-Time Password, OTP)?
А) Пароли, которые не меняются
Б) Пароли, действительные только для одной сессии или операции +
В) Пароли, которые используются каждый раз при входе
Г) Пароли, которые можно использовать многократно

9. Какой из следующих методов аутентификации использует биометрические данные?
А) Пароль

Б) Смарт-карта
В) Распознавание лица+
Г) Токен

10. Что такое "принцип наименьших привилегий" в контексте авторизации?
А) Пользователи должны иметь доступ ко всем ресурсам
Б) Пользователи должны иметь только тот доступ, который необходим для выполнения их задач +
В) Все пользователи имеют одинаковые права
Г) Доступ предоставляется на основании возраста пользователя

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

Тест №4 Тема. Модели управления доступом к информации. Модели поддержания целостности информации

1. Что такое модель управления доступом?
А) Метод защиты физического доступа к зданиям
Б) Система правил, определяющая, кто может получить доступ к информации +
В) Процесс резервного копирования данных
Г) Метод анализа рисков

2. Какой из следующих типов управления доступом является наиболее распространенным?
А) Доступ на основе ролей (RBAC) +
Б) Доступ на основе атрибутов (ABAC)
В) Доступ на основе списков контроля доступа (ACL)
Г) Доступ на основе времени (TBAC)

3. Что подразумевает модель доступа на основе ролей (RBAC)?
А) Доступ предоставляется на основе индивидуальных пользователей
Б) Доступ определяется на основе ролей, назначенных пользователям +
В) Доступ зависит от времени суток
Г) Доступ контролируется на основе географического положения

4. Какой из следующих методов поддерживает целостность информации?
А) Шифрование данных
Б) Резервное копирование
В) Хеширование данных
Г) Все перечисленное +

5. Что такое хеширование?
А) Метод шифрования данных
Б) Процесс создания уникального значения для данных фиксированной длины +

В) Процесс восстановления данных
Г) Метод резервного копирования

6. Какой из следующих типов управления доступом основан на атрибутах пользователей?
А) RBAC
Б) ABAC +
В) MAC
Г) DAC

7. Что означает модель управления доступом с учетом обязательной политики (MAC)?
А) Пользователи могут изменять свои права доступа
Б) Доступ определяется политиками безопасности, установленными администратором +
В) Доступ основан на ролях пользователей
Г) Доступ зависит от времени и местоположения

8. Какой из следующих методов помогает предотвратить несанкционированные изменения данных?
А) Аутентификация пользователей
Б) Контроль версий +
В) Шифрование
Г) Архивация данных

9. Что позволяет обеспечить целостность данных в процессе их передачи?
А) Шифрование
Б) Использование контрольных сумм +
В) Аудит доступа
Г) Все перечисленное

10. Какой из следующих методов управления доступом позволяет пользователю самостоятельно управлять своими правами доступа?
А) DAC (Доступ на основе контроля) +
Б) MAC (Обязательный контроль доступа)
В) RBAC (Доступ на основе ролей)
Г) ABAC (Атрибутный контроль доступа)

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

Тест №5 Тема 5. Аудит вычислительной системы и архивация. Анализ уязвимости системы. DLP- системы. Системы обнаружения вторжений

1. Что такое аудит вычислительной системы?
А) Процесс создания резервных копий данных
Б) Оценка и проверка систем безопасности и процессов на соответствие стандартам+
В) Методы шифрования данных
Г) Обновление программного обеспечения

2. Какова основная цель архивации данных?
А) Защита от вирусов
Б) Увеличение скорости работы системы
В) Сохранение данных на случай их утраты или повреждения +
Г) Повышение производительности сети

3. Что такое анализ уязвимости системы?
А) Процесс шифрования данных
Б) Определение недостатков и уязвимостей в информационных системах +
В) Оценка производительности оборудования
Г) Разработка новых программных решений

4. Какой из следующих инструментов используется для анализа уязвимостей?
А) Антивирусное ПО
Б) Сканы на уязвимости +
В) Файрвол
Г) Шифровальщик

5. Что такое DLP-система?
А) Система защиты от вредоносного ПО
Б) Система предотвращения утечки данных +
В) Система резервного копирования
Г) Система аутентификации пользователей

6. Каковы основные функции DLP-системы?
А) Обнаружение, мониторинг и предотвращение утечек конфиденциальной информации +
Б) Шифрование данных
В) Обновление программного обеспечения
Г) Проведение аудита безопасности

7. Что такое система обнаружения вторжений (IDS)?
А) Система, которая предотвращает несанкционированный доступ
Б) Система, которая анализирует и регистрирует подозрительную активность в сети+
В) Система, которая шифрует данные
Г) Система для архивации данных

8. Какой тип IDS анализирует сетевой трафик в реальном времени?
А) Наблюдающая система (Passive IDS)
Б) Активная система (Active IDS)
В) Хостовая система (HIDS)
Г) Сетевая система (NIDS) +

9. Какой из следующих подходов используется для защиты системы от вторжений?
А) Регулярное обновление ПО

Б) Использование антивирусных программ
В) Установка систем обнаружения вторжений (IDS)
Г) Все перечисленное +

10. Какая из следующих задач не относится к функциям аудита вычислительной системы?

А) Оценка соответствия политик безопасности
Б) Анализ производительности сети +
В) Идентификация уязвимостей
Г) Проверка целостности данных

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

1. Какой из следующих типов атак подразумевает перехват и изменение данных между двумя сторонами?

А) Фишинг
Б) Человек посередине (Man-in-the-Middle) +
В) DDoS-атака
Г) SQL-инъекция

2. Что такое DDoS-атака?

А) Атака, направленная на получение конфиденциальных данных
Б) Распределенная атака с использованием нескольких систем для перегрузки сервиса +
В) Атака на серверы с целью их разрушения
Г) Атака с использованием вирусов

3. Какой из следующих методов используется для предотвращения несанкционированного доступа к сети?

А) Файрвол +
Б) Вирусный сканер
В) Антивирусная программа
Г) Архиватор

4. Что такое фишинг?

А) Метод шифрования данных
Б) Стратегия взлома сетевых устройств
В) Попытка обмана пользователей для получения их личной информации +
Г) Способ резервного копирования данных

5. Какой тип атаки направлен на получение доступа к базе данных через уязвимости SQL?

А) XSS-атака
Б) DDoS-атака
В) SQL-инъекция +
Г) Фишинг

6. Что такое XSS-атака?
А) Внедрение вредоносного кода в веб-страницы +
Б) Перехват сетевого трафика
В) Атака на сервер с целью его уничтожения
Г) Атака на систему управления данными

7. Какой из следующих типов атак использует подмену DNS-записей?
А) Спуфинг +
Б) Руткит
В) Фишинг
Г) DDoS-атака

8. Что такое руткит?
А) Программа для резервного копирования
Б) Вредоносное ПО, скрывающее свое присутствие в системе +
В) Антивирусная программа
Г) Инструмент для анализа сетевого трафика

9. Какой из следующих методов позволяет обнаружить вторжения в сеть?
А) IDS (система обнаружения вторжений) +
Б) VPN (виртуальная частная сеть)
В) Антивирус
Г) Файрвол

10. Что такое социальная инженерия?
А) Метод защиты информации
Б) Способы манипуляции людьми для получения конфиденциальной информации +
В) Процесс шифрования данных
Г) Метод резервного копирования

11. Какой из следующих способов используется для защиты от атак типа "отказ в обслуживании"?
А) Использование VPN
Б) Настройка файрвола +
В) Использование DLP-системы
Г) Процесс шифрования

12. Какой из следующих типов атак использует уязвимости в программном обеспечении для выполнения произвольного кода?
А) Вредоносное ПО
Б) Эксплойт +
В) Спуфинг
Г) XSS

13. Что такое "отказ в обслуживании" (DoS)?
А) Атака, создающая временные файлы на сервере
Б) Атака, блокирующая доступ к ресурсу +

В) Атака на базы данных
Г) Атака, использующая вирусы

14. Какой из следующих методов используется для защиты от SQL-инъекций?
А) Файрвол
Б) Шифрование данных
В) Параметризованные запросы+
Г) Использование VPN

15. Что такое шифрование?
А) Процесс создания резервных копий данных
Б) Преобразование данных +
В) Метод анализа сетевого трафика
Г) Процесс обнаружения уязвимостей

16. Какой из следующих типов атак нацелен на перехват логинов и паролей пользователей?
А) DDoS
Б) Фишинг +
В) Руткит
Г) SQL-инъекция

17. Что такое "сниффинг"?
А) Процесс шифрования данных
Б) Перехват и анализ сетевого трафика +
В) Атака на веб-приложения
Г) Метод резервного копирования

18. Какой из следующих методов используется для защиты сетевых соединений?
А) VPN (виртуальная частная сеть) +
Б) Архивирование данных
В) Использование DLP-системы
Г) Запуск антивируса

19. Что такое "вредоносное ПО"?
А) Программное обеспечение, предназначенное для защиты данных
Б) Программное обеспечение, созданное с целью вреда или кражи информации+
В) Программное обеспечение для резервного копирования
Г) Программное обеспечение для управления проектами

20. Какой из следующих методов используется для обнаружения вирусов?
А) IDS
Б) Антивирусные программы +
В) Файрвол
Г) Архивирование

21. Что такое "спуфинг"?
А) Метод защиты от вирусов
Б) Подмена источника данных для обмана +
В) Процесс резервного копирования
Г) Способ анализа данных

22. Какой из следующих методов используется для защиты от кражи данных?
А) Шифрование +
Б) Архивирование
В) Аудит безопасности
Г) Все перечисленное

23. Что такое "вирус"?
А) Программное обеспечение, способное самостоятельно копироваться и распространяться +
Б) Программное обеспечение для защиты данных
В) Программное обеспечение для анализа трафика
Г) Программное обеспечение для архивации данных

24. Соотнесите термин с его определением в контексте коллективной разработки приложений.

Операции:	Атаки:
1. Скачивание данных с удаленного сервера.	А) DDoS (Distributed Denial of Service)
2. Изменение данных в процессе их передачи.	Б). Man-in-the-Middle (MitM)
3. Установление соединения с сервером через фальшивый IP-адрес.	В). Sniffing
4. Атака на ресурсы сервера с целью их недоступности.	Г). Spoofing

Ответ: А4, Б3, В2, Г3

25. Вставьте пропущенное слово в предложение, чтобы оно стало верным и отражало суть коллективной разработки приложений.
Одним из наиболее распространенных видов атак на компьютерные системы является _____, при котором злоумышленник пытается перехватить и изменить данные, передаваемые по сети
Ответ: Man-in-the-Middle (MitM)

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 №____