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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

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 Основы управления информационной безопасностью

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 Основы управления информационной безопасностью 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 Основы управления информационной безопасностью

1. Паспорт оценочных материалов по дисциплине «Основы управления информационной безопасностью»

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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК¬1.2. Демонстрирует умение оценивать роль информационной безопасности при решении задачи профессиональной деятельности	Знать: основы информационной безопасности и её составляющие; методы и средства обеспечения информационной безопасности; нормативно-правовую базу в сфере информационной безопасности; потенциальные угрозы и риски, связанные с нарушением режима информационной безопасности. Уметь: анализировать потенциальные угрозы информационной безопасности в своей профессиональной деятельности; разрабатывать меры и мероприятия по обеспечению информационной безопасности; применять специализированные инструменты и системы защиты информации. Владеть: практическими навыками реализации мероприятий по защите информации.	Тема 1. Основы управления информационной безопасностью. Тема 2. Стандартизация систем и процессов управления информационной безопасностью Тема 3. Политика информационной безопасности	Реферат (тема 1-3), Тест (тема 1-3)	Тест (В1-15)
ОПК¬5. Способен применять нормативные	ОПК¬5.2. Демонстрирует умение решать	Знать: процедура прохождения нормоконтроля; стандартные формы отчетности и документирования; порядок	Тема 4. Системы управления информационной	Реферат (тема 4-6), Тест (тема 4-6)	Тест (В16-25)

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
правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	стандартные профессиональные задачи с целью выполнения требований нормоконтролеров РФ	действий при проведении проверок контролирующими органами. Уметь: готовить документацию и материалы к проверке нормами контроля; решать проблемы и исправлять недостатки, выявленные проверяющими инстанциями; эффективно взаимодействовать с представителями органов нормоконтроля. Владеть: навыками подготовки и оформления отчетной документации; технологией взаимодействия с представителями государственных структур; способностью оперативно реагировать на запросы и предписания нормоконтролирующих организаций.	безопасностью (СУИБ Тема 5. Оценка рисков информационной безопасности Тема 6. Процессы управления информационной безопасностью		

2. Оценочные материалы по дисциплине «Основы управления информационной безопасностью»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема 1. Основы управления информационной безопасностью.1. История интерпретируемых языков программирования.

1. Понятие и принципы информационной безопасности
2. Угрозы информационной безопасности в современном обществе
3. Методы и средства защиты информации
4. Роль управления рисками в информационной безопасности
5. Стандарты и нормативные документы в области информационной безопасности
6. Создание и внедрение политики безопасности информации
7. Аудит информационной безопасности: подходы и методы
8. Социальная инженерия как угроза информационной безопасности
9. Информационная безопасность в облачных вычислениях
10. Безопасность мобильных устройств: вызовы и решения
11. Криптография и её роль в обеспечении информационной безопасности .
12. Инциденты информационной безопасности: реагирование и управление
13. Обучение и повышение осведомленности сотрудников в области информационной безопасности
14. Системы управления информационной безопасностью (СУИБ)
15. Будущее информационной безопасности: тенденции и новшества

Тема 2. Стандартизация систем и процессов управления информационной безопасностью

1. Основы стандартизации в управлении информационной безопасностью
2. ISO/IEC 27001: Система управления информационной безопасностью
3. Сравнительный анализ стандартов ISO/IEC 27001 и NIST SP 800-53
4. Роль стандартизации в обеспечении безопасности данных
5. Стандарты в области управления рисками информационной безопасности
6. Стандарты и методологии в области защиты персональных данных (GDPR)
7. Разработка и внедрение внутренних стандартов безопасности в организации
8. Аудит соответствия стандартам безопасности информации
9. Стандарты и лучшие практики в области безопасности облачных вычислений
10. Совместимость стандартов информационной безопасности с другими стандартами управления
11. Влияние международных стандартов на национальное законодательство в области информационной безопасности
12. Критерии выбора стандартов для организации
13. Интеграция стандартов информационной безопасности в бизнес-процессы
14. Инновации в стандартизации процессов управления информационной безопасностью
15. Будущее стандартизации в области информационной безопасности

Тема 3. Политика информационной безопасности

1. Определение и основные элементы политики информационной безопасности
2. Процесс разработки политики информационной безопасности

3. Роль высшего руководства в формировании политики информационной безопасности

4. Виды политик информационной безопасности: от общей до специализированной

5. Интеграция политики информационной безопасности с другими корпоративными политиками

6. Анализ и оценка существующих политик информационной безопасности

7. Обучение сотрудников в рамках политики информационной безопасности

8. Политика безопасности информации в контексте соблюдения законодательства

9. Мониторинг и обновление политики информационной безопасности

10. Политика реагирования на инциденты информационной безопасности

11. Риски и вызовы при внедрении политики информационной безопасности

12. Кейс-стадии: успешные примеры реализации политики информационной безопасности

13. Этика и политика информационной безопасности

14. Роль технологий в реализации политики информационной безопасности

15. Будущее политик информационной безопасности: тренды и прогнозы

Тема 4. Системы управления информационной безопасностью (СУИБ

1. Понятие и основные компоненты Системы управления информационной безопасностью (СУИБ)

2. Стандарты ISO/IEC 27001: внедрение СУИБ

3. Методологии разработки СУИБ: подходы и лучшие практики

4. Оценка рисков как основа для разработки СУИБ

5. Интеграция СУИБ с другими системами управления

6. Роль технологии в СУИБ

7. Поддержка и улучшение СУИБ: мониторинг и аудит

8. Обучение и повышение осведомленности персонала как элемент СУИБ

9. Управление инцидентами в рамках СУИБ

10. Критерии успешной реализации СУИБ в организации

11. Кейс-стадии успешных СУИБ в различных отраслях

12. Применение искусственного интеллекта и машинного обучения в СУИБ

13. Будущее СУИБ: тренды и вызовы

14. Анализ недостатков и уязвимостей существующих СУИБ

15. СУИБ в условиях удаленной работы и гибридных моделей

Тема 5. Оценка рисков информационной безопасности

1. Понятие и значение оценки рисков информационной безопасности

2. Методологии оценки рисков: от качественных до количественных подходов

3. Процесс оценки рисков: этапы и процедуры

4. Идентификация угроз и уязвимостей в рамках оценки рисков

5. Классификация рисков информационной безопасности

6. Методы анализа рисков: качественные и количественные подходы

7. Использование инструментов и программного обеспечения для оценки рисков

8. Риск-ориентированный подход к управлению информационной безопасностью

9. Оценка рисков в контексте соблюдения нормативных требований

10. Кейс-стадии: успешные примеры оценки рисков в организациях

11. Роль высшего руководства в процессе оценки рисков

12. Мониторинг и пересмотр рисков: динамика и актуализация информации

13. Психология принятия решений в условиях неопределенности рисков

14. Будущее оценки рисков информационной безопасности: тренды и достижения

15. Взаимосвязь между оценкой рисков и реакцией на инциденты

Тема 6. Процессы управления информационной безопасностью

1. Общее понятие управления информационной безопасностью
2. Цикл управления информационной безопасностью: PDCA
3. Идентификация и оценка рисков как основа управления информационной безопасностью
4. Разработка и внедрение политики информационной безопасности
5. Управление инцидентами информационной безопасности
6. Обучение и повышение осведомленности сотрудников
7. Мониторинг и аудит процессов управления информационной безопасностью
8. Управление доступом и аутентификация
9. Управление безопасностью сетевой инфраструктуры
10. Управление безопасностью физической инфраструктуры
11. Управление безопасностью данных
12. Соответствие нормативным требованиям и стандартам
13. Использование технологий для управления информационной безопасностью
14. Анализ инцидентов и обратная связь
15. Будущее управления информационной безопасностью: тенденции и вызовы

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

Тест№1

Тема 1. Основы управления информационной безопасностью.

1. Что такое информационная безопасность?

А) Защита информации от несанкционированного доступа

Б) Обеспечение доступности информации для всех пользователей

В). Защита информации от потери, искажения и несанкционированного доступа +

Г). Увеличение объема информации в организации

2. Какой из следующих аспектов не является частью информационной безопасности?

А). Конфиденциальность

Б). Доступность

В). Целостность

Г). Увеличение прибыли +

3. Какой стандарт описывает требования к системам управления информационной безопасностью?

А). ISO 9001

Б). ISO 14001

В). ISO/IEC 27001 +

Г). ISO 31000

4. Что такое риск в контексте информационной безопасности?

А). Вероятность угрозы и уязвимости, приводящая к ущербу +

Б). Степень защиты информации

В). Метод оценки информации

Г). Тип угрозы для системы

5. Как называется процесс выявления и оценки рисков информационной безопасности?

А). Аудит

Б). Мониторинг

В). Оценка рисков +

Г). Реагирование на инциденты

6. Какой из следующих элементов не входит в процесс управления инцидентами?

А). Обнаружение инцидента

Б). Реакция на инцидент

В). Генерация прибыли +

Г). Анализ инцидента

7. Что подразумевается под политикой информационной безопасности?

А). Набор принципов и правил, регулирующих защиту информации +

Б). Документ о финансовых расходах на безопасность

В). Программа обучения сотрудников

Г). План по увеличению количества пользователей

8. Какой из перечисленных инструментов не используется для обеспечения безопасности информации?

А). Антивирус

Б). Системы управления доступом

В). Офисное программное обеспечение +

Г). Файрвол

9. Какова основная цель обучения сотрудников в области информационной безопасности?

А). Повышение осведомленности о рисках и угрозах +

Б). Увеличение рабочего времени

В). Снижение затрат на безопасность

Г). Увеличение числа сотрудников

10. Что такое криптография?

А). Процесс уничтожения информации

Б). Наука о защите информации с помощью шифрования +

В). Метод оценки рисков

Г). Процесс создания резервных копий 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

Тест№2

Тема 2. Стандартизация систем и процессов управления информационной безопасностью

1. Что такое стандартизация в контексте информационной безопасности?

А) Процесс создания уникальных решений для каждой организации

Б) Установление общих требований и критериев для защиты информации +

В) Упрощение процессов управления

Г) Процесс получения сертификатов для сотрудников

2. Какой стандарт является наиболее известным в области управления информационной безопасностью?

А) ISO 9001

Б) ISO 14001

В) ISO/IEC 27001 +

Г) ISO 50001

3. Какова основная цель стандарта ISO/IEC 27001?

А) Оптимизация финансовых процессов

Б) Обеспечение систематического подхода к управлению информационной безопасностью +

В) Увеличение производительности
сотрудников

Г) Разработка программного обеспечения

4. Какой элемент является частью системы управления информационной безопасностью (ИСУИБ)?

А) Технические средства

Б) Процессы и процедуры

В) Политики и стандарты безопасности +

Г) Обучение сотрудников

5. Какой из следующих аспектов не относится к стандартам управления информационной безопасностью?

А) Оценка рисков

Б) Реагирование на инциденты

В) Разработка новых технологий +

Г) Обучение персонала

6. Что подразумевается под процессом сертификации в контексте стандартов информационной безопасности?

А) Процесс обучения сотрудников

Б) Официальное подтверждение соответствия требованиям стандарта +

В) Разработка новых стандартов

Г) Процесс оценки финансовой устойчивости

7. Какой стандарт фокусируется на защите персональных данных?

А) ISO 9001

Б) ISO 14001

В) ISO/IEC 27018 +

Г) ISO 31000

8. Какой из следующих стандартов не относится к управлению рисками?

А) ISO 31000

Б) ISO/IEC 27005 +

В) ISO/IEC 27001

Г) ISO 22301

9. Что такое аудит в контексте управления информационной безопасностью?

А) Оценка соответствия процессов и систем установленным стандартам +

Б) Процесс создания новых стандартов
В) Процесс обучения персонала
Г) Разработка программного обеспечения
10. Какова основная задача стандарта ISO/IEC 27002?
А) Предоставление рекомендаций по управлению информационной безопасностью +
Б) Оценка финансовых рисков
В) Разработка программного обеспечения
Г) Обучение сотрудников

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. Политика информационной безопасности
1. Что такое политика информационной безопасности?
А) Набор юридических документов
Б) Официальный документ, определяющий цели и принципы безопасности информации +
В) Инструкция по эксплуатации программного обеспечения
Г) Программа обучения сотрудников
2. Какова основная цель политики информационной безопасности?
А) Увеличение объема данных в организации
Б) Защита конфиденциальности, целостности и доступности информации +
В) Снижение затрат на IT-ресурсы
Г) Обучение сотрудников новым технологиям
3. Какой из следующих элементов не является частью политики информационной безопасности?
А) Определение ролей и ответственности
Б) Процессы реагирования на инциденты
В)Бюджет на IT-оборудование +
Г) Процедуры управления рисками
4. Как часто должна пересматриваться политика информационной безопасности?
А) Один раз в пять лет
Б) Регулярно, в зависимости от изменений в организации и внешней среде +
В) Только при возникновении инцидентов
Г) Один раз в десять лет
5.Кто несет ответственность за реализацию политики информационной безопасности в организации?
А) Только IT-отдел
Б) Все сотрудники, включая руководство +
В) Только сотрудники, занимающиеся безопасностью

Г) Внешние консультанты

6. Какой стандарт предоставляет рекомендации по разработке политики информационной безопасности?

А) ISO 9001

Б) ISO 14001

В) SO/IEC 27002 +

Г) ISO 50001

7. Какой из следующих аспектов может быть включен в политику информационной безопасности?

А) Процедуры работы с персональными данными

Б) Политики доступа к информационным системам +

В) Финансовые отчеты

Г) Обучающие программы для клиентов

8. Что должно быть сделано после разработки политики информационной безопасности?

А) Политика должна быть оставлена без изменений

Б) Политика должна быть доведена до всех сотрудников и обучающего персонала +

В) Политика должна быть опубликована в интернете

Г) Политика должна быть отправлена только руководству

9. Какой из следующих факторов не влияет на политику информационной безопасности?

А) Законодательные требования

Б) Технологические изменения

В) Уровень зарплат сотрудников +

Г) Риски для информационной безопасности

10. Какой элемент помогает обеспечить соблюдение политики информационной безопасности?

А) Процедуры и инструкции

Б) Обучение и повышение осведомленности сотрудников +

В) Системы мониторинга

Г) Все вышеперечисленное

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. Системы управления информационной безопасностью (СУИБ

1. Что такое система управления информационной безопасностью (СУИБ)?

А) Набор программного обеспечения для защиты данных

Б) Комплексный подход к управлению рисками и обеспечению безопасности информации +

В) Инструмент для мониторинга сетевой активности

Г) Методика разработки программного обеспечения

2. Какой стандарт наиболее часто используется для создания СУИБ?

А) ISO 9001

Б) ISO 14001

В) ISO/IEC 27001 +

Г) ISO 50001

3. Какова основная цель СУИБ?

А) Увеличение производительности сотрудников

Б) Обеспечение защиты информации и управление рисками +

В) Снижение затрат на IT-ресурсы

Г) Разработка новых технологий

4. Какой из следующих элементов является частью СУИБ?

А) Только технические средства

Б) Политики и процедуры безопасности +

В) Только финансовые ресурсы

Г) Исключительно программное обеспечение

5. Что подразумевается под процессом управления рисками в СУИБ?

А) Идентификация, оценка и управление рисками, связанными с информационной безопасностью +

Б) Процесс разработки программного обеспечения

В) Оценка производительности сотрудников

Г) Анализ финансовых отчетов

6. Какое действие является частью процесса оценки уязвимостей в СУИБ?

А) Проведение регулярных обучений для сотрудников

Б) Проведение тестов на проникновение +

В) Анализ бизнес-процессов

Г) Разработка новых стандартов

7. Какой из следующих аспектов не является частью мониторинга в СУИБ?

А) Отслеживание инцидентов безопасности

Б) Проведение финансовых проверок +

В) Оценка эффективности мер безопасности

Г) Анализ нарушений политик безопасности

8. Кто должен быть вовлечен в процесс создания и внедрения СУИБ?

А) Только IT-отдел

Б) Все заинтересованные стороны, включая руководство и сотрудников +

В) Только руководство компании

Г) Внешние консультанты

9. Какой метод может быть использован для повышения осведомленности сотрудников о СУИБ?

А) Разработка программного обеспечения

Б) Проведение обучающих семинаров и тренингов +

В) Снижение зарплат

Г) Увеличение рабочего времени

10. Как часто необходимо пересматривать и обновлять СУИБ?

А) Один раз в год

Б) Периодически, в зависимости от изменений в организации и внешней среде+

В) Один раз в пять лет

Г) Только после инцидентов безопасности

Критерии оценивания тестовых заданий для текущего контроля

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

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

Тест№5

Тема 5. Оценка рисков информационной безопасности

1. Что такое оценка рисков информационной безопасности?
А) Процесс создания резервных копий данных
Б) Процесс идентификации, анализа и оценки рисков для информационных активов +
В) Оценка финансовой отчетности
Г) Проверка антивирусного программного обеспечения
2. Какой из следующих этапов не входит в процесс оценки рисков?
А) Идентификация активов
Б) Определение угроз
В) Установление бюджета на IT-ресурсы +
Г) Оценка уязвимостей
3. Что подразумевается под "угрозой" в контексте оценки рисков?
А) Уязвимость системы
Б) Потенциальное событие, способное нанести вред информации +
В) Метод защиты данных
Г) Процесс восстановления данных
4. Какой метод может быть использован для оценки уязвимостей?
А) Тестирование на проникновение +
Б) Повышение осведомленности сотрудников
В) Разработка новых политик безопасности
Г) Проведение финансового аудита
5. Что включает в себя анализ последствий угроз?
А) Оценка финансовых затрат на IT
Б) Определение воздействия угроз на бизнес-процессы и активы +
В) Проверка антивирусных систем
Г) Создание резервных копий данных
6. Какой из следующих терминов описывает вероятность возникновения угрозы?
А) Последствия
Б) Уязвимость
В) Вероятность +
Г) Воздействие
7. Какой метод можно использовать для количественной оценки рисков?
А) SWOT-анализ
Б) Метод анализа вероятности и воздействия +
В) Анализ чувствительности
Г) Метод "мозгового штурма"
8. Что такое риск в контексте информационной безопасности?

А) Защита информации от потери

Б) Вероятность того, что угроза реализация приведет к ущербу для активов +

В) Процесс восстановления данных

Г) Контроль доступа к информации

9. Какой из следующих методов управления рисками может быть использован для уменьшения рисков?

А) Увеличение бюджета на IT

Б) Внедрение мер безопасности и контроль доступа +

В) Игнорирование угроз

Г) Снижение зарплат сотрудников

10. Как часто необходимо проводить оценку рисков информационной безопасности?

А) Один раз в год

Б) Каждые пять лет

В)Регулярно и по мере изменения условий (новые угрозы, изменения в инфраструктуре и т.д.) +

Г) Только после инцидентов безопасности Критерии оценивания тестовых заданий для текущего контроля

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 №6

Тема 6. Процессы управления информационной безопасностью

1. Что такое управление информационной безопасностью?

А) Создание резервных копий данных

Б) Комплекс мероприятий по защите информации от угроз +

В) Мониторинг сетевой активности

Г) Разработка программного обеспечения

2. Какой из следующих процессов является основным в управлении информационной безопасностью?

А) Идентификация и оценка рисков +

Б) Разработка новых технологий

В) Проведение финансового аудита

Г) Увеличение производительности сотрудников

3. Какой из следующих этапов не является частью процесса управления инцидентами безопасности?

А) Обнаружение инцидента

Б) Установление бюджета на IT-ресурсы +

В) Реагирование на инцидент

Г) Анализ последствий инцидента

4. Какой метод может быть использован для обеспечения контроля доступа к информации?

А) Многофакторная аутентификация +

Б) Создание резервных копий

В) Проведение финансовых проверок

Г) Разработка новых политик безопасности

5. Что подразумевается под процессом управления изменениями в контексте информационной безопасности?

А) Обновление программного обеспечения

В)Процесс контроля и управления изменениями в IT-системах для минимизации рисков +

В) Проведение обучений для сотрудников

Г) Создание новых функций в приложениях

6. Какой из следующих элементов является частью процесса управления активами информационной безопасности?

А) Идентификация и классификация информационных активов +

Б) Проведение тестов на проникновение

В) Обучение сотрудников

Г) Разработка резервных копий

7. Какой из следующих процессов помогает в управлении уязвимостями? +

А) Регулярное сканирование систем на наличие уязвимостей

Б) Увеличение бюджета на IT

В) Проведение финансового аудита

Г) Разработка новых политик безопасности

8. Какая цель процесса мониторинга безопасности?

А) Увеличение объемов данных

Б) Обнаружение и реагирование на инциденты безопасности в реальном времени +

В) Проведение финансовых проверок

Г) Обучение сотрудников новым технологиям

9. Какой из следующих инструментов используется для анализа инцидентов безопасности?

А) Логи событий и системы мониторинга +

Б) Финансовая отчетность

В) Опросы сотрудников

Г) SWOT-анализ

10. Как часто необходимо пересматривать процессы управления информационной безопасностью?

А) Один раз в год

Б) Каждые пять лет

В) Регулярно и при изменении условий, угроз или инфраструктуры +

Г) Только после инцидентов безопасности Критерии оценивания тестовых заданий для текущего контроля

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 является основной целью управления информационной безопасностью?
a) Максимизация прибыли организации
b) Обеспечение конфиденциальности, целостности и доступности информации
c) Ускорение обработки данных
d) Обеспечение физической безопасности персонала
2. Какой из перечисленных документов определяет общие подходы к обеспечению ИБ в организации?
a) Политика информационной безопасности
b) Техническое задание на разработку ПО
c) Устав организации
d) График отпусков сотрудников
3. Согласно ISO/IEC 27001, что является первым этапом реализации системы управления ИБ (СУИБ)?
a) Внедрение антивирусного ПО
b) Определение контекста организации и заинтересованных сторон
c) Проведение аудита ИБ
d) Назначение ответственного по ИБ
4. Что такое «информационный риск»?
a) Вероятность наступления угрозы с учётом уязвимостей и последствий
b) Любое вредоносное ПО
c) Неисправность сервера
d) Отсутствие политики ИБ
5. Какой из перечисленных стандартов является национальным российским аналогом ISO/IEC 27001?
a) ГОСТ Р 57580
b) ГОСТ Р ИСО/МЭК 27001
c) ФЗ-152
d) ГОСТ Р 56939
6. Что включает в себя «анализ рисков информационной безопасности»?
a) Только проверку наличия лицензий на ПО
b) Идентификацию активов, угроз, уязвимостей и оценку уровня риска
c) Обучение сотрудников правилам внутреннего распорядка
d) Покупку оборудования защиты
7. Какой из перечисленных принципов НЕ относится к триаде CIA (основные свойства ИБ)?
a) Конфиденциальность
b) Целостность
c) Аутентификация
d) Доступность
8. Что такое «политика информационной безопасности»?
a) Набор технических инструкций для ИТ-специалистов
b) Документ, определяющий цели, принципы и общие подходы к обеспечению ИБ
c) Учебное пособие по криптографии
d) Перечень запрещённых сайтов
9. Какой федеральный закон регулирует обработку персональных данных в РФ?
a) ФЗ-187
b) ФЗ-152
c) ФЗ-149

d) ФЗ-263
10. Кто несёт ответственность за управление ИБ в организации согласно нормативным требованиям РФ?
a) Только ИТ-директор
b) Только служба безопасности
c) Руководитель организации
d) Внешний аудитор
11. Какой из перечисленных методов НЕ является мерой управления ИБ?
a) Разработка регламентов доступа к информации
b) Проведение обучения сотрудников
c) Установка кондиционера в серверной
d) Шифрование данных
12. Что подразумевает «классификация информации»?
a) Разделение информации по уровню ценности и чувствительности
b) Архивирование старых данных
c) Использование облачного хранилища
d) Перевод документов на иностранный язык
13. Какой из перечисленных подходов используется при выборе мер защиты в СУИБ?
a) На основе стоимости оборудования
b) На основе результатов анализа рисков
c) Произвольный выбор
d) По рекомендации коллег
14. Что такое «инцидент информационной безопасности»?
a) Любое событие, нарушающее политику ИБ или угрожающее активам
b) Отключение электричества
c) Отпуск сотрудника
d) Обновление антивируса
15. Какой из перечисленных документов относится к внутренним регламентам ИБ?
a) Приказ о назначении ответственного за ИБ
b) Письмо из Минцифры
c) Счёт за интернет
d) Трудовой договор
16. Какова роль внутреннего аудита в СУИБ?
a) Оценка соответствия реализованных мер требованиям политики и стандартов ИБ
b) Подбор персонала в ИТ-отдел
c) Закупка оборудования
d) Формирование маркетинговой стратегии
17. Что означает термин «уязвимость» в контексте ИБ?
a) Слабое место в системе, которое может быть использовано угрозой
b) Вредоносное ПО
c) Отсутствие бюджета на ИБ
d) Высокая нагрузка на сервер
18. Какой из перечисленных документов НЕ требуется при сертификации по ISO/IEC 27001?
a) Политика ИБ
b) Матрица рисков
c) Отчёт о прибыли компании
d) Реестр активов
19. Какой уровень защищённости персональных данных устанавливается по ФЗ-152?
a) Один уровень
b) Два уровня
c) Три уровня

d) Четыре уровня
20. Какой из перечисленных принципов лежит в основе модели PDCA в СУИБ?
a) Планирование → Действие → Проверка → Коррекция
b) Проектирование → Разработка → Тестирование → Внедрение
c) Анализ → Производство → Продажа → Поддержка
d) Покупка → Установка → Использование → Утилизация
21. Что такое «риск-ориентированный подход» в управлении ИБ?
a) Сосредоточение усилий на угрозах с наибольшими последствиями для бизнеса
b) Защита всех данных одинаково
c) Использование только бесплатных средств защиты
d) Отказ от внедрения СУИБ
22. Какой из перечисленных документов может содержать перечень разрешённых и запрещённых действий пользователей?
a) Регламент работы с информацией
b) График отпусков
c) Прайс-лист на оборудование
d) Устав организации
23. Кто определяет цели системы управления ИБ?
a) Только внешний консультант
b) Руководство организации
c) Бухгалтерия
d) Пользователи сети
24. Какой из перечисленных видов угроз является внутренним?
a) DDOS-атака извне
b) Утечка данных сотрудником
c) Сбой электропитания
d) Взлом из внешней сети
25. Что подразумевает «подход на основе процессов» в СУИБ?
a) Управление ИБ как совокупностью связанных бизнес-процессов
b) Использование только программных решений
c) Работа только с внешними аудиторами
d) Игнорирование человеческого фактора
26. Какое из следующих положений НЕ относится к требованиям ФЗ-152?
a) Назначение ответственного за обработку ПДн
b) Получение согласия субъекта на обработку ПДн
c) Обязательное хранение ПДн только на территории РФ
d) Обязательное использование только отечественного ПО
27. Какой из перечисленных методов защиты относится к организационным мерам?
a) Установка межсетевого экрана
b) Разработка и утверждение регламентов доступа
c) Шифрование базы данных
d) Резервное копирование
28. Что такое «реестр рисков»?
a) Список всех угроз, известных человечеству
b) Документ, содержащий идентифицированные риски, их уровень и меры по снижению
c) Журнал посещений серверной
d) Каталог оборудования
29. Какой из перечисленных стандартов описывает практические рекомендации по контролю ИБ?
a) ISO/IEC 27000
b) ISO/IEC 27002
c) ISO/IEC 27005

d) ISO 9001
30. Что такое «информационный актив»?
a) Любой ресурс, имеющий ценность для организации (данные, оборудование, ПО и др.)
b) Только серверы
c) Только персональные данные
d) Только документы в бумажном виде

Ключ к тесту:
1 – b, 2 – a, 3 – b, 4 – a, 5 – b, 6 – b, 7 – c, 8 – b, 9 – b, 10 – c, 11 – c, 12 – a, 13 – b, 14 – a, 15 – a, 16 – a, 17 – a, 18 – c, 19 – d, 20 – a, 21 – a, 22 – a, 23 – b, 24 – b, 25 – a, 26 – d, 27 – b, 28 – b, 29 – b, 30 – a

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 №____