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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Специальность10.05.01 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 Защищенные информационные системы.

обсуждены и рекомендованы к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

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 Защищенные информационные системы 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 Защищенные информационные системы.

1. Паспорт оценочных материалов по дисциплине «Защищенные информационные системы»

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
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации,	ОПК-6.1. Применяет в профессиональной деятельности знания нормативной правовой базы при организации защиты информации ограниченного доступа в компьютерных системах и сетях	Знать: нормативные правовые акты и методические документы, регламентирующие организацию защиты информации ограниченного доступа в компьютерных системах и сетях. Умеет: Применять в профессиональной деятельности знания нормативных и правовых актов и нормативных методических документов при организации защиты информации ограниченного доступа в информационных системах Владеть: навыками практического применения положений нормативных актов и методических рекомендаций для обеспечения информационной безопасности организаций.	Тема 1. Понятие и особенности функционирования информационной системы (ИС). Архитектуры, применяемые в информационных системах. Тема 2. Основные аспекты построения защищенных информационных систем	Реферат (Тема 1-2) Тест (тема 1-2)	Тест (В 1-6 тестового задания)
	ОПК-6.2 Демонстрирует умения организации	Знать: основные угрозы объекту информатизации и меры физической защиты, используемые для	Тема 3. Определение уровня защищенности	Реферат (Тема 3) Тест (Тема 3)	Тест (В 7-13 тестового задания)

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
Федеральной службы по техническому и экспортному контролю	физической защиты объекта информатизации	минимизации этих угроз. Уметь: проектировать систему физической защиты объекта информатизации, включающую инженерно-технические средства охраны и контроль доступа. Владеет: умениями организации физической защиты информационной системы и обоснованного выбора инженерно-технических средств защиты	данных в информационной системе		
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах,	ОПК-9.1. Демонстрирует умение решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития компьютерных сетей	Знать: современное состояние и перспективные направления развития компьютерных сетей, протоколы и топологии, влияющие на решение профессиональных задач. Умеет: решать задачи защиты информации в информационных системах с учетом текущего состояния и тенденций развития компьютерных сетей. Владеть: навыками выбора оптимальных архитектур и протоколов для построения высокопроизводительных и надежных	Тема 4. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)	Реферат (Тема 4) Тест (Тема 4)	Тест (В 14-18 тестового задания)

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
компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации		сетей в профессиональной деятельности.			
	ОПК-9.2.Демонстрирует умение решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	Знать: текущее состояние и перспективы развития сетей и систем передачи информации, ключевые технологии и протоколы. Уметь: решать задачи защиты информации в информационных системах с учетом текущего состояния и тенденций развития сетей и систем передачи информации Владеть: навыками эффективного использования современных технологий и стандартов передачи информации для успешной реализации профессиональных задач.	Тема 5. Описание угроз безопасности информации (модель угроз безопасности информации) Тема 6. Методы выбора системы защиты информации	Реферат (Тема 5-6) Тест (Тема 5-6) Практическое задание (Тема 1-6)	Тест (В 19-25 тестового задания)

2. Оценочные материалы по дисциплине «Базы данных»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема 1. Понятие и особенности функционирования информационной системы (ИС). Архитектуры, применяемые в информационных системах.

1. Понятие и основные функции информационной системы
2. Классификация информационных систем по типам и областям применения
3. Особенности жизненного цикла информационной системы
4. Модель функционирования современной информационной системы
5. Типы архитектур информационных систем: концептуальный обзор
6. Многослойная архитектура в информационных системах: принципы и особенности
7. Клиент-серверная архитектура: понятие, преимущества и недостатки
8. Модель «триуровневая» архитектура ИС: структура и применение
9. Модели архитектур облачных информационных систем
10. Интеграция и взаимодействие различных архитектур в сложных информационных системах
11. Безопасность и защиты информации в архитектурах информационных систем
12. Роль архитектурных решений в повышении эффективности информационных систем
13. Современные тенденции развития архитектур информационных систем
14. Преимущества и ограничения использования микросервисной архитектуры в ИС
15. Практические примеры реализации архитектур в конкретных областях (банки, здравоохранение, торговля)

Тема 2. Основные аспекты построения защищенных информационных систем.

1. Понятие и основные принципы защиты информационных систем
2. Классификация угроз и рисков для информационных систем
3. Методы и средства обеспечения информационной безопасности
4. Аутентификация и авторизация в защищенных информационных системах
5. Протоколы шифрования и их роль в обеспечении конфиденциальности данных
6. Модель защиты информации — концепция «CIA triad» (Конфиденциальность, Целостность, Доступность)
7. Методы обнаружения и предотвращения кибератак на информационные системы
8. Планирование политики безопасности и управление рисками
9. Защита сети: файрволы, IDS/IPS, VPN и другие средства

10. Обеспечение безопасности при использовании облачных технологий
11. Криптографические средства и их применение в информационной безопасности
12. Методы защиты персональных данных и соответствие стандартам (например, GDPR, FSTEC)
13. Аудит безопасности информационных систем: задачи и инструменты
14. Обучение сотрудников и культура безопасности в организации
15. Современные вызовы и тенденции в построении защищенных информационных систем

Тема 3. Определение уровня защищенности данных в информационной системе

1. Понятие и методология оценки уровня защищенности данных
2. Критерии и показатели уровня защищенности информации
3. Методы и инструменты оценки рисков и уязвимостей данных
4. Стандарты и нормативы оценки уровня защищенности данных (например, ISO/IEC 27001, GDPR)
5. Модель оценки защищенности данных на основе уровня угроз
6. Методы количественной и качественной оценки защищенности информации
7. Практические методы тестирования и аудита защищенности данных
8. Роль оценки защищенности данных в управлении ИТ-безопасностью
9. Использование метрик и KPI для измерения уровня безопасности данных
10. Оценка уровня защищенности в рамках информационных систем с многоуровневой архитектурой
11. Инструменты автоматизированной оценки защищенности данных
12. Особенности определения уровня защищенности при использовании облачных технологий
13. Кейс-аналитика: оценка уровня защищенности данных в конкретных бизнес-проектах
14. Методы повышения уровня защиты данных на основе результатов оценки
15. Проблемы и перспективы стандартизации оценки защищенности данных в ИС

Тема 4. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)

1. Понятие модели нарушителя в информационной безопасности
2. Основные типы источников угроз: внутренние и внешние
3. Классификация злоумышленников по мотивам и возможностям
4. Социальные инженеры: роль человеческого фактора в атаках
5. Профессиональные киберпреступники: инструменты и методы атак
6. Государственные и террористические источники угроз: особенности и цели
7. Роль случайных и непреднамеренных нарушителей
8. Анализ возможностей различных типов киберзлоумышленников
9. Модель нарушителя: этапы и сценарии реализации атаки
10. Инструменты и методы оценки потенциальных возможностей нарушителя
11. Риски и слабые места, используемые в атаках различными источниками
12. Обоснование необходимости выявления источников угроз и их возможностей
13. Практические подходы к моделированию и анализу поведения нарушителей
14. Стратегии защиты, основанные на моделях нарушителя и его возможностях
15. Современные вызовы в оценке и моделировании потенциальных источников атак

Тема 5. Описание угроз безопасности информации (модель угроз безопасности информации)

1. Понятие и структура модели угроз безопасности информации

2. Классификация угроз информации по типам и источникам
3. Основные виды угроз: конфиденциальности, целостности и доступности данных
4. Модель угроз безопасности информации: этапы и компоненты
5. Процесс идентификации угроз в информационной системе
6. Техники анализа и оценки угроз безопасности информации
7. Методология построения модели угроз: пример и практические шаги
8. Реальные сценарии угроз безопасности информации и их моделирование
9. Инструменты автоматизированного анализа и моделирования угроз
10. Роль модели угроз в разработке системы защиты информации
11. Обобщенная модель угроз для сложных информационных систем
12. Модель угроз и управление рисками в информационной безопасности
13. Анализ уязвимостей как часть модели угроз безопасности
14. Практический пример построения модели угроз для корпоративной ИТ-инфраструктуры
15. Преимущества и ограничения моделей угроз при обеспечении информационной безопасности

Тема 6. Методы выбора системы защиты информации

1. Основные критерии и подходы к выбору системы защиты информации
2. Методы оценки и сравнения средств защиты в информационных системах
3. Многоуровневый подход к выбору системы защиты информации
4. Ключевые факторы при выборе системы криптографической защиты
5. Оценка эффективности антивирусных и анталюных систем защиты
6. Методы определения необходимых мер по обеспечению безопасности данных
7. Порядок выбора системы защиты в зависимости от уровня угроз и рисков
8. Использование аналитических методов и моделей при выборе средств защиты
9. Методы оценки стоимости и окупаемости системы защиты информации
10. Роль нормативных стандартов и требований при выборе системы защиты
11. Практический подход к выбору системы защиты для малого и среднего бизнеса
12. Автоматизированные системы поддержки принятия решений при выборе защиты информации
13. Модель оценки и выбора системы защиты в условиях ограниченного бюджета
14. Интеграция различных технологий защиты для достижения комплекса безопасности
15. Кейс-аналитика: подбор системы защиты информации для конкретных отраслей (банки, медицина, промышленность)

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 практических заданий

Тема 1. Понятие и особенности функционирования информационной системы (ИС). Архитектуры, применяемые в информационных системах.

Определите понятие информационной системы и опишите основные компоненты (входы,Processing, выходы, управляющие элементы, базы данных).

Проведите обзор популярных архитектур информационных систем: клиент-сервер, многоуровневая, распределенная, облачная.

Для каждой архитектуры определить её преимущества и недостатки, области применения.

Разработайте схему архитектуры выбранной информационной системы (например, многоуровневой) и обозначьте основные элементы.

Обоснуйте выбор архитектуры для конкретной задачи (например, автоматизация учета в предприятии, облачные решения для хранения данных).

Вопросы для самоконтроля:

Что такое архитектура информационной системы и почему она важна?

1. Какие основные виды архитектур информационных систем существуют и в чем их отличия?
2. В чем преимущества многоуровневых архитектур по сравнению с одноуровневыми?
3. Какие особенности распределенных архитектур делают их подходящими для масштабируемых систем?
4. Почему выбор архитектуры ИС важен для обеспечения надежности, безопасности и эффективности работы системы?

Цель работы – развитие навыков анализа и проектирования архитектур информационных систем, понимание их особенностей и области применения.

Используемые материалы: презентация в MS PowerPoint с схемами и краткими описаниями архитектурных решений.

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.

Тема 2. Системы управления базами данных.

Определите понятие системы управления базами данных и опишите её основные функции.

Изучите основные виды систем управлений базами данных (реляционные, иерархические, сетевые, документарные, графовые), их особенности и области применения.

Для выбранного типа СУБД подготовьте пример области применения и сформулируйте преимущества и ограничения этого типа.

Нарисуйте блок-схему архитектуры реляционной системы управления базами данных и обозначьте ключевые компоненты (системный каталог, ядро, интерфейсы, средства хранения данных).

Проанализируйте требования к системе управления базами данных для автоматизации учета и управления информацией в небольшой компании. Обоснуйте, какой тип СУБД лучше всего подходит и почему.

Вопросы для самоконтроля:

Что такое система управления базами данных и какие основные задачи она решает?

1. В чем различие между разными моделями баз данных (реляционная, иерархическая, сетевая, документарная)?
2. Какие преимущества предоставляет использование реляционной модели данных?
3. Какие основные компоненты входят в архитектуру системы управления базами данных?
4. Почему важно правильно выбрать тип СУБД для конкретного приложения или организации?

Цель работы – развитие практических навыков анализа архитектуры систем управления базами данных и понимания их особенностей для оптимального выбора и использования.

Используемые материалы: презентации в MS PowerPoint с схемами архитектур и характеристиками типов баз данных.

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.

Тема 3. Определение уровня защищенности данных в информационной системе

Определите понятие уровня защищенности данных и его значение в контексте информационной безопасности.

Ознакомьтесь с существующими моделями определения уровней защищенности (например, классификация по чувствительности данных: секретные, конфиденциальные, публичные).

Проанализируйте критерии оценки уровня защиты данных: степень защиты, требования к хранению и обработке информации, возможные угрозы.

Выберите пример информационной системы (например, корпоративный сервер, облачное хранилище) и определите уровень защищенности данных в ней, обосновав свой выбор по предложенным критериям.

Разработайте рекомендации по повышению уровня защищенности данных в выбранной системе (использование шифрования, контроль доступа, резервное копирование, аудит).

Вопросы для самоконтроля:

1. Что такое уровень защищенности данных и зачем он нужен?
2. Какие существуют уровни защищенности данных и чем они отличаются?
3. Какие основные критерии используют при оценке уровня защищенности информации?
4. Почему важно правильно определить уровень защищенности данных в информационной системе?
5. Какие меры можно предпринять для повышения уровня защиты данных в организации?

Цель работы – развитие практических навыков оценки и классификации уровня защищенности данных, а также формирование рекомендаций по их защите.

Используемые материалы: презентация в MS PowerPoint с иллюстрациями, схемами и примерами оценки уровня защищенности.

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.

Тема 4. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)

Ознакомьтесь с концепцией модели нарушителя и её роль в информационной безопасности.

Сформулируйте перечень потенциальных источников атак на информационные системы: внутренние и внешние угрозы (например, злоумышленники, конкуренты, недобросовестные сотрудники, технические сбои, природные катастрофы).

Для каждого источника определите его возможные возможности и методы атаки (фишинг, внедрение вредоносного ПО, эксплуатация уязвимостей, социальная инженерия, DDoS-атаки и др.).

Выберите один из источников атак, разработайте сценарий атаки, укажите возможные слабости системы и меры по их устранению или снижению риска.

Создайте таблицу или схему, в которой отражены источники угроз, их возможности и предпринятые меры защиты.

Вопросы для самоконтроля:

1. Что такое модель нарушителя и какая её роль в обеспечении информационной безопасности?
2. Какие основные источники атак возможны в информационных системах?
3. Какие виды атак осуществимы от различных источников угроз?
4. Почему важно знать возможности потенциальных нарушителей при разработке мер защиты?
5. Какие меры позволяют снизить риски и отразить возможности угроз в модели нарушителя?

Цель работы – развитие навыков идентификации источников угроз и оценки их возможностей для формирования адекватных мер защиты информации.

Используемые материалы: презентация в MS PowerPoint с схемами, таблицами и сценариями атак.

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.

Тема 5. Описание угроз безопасности информации (модель угроз безопасности информации)

Определите понятие угрозы безопасности информации и её роль в системе информационной безопасности.

Ознакомьтесь с основными типами угроз: случайные и преднамеренные, внутренние и внешние, технические и организационные.

Проанализируйте главные категории угроз: утечка данных, подделка, отказ в обслуживании, внедрение вредоносного кода, перехват данных, социальная инженерия.

Для каждой категории угроз опишите возможные причины, последствия и области применения.

На основе анализа сформулируйте модель угроз безопасности информации, выделив типы угроз и их приоритеты.

Разработайте рекомендации по защите информации от каждого типа угроз.

Вопросы для самоконтроля:

1. Что такое угроза информации и почему её важно учитывать при проектировании системы безопасности?
2. Какие основные виды угроз существуют и чем они отличаются?
3. Как осуществляется классификация угроз по типам и уровням опасности?
4. В чем важность моделирования угроз для разработки эффективной системы защиты?

5. Какие меры защиты помогают предотвратить или минимизировать ущерб от угроз?

Цель работы – развитие навыков описания и анализа угроз информационной безопасности, а также формирование представления о моделировании угроз для повышения уровня защиты данных.

Используемые материалы: презентация в MS PowerPoint с схемами, классификациями и примерами угроз.

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.

Тема 6. Методы выбора системы защиты информации

Ознакомьтесь с основными критериями и требованиями, которые учитываются при выборе метода защиты информации (например, уровень чувствительности данных, технические возможности, стоимости реализации).

Изучите различные методы защиты информации: криптографические средства, системы контроля доступа, системы обнаружения вторжений, управление идентификацией и аутентификацией, резервное копирование и восстановление данных.

Проанализируйте преимущества и ограничения каждого метода защиты в контексте конкретных сценариев (корпоративные системы, облачные сервисы, мобильные устройства).

Разработайте алгоритм выбора оптимальной системы защиты на основе поставленных требований, бюджета и возможных угроз (например, при высокой чувствительности данных предпочтение отдавать криптографическим средствам и системам контроля доступа).

Создайте сравнительную таблицу или диаграмму, в которой представлены основные методы защиты, их параметры и приоритеты применения в различных условиях.

Вопросы для самоконтроля:

1. Какие основные критерии учитываются при выборе методов защиты информации?
2. Чем отличаются криптографические и не криптографические методы защиты?
3. Как определить наиболее подходящий метод защиты для конкретной организации или системы?
4. Какие ограничения и риски связаны с применением каждого из методов?
5. Почему важно учитывать особенности угроз и требований при выборе системы защиты?

Цель работы – развитие навыков анализа требований и условий для выбора эффективных методов защиты информации, а также умения составлять сравнительные оценки и рекомендации.

Используемые материалы: презентация в MS PowerPoint с схемами, таблицами и примерами методов защиты.

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

Тест №1

Тема 1. Понятие и особенности функционирования информационной системы (ИС). Архитектуры, применяемые в информационных системах

1. Что такое информационная система (ИС)?

А) Совокупность программ и оборудования, позволяющих обрабатывать данные.+

Б) Совокупность процессов, направленных на организацию работы бизнеса.

В) Манипуляция с информацией без использования технологий.

Г) Набор стандартных правил бухгалтерского учета.

2. Основная функция информационной системы заключается в:

А) Фиксации финансовых операций.

Б) Обработке, хранении и распространении информации.+

В) Создании новых технологий.

Г) Управлении производственными ресурсами без обработки информации.

3. Какая из архитектур является наиболее распространенной в современных информационных системах?

А) Монолитная архитектура.

Б) Одноуровневая архитектура.

В) Клиент-серверная архитектура.+

Г) Централизованная архитектура без клиентов.

4. В архитектуре «клиент-сервер» роль клиента заключается в:

А) Обеспечении хранения данных.

Б) Отправке запросов и получении данных с сервера.

В) Администрировании сети.+

Г) Физическом управлении оборудованием.

5. Какие компоненты обычно входят в архитектуру «триуровневая»?

А) Клиент, сервер, база данных.
Б) Пользователь, приложение, сеть.
Г) Представление, бизнес-логика, данные.+
Д) Операционная система, облако, интерфейс.

6. Что из перечисленного является одним из преимуществ многослойных (многоуровневых) архитектур ИС?
А) Упрощение разработки и обслуживания системы.+
Б) Увеличение затрат времени на изменение системы.
В) Ограничение масштабируемости.
Г) Полное отсутствие необходимости в документации.

7. Какова основная причина внедрения архитектур типа «клиент-сервер»?
А) Обеспечить централизованное управление и распределение ресурсов.+
Б) Исключить использование сети.
В) Сделать систему однопользовательской.
Г) Ввести бизнес-логики в физический уровень.

8. В чем заключается отличие архитектуры «монолит» от архитектуры «модульной»?
А) Монолитная — единая целостная система; модульная — состоит из взаимозаменяемых компонентов.+
Б) Монолитная — более гибкая; модульная — менее гибкая.
Г) Монолит — применяется только в аппаратуре; модульная — только в программных системах.
Д) Нет, отличий.

9. Какие задачи обычно решаются с помощью архитектуры типа «микросервисы»?
А) Обеспечение масштабируемости и устойчивости системы.+
Б) Упрощение структур данных.
В) Минимизация использования сети.
Г) Создание единой монолитной системы.

10. Какие элементы входят в архитектурную модель «облачная» (cloud) ИС?
А) Пользователи, приложение, устройство хранения данных.
Б) Облачные сервисы, клиентские устройства, инфраструктура облака.+
В) Тонкие клиенты и центральный сервер.
Г) Только физическое оборудование без программных компонентов.

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 2. Основные аспекты построения защищенных информационных систем

1. Какое из следующих определений наиболее точно отражает понятие «защищенная информационная система»?
А) Система, использующая только криптографические средства.
Б) Информационная система, построенная с учетом мер по обеспечению конфиденциальности, целостности и доступности информации.+
В) Любая система, подключенная к сети Интернет.
Г) Система, в которой не используются методы аутентификации.

2. В какой области основное внимание уделяется предотвращению несанкционированного доступа к информации?
А) Обеспечение доступности.
Б) Обеспечение целостности.
В) Обеспечение конфиденциальности.+
Г) Обеспечение скорости обработки данных.

3. Что из перечисленного является ключевым элементом «механизмов аутентификации»?
А) Шифрование данных.
Б) Проверка личности пользователя.+
В) Контроль доступа.
Г) Создание резервных копий.

4. Какой принцип лежит в основе построения системы контроля доступа?
А) Разделение информации по уровням секретности.
Б) Предоставление определенной категории пользователей определенных прав доступа.+
В) Шифрование всей информации.
Г) Автоматическое удаление устаревших данных.

5. Что такое «механизм обнаружения вторжений» (IDS)?
А) Система, автоматически предотвращающая попытки вторжений.
Б) Инструмент, регистрирующий и анализирующий подозрительную активность для выявления вторжений.+
В) Средство шифрования данных.
Г) Программа для резервного копирования.

6. Какие меры относятся к техническим аспектам построения защищенной ИС?
А) Политики безопасности и инструкции.
Б) Использование межсетевых экранов, систем шифрования и антивирусных программ.+
В) Обучение персонала.
Г) Регулярные совещания отдела безопасности.

7. Почему важно реализовывать полноценную систему управления безопасностью информации (СУСИ)?
А) Для автоматизации всех бизнес-процессов.
Б) Для системного планирования, контроля и улучшения мер по обеспечению безопасности. +
В) Для ускорения обработки данных.
Г) Для минимизации затрат на IT-инфраструктуру.

8. Что из перечисленного считается одним из способов защиты целостности данных?
А) Шифрование данных при передаче и хранении.

Б) Использование систем цифровой подписи.+
В) Ограничение доступа по IP-адресам.
Г) Автоматическая обработка данных.

9. В какой степени важна роль резервного копирования в системе обеспечения информационной безопасности?
А) Только при физическом повреждении оборудования.
Б) Важна для восстановления данных после сбоев или атак.+
В) Не имеет большого значения.
Г) Только для хранения старых данных.

10. Что из следующего важно учитывать при построении защищенной ИС?
А) Только технические средства защиты.
Б) Обучение персонала, техсредства, процедуры и политика безопасности.+
В) Только программное обеспечение.
Г) Исключительно скоростные характеристики системы.

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 3. Определение уровня защищенности данных в информационной системе

1. Что такое уровень защищенности данных в информационной системе?
А) Степень, в которой данные доступны для пользователей.
Б) Степень, в которой данные защищены от несанкционированного доступа, повреждения или утраты. +
В) Количество данных, обрабатываемых системой.
Г) Время, за которое данные могут быть восстановлены.

2. Какой из показателей не относится к уровню защищенности данных?
А) Конфиденциальность.
Б) Поддержка мультианглоязычности. +
В) Целостность.
Г) Доступность.

3. Что из перечисленного является одним из способов оценки уровня защищенности данных?
А) Анализ бизнес-процессов.
Б) Проведение тестов на проникновение (penetration testing). +
В) Оценка скорости обработки данных.
Г) Проведение маркетингового исследования.

4. Какие меры обычно применяются для повышения уровня защищенности данных?

А) Использование шифрования, контроль доступа, аудит. +

Б) Увеличение объема хранения.

В) Публикация данных в открытом доступе.

Г) Ускорение обработки запросов.

5. Как связан уровень защищенности данных с возможностью их восстановления?

А) Чем выше уровень защищенности — тем быстрее данные можно восстановить.

Б) Высокий уровень защищенности обычно требует более сложных и длительных процедур восстановления. +

В) Нет никакой связи.

Г) Более высокий уровень защищенности всегда исключает необходимость восстановления.

6. Какими средствами можно повысить уровень защищенности данных?

А) Физическая установка видеонаблюдения.

Б) Использование шифрования, системы аутентификации, системы резервного копирования. +

В) Увеличение пропускной способности сети.

Г) Внедрение новейших устройств пользовательского интерфейса.

7. Какие показатели используются для количественной оценки уровня защищенности?

А) Процент успешных атак.

Б) Количество инцидентов безопасности, время реагирования, степень нарушения целостности. +

В) Общий объем данных.

Г) Количество пользователей системы.

8. Что из следующего помогает определить уровень защищенности данных?

А) Проведение аудита безопасности. +

Б) Обучение пользователей.

В) Разработка новых бизнес-процессов.

Г) Публикация отчетов в СМИ.

9. Какая роль у регулярных проверок и тестирования в оценке уровня защищенности данных?

А) Повышение уровня производительности.

Б) Обнаружение слабых мест и контроль эффективности средств защиты. +

В) Уменьшение затрат на инфраструктуру.

Г) Ускорение обработки данных.

10. Почему важно регулярно пересматривать уровень защищенности данных?

А) Чтобы снизить затраты на безопасность.

Б) Чтобы учесть новые угрозы, уязвимости и технологические изменения. +

В) Для повышения скорости передачи данных.

Г) Это не важно, уровень остается постоянным.

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 4 Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)

1. Какая из следующих категорий источников угроз наиболее часто связана с внутренними злоумышленниками?
А) Внешние злоумышленники (хакеры).
Б) Внутренние сотрудники или доверенные лица. +
В) Автоматизированные вирусы и черви.
Г) Поставщики оборудования.

2. Какой из перечисленных источников атак обычно обладает наибольшими возможностями для проведения сложных и целенаправленных атак?
А) Вирусы и трояны.
Б) Внутренние злоумышленники. +
В) Программные слепоты.
Г) Атаки через третьих лиц без их ведома.

3. Что из перечисленного является наиболее вероятным источником атак, использующим социальную инженерию?
А) Внешние хакеры.
Б) Внутренние злоумышленники.
В) Аутсайдеры, использующие психологические методы для получения доступа. +
Г) Автоматизированные скрипты.

4. Какие возможности могут иметь внешние злоумышленники при атаке на информационную систему?
А) Получение несанкционированного доступа, внедрение вредоносных программ, перехват трафика. +
Б) Только просмотр открытых данных.
В) Только физический урон оборудованию.
Г) Изменение настроек системы без доступа к сети.

5. Что такое модель нарушителя в контексте оценки потенциальных источников угроз?
А) Теоретическая модель, описывающая профиль и возможности потенциального злоумышленника. +
Б) Игра, симулирующая действия хакера.
В) Описание системы защиты от атак.
Г) Архитектура сети и её уязвимости.

6. Какие из перечисленных характеристик не являются частью модели нарушителя?
А) Мотивы выполнения атаки.
Б) Уровень технических знаний.
В) Финансовые затраты на покупку оборудования. +
Г) Время и ресурсы, необходимые для атаки.

7. Почему важно учитывать модели нарушителя при построении системы информационной безопасности?
А) Для снижения затрат на оборудование.
Б) Для определения и анализа потенциальных угроз и разработке эффективных мер защиты. +
В) Для повышения пропускной способности сети.
Г) Для проведения маркетинговых исследований.

8. Какие источники атак могут использовать автоматизированные скрипты или боты?
А) Внутренние злоумышленники.
Б) Внешние злоумышленники или ботнеты. +
В) Пользователи с постоянным доступом.
Г) Поставщики оборудования.

9. Что из перечисленного помогает определить возможности потенциальных злоумышленников?
А) Обучение сотрудников.
Б) Ведение учёта уязвимостей и проведение тестов на проникновение. +
В) Обеспечение резервного копирования.
Г) Установка антивирусных программ.

10. Какие меры могут снизить возможности внешних источников атак?
А) Ограничение физического доступа в офис.
Б) Использование брандмауэров, систем обнаружения вторжений, шифрование данных. +
В) Обучение работников.
Г) Улучшение дизайна интерфейса.

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

Тема 5. Описание угроз безопасности информации (модель угроз безопасности информации)

1. Что такое модель угроз безопасности информации?

А) Формальная структура, описывающая возможные угрозы и их источники для системы. +

Б) Совокупность архитектурных решений для защиты данных.

В) Процесс определения уровня защищенности системы.

Г) Набор правил и процедур по обеспечению безопасности.

2. Какая из следующих характеристик лучше всего описывает цель модели угроз?

А) Выявление уязвимостей системы.

Б) Определение потенциальных опасностей и возможностей злоумышленника. +

В) Установка программных средств защиты.
Г) Разработка бизнес-планов.

3. Какой элемент не входит в состав модели угроз?
А) Источник угрозы.
Б) Возможность реализации угрозы.
В) Используемое оборудование. +
Г) Последствия реализации угрозы.

4. Зачем необходимо создавать модель угроз при проектировании информационной системы?
А) Для определения слабых мест и разработки мер защиты. +
Б) Чтобы увеличить сбор данных пользователей.
В) Для ускорения обработки транзакций.
Г) Для уменьшения стоимости инфраструктуры.

5. Какое описание наиболее точно характеризует угрозу в контексте модели угроз?
А) Возможность или событие, которое может нанести вред системе или данным. +
Б) Конфиденциальная часть информации.
В) Программное обеспечение, предотвращающее атаки.
Г) Устройство, обеспечивающее безопасность.

6. Что из перечисленного не является примером угрозы безопасности информации?
А) Вирусная атака.
Б) Физический пожар.
В) Внутренний случайный сбой.
Г) Внедрение дополнительных уровней защиты. +

7. Чем отличается модель угроз от перечня уязвимостей?
А) Модель угроз описывает потенциальные атаки и их источники, уязвимости — слабые места в системе. +
Б) Модель угроз предполагает физическую защиту, уязвимости — программную.
В) Модель угроз — это документация, уязвимости — программный код.
Г) Нет никакой разницы.

8. Какая стадия предполагает анализ возможных сценариев реализации угроз?
А) Разработка архитектуры системы.
Б) Моделирование угроз. +
В) Внедрение программных средств защиты.
Г) Мониторинг систем безопасности.

9. Что из перечисленного является одним из способов обновления модели угроз?
А) Регулярное проведение анализа новых угроз и изменений в среде. +
Б) Увеличение пропускной способности сети.
В) Обучение пользователей.
Г) Внедрение новых интерфейсов.

10. Почему важно учитывать вероятностный аспект при моделировании угроз?
А) Для определения уровня риска и приоритетов по защите. +
Б) Для быстрого восстановления системы.
В) Для создания резервных копий.
Г) Для обеспечения конфиденциальности 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

Тема 6. Методы выбора системы защиты информации

1. Какой из методов является первым этапом при выборе системы защиты информации?

А) Анализ рисков и угроз. +
Б) Установка программного обеспечения.
В) Настройка сетевых устройств.
Г) Обучение персонала.

2. Какова основная цель метода оценки рисков при выборе системы защиты?

А) Определить стоимость системы.
Б) Выявить наиболее уязвимые точки и определить меры защиты. +
В) Выбрать наиболее коммерчески привлекательное решение.
Г) Уменьшить расходы на защиту.

3. Какой из следующих методов относится к количественным методам выбора системы защиты?

А) Анализ стоимости и эффективности мер защиты. +
Б) Определение угроз через сценарии.
В) Проведение тестирования системы.
Г) Оценка пользовательского опыта.

4. В каком случае применяется метод сравнения различных вариантов защиты?

А) Когда нужно подобрать наиболее подходящую систему защиты из нескольких вариантов. +
Б) При разработке программного обеспечения.
В) Во время внедрения аппаратных средств.
Г) Для обучения сотрудников.

5. Что из перечисленного не относится к методам выбора системы защиты?

А) Метод экспертных оценок.
Б) Метод анализа стоимости.
В) Метод автоматической установки системы. +
Г) Метод сравнения технических характеристик.

6. В чем заключается преимущество метода анализа затрат и эффективности?

А) Он позволяет выбрать наиболее дешевое решение.
Б) Он обеспечивает баланс между затратами и уровнем защиты. +
В) Он ускоряет внедрение системы.
Г) Он исключает необходимость профессиональных оценок.

7. Какой метод предполагает использование экспертных мнений для оценки вариантов защиты?

А) Эвристический метод. +

Б) Метод аналитического иерархического процесса (ABC).

В) Метод автоматизированного тестирования.

Г) Метод Cost-Benefit анализа.

8. Почему важно учитывать интеграцию выбранной системы защиты с существующей инфраструктурой?

А) Чтобы обеспечить совместную работу и минимизировать возможные конфликты. +

Б) Чтобы снизить стоимость внедрения.

В) Для ускорения процесса покупки.

Г) Для увеличения сложности системы.

9. Какой из методов используется для оценки предпочтений при выборе системы защиты?

А) Метод парных сравнений и матриц приоритетов. +

Б) Метод случайного выбора.

В) Метод автоматической генерации решений.

Г) Метод анализа логов.

10. Какой из методов помогает выявить потенциальные недостатки выбранной системы защиты еще до её внедрения?

А) Моделирование угроз и тестирование системы. +

Б) Обучение персонала.

В) Физическая охрана.

Г) Установка антивирусных программ.

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. Что такое защищённая информационная система?

А) Информационная система, имеющая механизмы защиты данных и ресурсов. +

Б) Любая система, использующая шифрование.

В) Система, исключающая все виды угроз.

Г) Информационная система без доступа из Интернета.

2. Какие из перечисленных элементов являются основными компонентами защищённой ИС?
А) Защитные механизмы, средства контроля, процедуры управления безопасностью +
Б) Офисная техника и программное обеспечение.
В) Клиентские устройства и сети.
Г) Социальная инфраструктура.

3. Что такое аутентификация в контексте защищённой ИС?
А) Процесс проверки идентичности пользователя или устройства. +
Б) Процесс шифрования данных.
В) Передача данных через зашифрованное соединение.
Г) Создание резервных копий.

4. Какой механизм обеспечивает контроль доступа к ресурсам информационной системы?
А) Аутентификация +
Б) Шифрование данных
В) Мониторинг сети
Г) Антивирусное программное обеспечение

5. Что из перечисленного не входит в методы защиты информации?
А) Шифрование данных
Б) Физическая охрана серверов
В) Обучение персонала
Г) Отказоустойчивая архитектура +

6. Что такое резервное копирование данных?
А) Создание копий информации для восстановления при потере. +
Б) Шифрование всех данных.
В) Передача данных в облако.
Г) Установка антивирусных программ.

7. Какие меры обеспечивают физическую защиту информационных систем?
А) Ограждения, системы видеонаблюдения, контроль доступа +
В) Шифрование данных
В) Создание паролей
Г) Обучение персонала

8. Какие угрозы могут быть минимизированы с помощью защиты информации?
А) Неавторизованный доступ, утечка данных, повреждение данных +
Б) Только природные катастрофы
В) Только внутренние ошибки сотрудников
Г) Только программные сбои

9. Что такое криптографическая защита информации?
А) Методы преобразования данных в закрытый формат для обеспечения конфиденциальности +
Б) Установка физических барьеров
В) Обучение персонала
Г) Ограничение доступа к машине

10. Как называется система, которая обеспечивает обнаружение и предотвращение инцидентов безопасности?

А) Система обнаружения и предотвращения вторжений (IDS/IPS) +
Б) Система индексирования данных
В) Корпоративный чат
Г) Контрольная точка доступа

11. Что такое политик безопасности информационной системы?
А) Документ, определяющий правила и процедуры защиты информации +
Б) Устав компании
В) Документ о лицензировании ПО
Г) Инструкция по эксплуатации оборудования

12. Что из перечисленного является примером защиты на уровне сети?
А) Брандмауэр +
Б) Шифрование файлов
В) Ограничение доступа к файлам
Г) Обучение сотрудников

13. Какой аспект важен при создании защищённой системы с точки зрения архитектуры?
А) Модульность и сегментация сети +
Б) Максимальная интеграция всех элементов в один узел
В) Минимизация компонентов системы
Г) Использование только открытых протоколов

14. Что такое многоуровневая защита (многоуровневая модель безопасности)?
А) Защита данных на разных уровнях системы (физическом, сетевом, приложенческом) +
В) Использование нескольких паролей подряд
В) Модуль защиты только базы данных
Г) Аутентификация по отпечаткам пальцев

15. Какие функции выполняет централизованный менеджмент безопасности?
А) Координацию мер защиты, мониторинг инцидентов, управление доступом +
Б) Создание бэкап-копий данных
В) Обеспечение электропитания серверов
Г) Распределение аппаратных ресурсов

16. Как называется механизм, автоматически блокирующий подозрительную активность?
А) Система автоматического реагирования (ART) +
В) Резервное копирование
В) Мониторинг трафика
Г) Аутентификация пользователя

17. Что такое аудит безопасности информационной системы?
А) Процесс проверки соответствия системы установленным политикам и стандартам +
Б) Процесс установки новых средств защиты
В) Руководство по эксплуатации оборудования
Г) Доклад о провале системы

18. Зачем необходима регулярная проверка системы защиты?
А) Для обнаружения уязвимостей и обеспечения актуальности мер безопасности +
В) Для обновления оргтехники
В) Для расширения оборудования
Г) Для увеличения пропускной способности сети

19. Какие меры следует принимать для защиты данных в облачных системах?
А) Шифрование, контроль доступа, аудит действий +
В) Обеспечить только физическую безопасность оборудования +
В) Полностью доверять облачному провайдеру
Г) Не использовать резервные копии

20. Что означает термин «разделение доверия» в системе безопасности?
А) Создание различных уровней доступа и контроля между компонентами системы +
Б) Использование одного пароля на всех уровнях
В) Обеспечение общего доступа для всех пользователей
Г) Удаление старых учетных записей

21. Что такое «защищённая зона» в контексте информационной системы?
А) Изолированное от внешних угроз пространство для хранения особо важных данных +
В) Общий офисный кабинет
В) Внутренняя сеть без контроля доступа
Г) Область, открытая для всех сотрудников

22. Почему важно обучать сотрудников правилам информационной безопасности?
А) Потому что большинство угроз связаны с человеческим фактором +
В) Для сокращения затрат на техническую безопасность
В) Для улучшения коммуникации внутри компании
Г) Для повышения их квалификации

23. Какие основные показатели эффективности защищённой системы?
А) Надёжность, своевременность обнаружения и устранения угроз, доступность +
В) Количество оборудования и программного обеспечения
В) Время, затраченное на внедрение защиты
Г) Количество сотрудников в отделе безопасности

24. Установите соответствие:
1) Процесс проверки личности пользователя или устройства в системе.
2) Документ, содержащий регламенты и правила защиты информации.
3) Уровень или модель защиты, реализуемая в информационной системе.
А) Политика безопасности
В) Аутентификация
С) Модель многоуровневой защиты

Ответ:
1 — В) Аутентификация
2 — А) Политика безопасности
3 — С) Модель многоуровневой защиты

25. Вставь пропущенное слово:
_____ — это процесс подтверждения личности пользователя перед предоставлением доступа к системе или информации.
Ответ: Аутентификация

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 №____