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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

РАЗРАБОТКА И РЕАЛИЗАЦИЯ ПРОЕКТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Оценочные материалы по дисциплине разработка и реализация проектов в сфере информационной безопасности

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 разработка и реализация проектов в сфере информационной безопасности 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 разработка и реализация проектов в сфере информационной безопасности.

1. Паспорт оценочных материалов по дисциплине «Базы данных»

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-3.2 Способен использовать современные технологии программирования для разработки защищенного программного обеспечения	ОПК-3.2.1 Демонстрирует умение анализа средств защиты информации и выполнения анализа защищенности сетевых сервисов с использованием средств мониторинга и автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Знает: основные средства защиты информации, принципы их работы и применения, а также методы анализа защищенности сетевых сервисов. Уметь: проводить анализ событий информационной безопасности с использованием средств мониторинга, выявлять попытки несанкционированного доступа и реагировать на них с помощью автоматизированных систем. Владеет: навыками настройки и управления средствами защиты информации для обеспечения устойчивости компьютерных систем и сетей.	Тема 1. Основы управления проектами в сфере информационной безопасности	Реферат (Тема 1) Тест (тема 1)	Тест (В 1-15 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
	ОПК-3.2.2 Демонстрирует умение организовывать аудит безопасности и участвовать в проверках защищенности компьютерных сетей и информационных систем	Знает: методы и инструменты проведения аудита информационной безопасности, а также основные подходы к проверке защищенности компьютерных сетей и информационных систем. Умеет: организовывать и проводить аудит безопасности, выявлять уязвимости и оценивать их влияние на информационные системы. Владеет: навыками участия в проверка защищенности, документирования результатов аудита и разработки рекомендаций по улучшению уровня безопасности.	Тема 2. Разработка проектной документации для систем защиты информации Структура проектной документации. Требования стандартов (ГОСТ, ISO). Анализ рисков и угроз в проектах. Тема 3. Реализация и оценка проектов в сфере нформационной безопасности Этапы внедрения проектов. Методы оценки эффективности. Инструменты мониторинга и контроля реализации	Реферат (Тема 2-3) Тест (Тема 2-3) Практическое задание (Тема 1-3)	Тест (В 16-25 тестового задания)

2. Оценочные материалы по дисциплине «Базы данных»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема1. Основы управления проектами в сфере информационной безопасности

1. Этапы жизненного цикла проекта в области информационной безопасности
2. Методы оценки рисков в проектах информационной безопасности.
3. Стратегии реагирования на инциденты информационной безопасности
4. Управление персоналом в проектах информационной защиты
5. Оценка эффективности мероприятий по защите информации
6. Метрики и инструменты анализа результатов проектов ИБ.
7. Стандартизация и сертификация ИБ-проекта.
8. Выбор технологий и решений для комплексного подхода к обеспечению безопасности.
9. Законодательные требования и международные стандарты (ISO, ГОСТ).
10. Управление конфигурациями и процессами изменений.
11. Особенности гибких подходов к управлению проектами ИБ.
12. Мониторинг и аудит информационной безопасности организаций
13. Формирование бюджета и оценка затрат в проекте информационной безопасности
14. Обеспечение непрерывности бизнеса в условиях киберинцидентов
15. Разработка планов восстановления работоспособности критически важных сервисов.
16. Современные угрозы информационной безопасности и способы их предотвращения
17. Проблемы внедрения и эксплуатации систем управления информационной безопасностью (СУИБ)

Тема 2. Разработка проектной документации для систем защиты информации.

1. Структура и содержание технического задания на создание системы защиты информации.
2. Этапы разработки концепции системы защиты информации и её документальное оформление.
3. Составление паспорта информационной системы и специфика отражения требований по защите информации.
4. Методология проектирования защищённых сетей передачи данных и оформления проектных документов.
5. Документация по построению центров обработки данных с учётом мер информационной безопасности.
6. Регламентация процедур администрирования и сопровождения системы защиты информации.
7. Проектирование механизмов резервного копирования и аварийного восстановления данных.
8. Документирование процедуры аттестации объектов информатизации по требованиям информационной безопасности.
9. Порядок подготовки инструкций пользователей по соблюдению требований информационной безопасности.

10. Организация работ по тестированию и оценке соответствия разрабатываемой системы защиты информации установленным стандартам.

11. Формирование перечня нормативных актов и стандартов, используемых при создании технической документации по защите информации.

12. Правила формирования эксплуатационной документации на систему защиты информации.

13. Оценка рисков утечки конфиденциальной информации и отражение соответствующих мер в проектной документации.

14. Оформление акта ввода в эксплуатацию системы защиты информации.

15. Принципы описания организационно-технических мероприятий по защите персональных данных в рамках корпоративной информационной системы.

Тема 3. Реализация и оценка проектов в сфере информационной безопасности

1. Процесс планирования и реализации проектов информационной безопасности
2. Практические методы оценки зрелости информационной безопасности организации
3. Подходы к измерению эффективности реализованных проектов информационной безопасности .
4. Критерии выбора технических решений для проектов информационной безопасности
5. Анализ рисков и угроз в процессе реализации проектов информационной безопасности
6. Особенности внедрения систем обнаружения вторжений (IDS)
7. Реализация криптографических методов защиты информации в корпоративных сетях
8. Создание комплексной системы мониторинга и реагирования на инциденты информационной безопасности (SIEM)
9. Аудит состояния информационной безопасности перед реализацией крупных проектов .
10. Принципы и технологии организации виртуальных частных сетей (VPN)
11. Подготовка персонала и повышение осведомленности сотрудников в рамках проектов информационной безопасности
12. Оптимизация затрат на реализацию проектов информационной безопасности
13. Оценка соответствия требованиям регуляторов (например, PCI DSS, GDPR, ФЗ-152)
14. Разработка плана по восстановлению данных и отказоустойчивости систем в проектах ИБ .
15. Перспективы развития проектов информационной безопасности в цифровой экономике

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. Основы управления проектами в сфере информационной Безопасности

Основные элементы системы управления информационной безопасностью (СУИБ). Циклы и процессы управления проектами. Планирование, контроль и управление рисками. Этапы жизненного цикла проекта в области информационной безопасности. Методологии управления проектами (PMBOK, PRINCE2, Agile).Подходы к управлению рисками в проектах информационной безопасности. Мониторинг и оценка эффективности реализации проектов.

Вопросы для самоконтроля:

1.Что включает в себя система управления информационной безопасностью?

2.Какова структура этапов жизненного цикла проекта информационной безопасности?

3.Чем отличаются методологии PMBOK, PRINCE2 и Agile в управлении проектами?

4.Какие подходы используются для оценки рисков в проекте информационной безопасности?

5.Как осуществляется мониторинг и оценка эффективности проектов информационной безопасности?

Цель работы – формирование практических навыков по проведению многомерного проектирования баз данных.

В работе используется презентация слайдов выполненная в MS Powerpoint

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. Разработка проектной документации для систем защиты информации.

Документированный проект системы защиты информации, включая описания всех элементов и деталей реализации. Инструкция по эксплуатации и обслуживанию предлагаемой системы. Экономическое обоснование целесообразности принятия разработанных предложений.

Вопросы для самоконтроля:

1.Какие нормативные документы определяют обязательные требования к разработке систем защиты информации?

2.По каким критериям выбираются технические средства защиты информации?

3.Какие принципы обеспечивают эффективность проектирования систем защиты информации?

4.Как рассчитывается бюджет проекта по созданию системы защиты информации?

Цель работы- приобретение навыков разработки технической и организационной документации для создания эффективных систем защиты информации (СЗИ) предприятий.

В работе используется презентация слайдов выполненная в MS Powerpoint

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. Реализацияи оценка проектов в сфере информационной безопасности

Методы обработки и анализа больших объемов данных применительно к задаче обеспечения информационной безопасности. Модели и схемы организации хранения и анализа защищаемых данных. Обучение моделей машинного обучения для выявления аномалий и предотвращения кибератак. Принципы построения и эксплуатации хранилищ данных для нужд анализа и расследования инцидентов информационной безопасности. Оценка качества методов анализа данных и выявление ошибок переобучения моделей.

Вопросы для самоконтроля:

1.Какие существуют формы представления данных в задачах информационной безопасности?

2.Опишите различия между аналитическим и информационным подходами к моделированию данных.

3.Назовите основные типы алгоритмов анализа данных, используемых в сфере информационной безопасности.

4.Приведите пример ситуации эффекта переобучения модели.

5.Перечислите требования к алгоритмам анализа данных в условиях ограничения ресурсов.

Цель работы− формирование практических навыков по проведению многомерного проектирования баз данных.

В работе используется презентация слайдов выполненная в MS Powerpoint

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. Основы управления проектами в сфере информационной безопасности

1.Какое из следующих утверждений лучше всего описывает управление проектом?

А) Это процесс, который включает только планирование.

Б) Это набор методов, используемых для завершения проекта с максимальной эффективностью.+

В) Это исключительно финансовый контроль за проектом.

Г) Это единовременное мероприятие без необходимости анализа результатов.

2.Какой из этапов жизненного цикла проекта включает в себя определение целей и задач проекта?

А) Исполнение

Б) Инициация +

В) Завершение

Г) Планирование

3.Что такое "область применения проекта" (scope)?

А) Количество ресурсов, необходимых для выполнения проекта.

Б) Общая сумма бюджета, выделенного на проект.

В) Определение всех работ, которые должны быть выполнены для достижения целей проекта. +

Г) Список всех участников проекта.

4.Какой из следующих факторов не является ограничением проекта?

А) Время

Б) Бюджет

В) Качество

Г) Уровень удовлетворенности клиентов+

5.Какой метод используется для оценки рисков в проекте?

А) SWOT-анализ+

Б) PERT-анализ

В) Gantt-диаграмма

Г) Критический путь

6.Что такое "управление заинтересованными сторонами" (stakeholders management)?

А) Процесс контроля за расходами проекта.

Б) Процесс выявления, анализа и управления потребностями и ожиданиями заинтересованных сторон .+

В) Процесс создания отчетов о ходе выполнения проекта.
Г) Процесс оценки качества конечного продукта.

7.Какой из следующих документов является основным для управления проектом?
А) Бюджет проекта
Б) План управления проектом +
В) Отчет о рисках
Г) График выполнения работ

8.Что такое "критический путь" в управлении проектами?
А) Это последовательность задач, которые могут быть выполнены параллельно.
Б) Это самая длинная последовательность задач, определяющая минимальное время завершения проекта. +
В) Это набор задач, которые не требуют ресурсов.
Г) Это список всех задач, выполняемых в проекте.

9.Какой из следующих методов управления проектами основан на гибком подходе и итеративном развитии?
А) Водопадная модель
Б) Agile +
В) PRINCE2
Г) Критический путь

10.Какой из следующих аспектов является важным при оценке качества проекта?
А) Соответствие срокам выполнения +
Б) Общее количество участников проекта
В) Количество проведенных совещаний
Г) Периодичность отчетности

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. Разработка проектной документации для систем защиты информации

1.Какой документ определяет общие требования к системе защиты информации?
А) Техническое задание +
Б) План проекта
В) Отчет о тестировании
Г) Договор на выполнение работ

2.Что включает в себя анализ рисков при разработке проектной документации?

А) Определение бюджета проекта

Б) Выявление уязвимостей и угроз безопасности +

В) Составление графика выполнения работ

Г) Оценка производительности системы

3.Какой из следующих документов описывает архитектуру системы защиты информации?

А) Проектная документация +

Б) Инструкции по эксплуатации

В) Техническое задание

Г) Отчет о проведенных испытаниях

4.Какой из перечисленных элементов не является частью проектной документации для систем защиты информации?

А) Описание функциональных требований

Б) План управления конфигурацией

В) Отчет о финансовых расходах

Г) Описание архитектуры системы +

5.Какой документ служит основой для разработки политики безопасности информации?

А) Анализ рисков +

Б) Техническое задание

В) Проектная документация

Г) Отчет о тестировании

6.Что такое "техническое задание" в контексте разработки систем защиты информации?

А) Документ, описывающий только бюджет проекта

Б) Документ, определяющий цели, задачи и требования к системе +

В) Документ, содержащий только инструкции по эксплуатации

Г) Документ, фиксирующий результаты тестирования системы

7.Какой из следующих документов описывает процедуры реагирования на инциденты безопасности?

А) План управления проектом

Б) Политика безопасности +

В) Проектная документация

Г) Отчет о тестировании

8.Что является целью создания проектной документации для систем защиты информации?

А) Упрощение процесса разработки программного обеспечения

Б) Обеспечение соответствия требованиям законодательства и стандартам +

В) Снижение затрат на проект

Г) Увеличение числа участников проекта

9.Какой из следующих аспектов должен быть учтен при разработке проектной документации?

А) Удобство использования интерфейса пользователя
Б) Уровень квалификации команды разработчиков
В) Методология разработки программного обеспечения
Г) Все вышеперечисленное +

10.Какой из следующих документов может содержать информацию о тестировании системы защиты информации?
А) Проектная документация
Б) Политика безопасности
В) Техническое задание
Г) Отчет о тестировании +

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. Реализацияи оценка проектов в сфере информационной безопасности

1.Какой из следующих этапов является первым в реализации проекта по информационной безопасности?
А) Оценка рисков
Б) Разработка плана проекта
В) Определение требований +
Г) Проведение тестирования

2.Какой метод оценки рисков наиболее часто используется в проектах по информационной безопасности?
А) SWOT-анализ
Б) Метод анализа уязвимостей +
В) Метод Монте-Карло
Г) Метод FMEA (анализ видов и последствий отказов)

3.Что подразумевается под термином "проектная документация" в контексте информационной безопасности?
А) Набор документов, описывающих только технические требования
Б) Комплекс документов, охватывающих все аспекты проекта +
В) Только финансовые отчеты о проекте
Г) Документы, касающиеся только тестирования системы

4. Какой из следующих показателей не является критерием успеха проекта в сфере информационной безопасности?

А) Соответствие требованиям законодательства
Б) Уровень удовлетворенности пользователей
В) Количество обнаруженных уязвимостей +
Г) Сроки выполнения проекта

:

5.Какой из следующих методов управления проектами наиболее подходит для проектов в сфере информационной безопасности?
А) Метод водопада
Б) Agile +
В) Прямое управление
Г) Классическая модель

6.Что такое "пороговая оценка" в контексте оценки проектов по информационной безопасности?
А) Минимальное количество ресурсов, необходимых для начала проекта
Б) Уровень риска, при котором проект считается приемлемым +
В) Максимальный бюджет, выделенный на проект
Г) Минимальное количество участников, необходимых для реализации проекта

7.Какой из перечисленных факторов не влияет на стоимость реализации проекта в сфере информационной безопасности?
А) Уровень квалификации команды
Б) Сложность системы защиты информации
В) Количество пользователей системы
Г) Состояние офисного оборудования +

8.Какой из следующих методов позволяет проводить оценку эффективности мер по защите информации?
А) Анализ затрат и выгод
Б) SWOT-анализ
В) Опрос пользователей
Г) Все вышеперечисленное +

:

9.Какой документ фиксирует результаты оценки рисков и предлагает меры по их снижению?
А) Техническое задание
Б) План управления рисками +
В) Проектная документация
Г) Отчет о тестировании

10.Что такое "индикаторы эффективности" в контексте проектов по информационной безопасности?
А) Показатели, используемые для оценки успешности проекта +
Б) Методы тестирования систем защиты
В) Набор правил для разработки программного обеспечения
Г) Документы, описывающие архитектуру 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

2.2 Оценочные материалы для проведения промежуточной аттестации

1.Какой из следующих этапов управления проектом является первым?
А) Планирование
Б) Инициация +
В) Реализация
Г) Завершение

2.Что такое "проектная документация" в контексте систем защиты информации?
А) Набор документов, описывающих только технические аспекты системы
Б) Комплекс документов, охватывающих все стадии проекта +
В) Документы, касающиеся только финансовых аспектов проекта
Г) Отчеты о тестировании системы

3.Какой из следующих элементов не является частью плана управления проектом?
А) Описание проекта
Б) Оценка рисков
В) План коммуникаций
Г) Пошаговая инструкция по эксплуатации системы +

4.Какой метод оценки рисков наиболее распространен в сфере информационной безопасности?
А) SWOT-анализ
Б) Метод анализа уязвимостей +
В) Метод FMEA (анализ видов и последствий отказов)
Г) Метод Монте-Карло

5.Что такое "жизненный цикл проекта"?
А) Период времени, в течение которого проект должен быть завершен
Б) Последовательность этапов, через которые проходит проект от начала до завершения +
В) Список всех ресурсов, необходимых для выполнения проекта
Г) Процесс оценки эффективности проекта после его завершения

6.Какой документ фиксирует все требования к системе защиты информации?
А) Техническое задание +
Б) План управления проектом
В) Отчет о рисках
Г) Порядок тестирования

7.Какой из следующих показателей не используется для оценки успешности проекта в сфере информационной безопасности?

А) Соответствие требованиям законодательства
Б) Уровень удовлетворенности пользователей
В) Количество инцидентов безопасности после внедрения системы
Г) Общее количество сотрудников компании+

8.Какой из следующих методов управления проектами наиболее подходит для проектов в сфере информационной безопасности?
А) Метод водопада
Б) Agile +
В) Классическая модель
Г) Прямое управление

9.Что такое "план управления рисками"?
А) Документ, описывающий все возможные риски проекта и меры по их минимизации +
Б) Список всех участников проекта и их ролей
В) График выполнения всех задач проекта
Г) Отчет о тестировании системы защиты информации

10.Какой из следующих факторов не влияет на успех реализации проекта в сфере информационной безопасности?
А) Уровень квалификации команды
Б) Наличие четкой стратегии управления проектом
В) Общее состояние экономики страны +
Г) Сложность системы защиты информации

11.Что такое "система управления проектами"?
А) Набор методов и инструментов для планирования и контроля проектов +
Б) Программное обеспечение для автоматизации документооборота
В) Группа людей, отвечающих за выполнение проекта
Г) Документ, описывающий цели проекта

12.Какой из следующих документов описывает процессы тестирования системы защиты информации?
А) Техническое задание
Б) План тестирования +
В) Отчет о рисках
Г) Порядок эксплуатации

13.Что такое "индикаторы успеха" в управлении проектами?
А) Параметры, которые измеряют эффективность работы команды
Б) Показатели, определяющие качество конечного продукта
В) Критерии, по которым оценивается успешность выполнения проекта
Г) Все вышеперечисленное +

14.Какой из следующих подходов не является частью методологии Agile?
А) Итеративная разработка
Б) Гибкость в изменениях требований
В) Строгая документация на всех этапах +
Г) Регулярные встречи команды

15.Что такое "анализ заинтересованных сторон" в управлении проектом?

А) Оценка влияния внешних факторов на проект
Б) Определение всех участников проекта и их интересов +
В) Изучение конкурентов на рынке
Г) Оценка финансовых затрат на проект

16.Какой из следующих документов определяет бюджет проекта?
А) Техническое задание
Б) Бюджетный план +
В) План управления рисками
Г) Отчет о выполнении работ

17.Что такое "мониторинг и контроль" в управлении проектом?
А) Процесс анализа результатов после завершения проекта
Б) Наблюдение за выполнением задач и корректировка действий по мере необходимости +
В) Составление отчетов о работе команды
Г) Оценка стоимости проекта

18.Какой из следующих методов может быть использован для оценки уязвимостей системы?
А) SWOT-анализ
Б) Пентестинг (тестирование на проникновение) +
В) Метод мозгового штурма
Г) Анализ причинно-следственных связей

19.Что такое "проектное управление"?
А) Управление процессами разработки программного обеспечения
Б) Управление всеми аспектами работы над проектом от начала до завершения +
В) Управление финансами компании
Г) Управление командой сотрудников

20.Какой из следующих показателей используется для оценки качества системы защиты информации?
А) Количество инцидентов безопасности за месяц +
Б) Количество сотрудников в команде безопасности
В) Общая стоимость системы защиты информации
Г) Уровень удовлетворенности клиентов

21.Что такое "план коммуникаций" в управлении проектом?
А) Документ, описывающий, как будет происходить обмен информацией между участниками проекта +
Б) График встреч команды проекта
В) Отчет о выполнении задач проекта
Г) Список всех заинтересованных сторон

22.Какой из следующих этапов включает в себя завершение всех работ по проекту?
А) Инициация
Б) Планирование
В) Реализация
Г) Завершение +

23.Что такое "обратная связь" в контексте управления проектами?

А) Процесс получения информации о выполнении задач от команды или заинтересованных сторон +

Б) Оценка качества конечного продукта после его завершения

В) Процесс исправления ошибок в документации проекта

Г) Наблюдение за работой конкурентов

24. Установите правильное соответствие между элементами

1. Процесс идентификации и анализа рисков	А) Risk Management Plan
2. Методология гибкого управления проектами	Б) Agile Methodology
3.Система показателей оценки эффективности проекта	В) Key PerformanceIndicators
4.Модель зрелости процессов управления проектам	Г) Project Management Maturity Model (PMMM)

Правильные ответы:1-:А,2-Б,3-В,4-Г

25. В процессе управления проектом в сфере информационной безопасности важным этапом является _____, который включает в себя идентификацию, анализ и оценку рисков, связанных с проектом.

Правильный ответ: Оценка рисков

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 №____