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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

СТАНДАРТЫ 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 Стандарты 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 Стандарты 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 Стандарты 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-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 Применяет в профессиональной деятельности знания нормативной правовой базы РФ в области информационной безопасности	Знать: профессиональной деятельности знания нормативной правовой базы РФ в области информационной безопасности Уметь: Проводить анализ знаний нормативной правовой базы РФ в области информационной безопасности Владеть: знаниями нормативной правовой базы РФ в области информационной безопасности	Тема 1. Понятие безопасности информации. Тема 2. Международные и российские стандарты по защите информации: их взаимосвязь и различия. Тема 3. Особенности процесса стандартизации и стандарты безопасности в сети Интернет. Тема 4. Особенности государственных стандартов программных продуктов Тема 5. Государственные	Реферат (Тема 1) Тест (тема 1)	Тест (П 1-20 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
			стандарты: общие положения.		
	ОПК-5.2 Демонстрирует умение решать стандартные профессиональные задачи с целью выполнения требований нормоконтролеров РФ	Знать. Стандарты и методологии управления проектами (например, PMBOK, Agile) Уметь: Взаимодействовать с заинтересованными сторонами и обеспечивать их вовлеченность в проект. Владеть: Способностью применять на практике методы оценки и контроля выполнения проекта на всех его этапах. расходами на ИТ предприятия; Уметь: инициировать и планировать выполнения задач управления ИТ-инфраструктурой и согласование с заинтересованными лицами этих планов и определять цель управления расходами на ИТ, согласовывать их с заинтересованными лицами и доводить их до сведения персонала, управляющего расходами на ИТ предприятия; Владеть: навыками инициации и планирования выполнения задач управления ИТ-инфраструктурой и	Тема 6. Руководящий документ Гостехкоммиссии: Межсетевые экраны Тема 7. Основы сертификации (на примере средств защиты информации). Тема 8. Сертификация на соответствие требованиям по безопасности информации Тема 9. Системы сертификации средств защиты информации: требования безопасности информации.	Реферат (Тема 2-4) Тест (Тема 2-4) Практическое задание (Тема 1-4)	Тест (П 21-25 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
		согласования с заинтересованными лицами этих планов и определения цели управления расходами на ИТ, согласования их с заинтересованными лицами и доведения их до сведения персонала, управляющего расходами на ИТ предприятия			

2. Оценочные материалы по дисциплине «Базы данных»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема1. Понятие безопасности информации.

1. Введение в безопасность информации

2. Основные компоненты безопасности информации

3. Угрозы безопасности информации

4. Политики безопасности информации

5. Технологии защиты информации

6. Роль обучения сотрудников в безопасности информации

7. Законодательство в области безопасности информации

8. Стандарты безопасности информации

9. Оценка рисков в области безопасности информации

10. Инциденты безопасности информации

11. Аудит безопасности информации

12. Будущее безопасности информации

13. Этические аспекты безопасности информации

14. Социальная инженерия как угроза безопасности информации

15. Роль международного сотрудничества в обеспечении безопасности информации

Тема 2. Международные и российские стандарты по защите информации: их взаимосвязь и различия.

1. Введение в международные стандарты защиты информации
2. Основные международные стандарты по защите информации
3. Обзор российских стандартов в области защиты информации
4. Взаимосвязь между международными и российскими стандартами
5. Сравнительный анализ ISO/IEC 27001 и ГОСТ Р 56326
6. Роль ISO/IEC 27002 в контексте российских стандартов
7. Защита персональных данных: международные и российские подходы
8. Стандарты безопасности информации в сфере финансов
9. Особенности внедрения международных стандартов в России
10. Адаптация международных стандартов к российскому законодательству
11. Проблемы и вызовы при гармонизации стандартов
12. Практические примеры применения стандартов в России
13. Будущее международных и российских стандартов по защите информации

14. Роль государственных органов в стандартизации защиты информации
15. Перспективы развития национальных стандартов в свете международных тенденций

Тема 3. Особенности процесса стандартизации и стандарты безопасности в сети Интернет.
1. Введение в процесс стандартизации в области безопасности в сети Интернет
2. История и развитие стандартов безопасности в Интернете
3. Основные организации, занимающиеся стандартизацией в области ИТ-безопасности
4. Стандарты ISO/IEC 27001 и их применение в кибербезопасности
5. Роль NIST в разработке стандартов безопасности для Интернета
6. Стандарты безопасности для веб-приложений: OWASP и их влияние
7. GDPR и его влияние на стандарты безопасности данных в Интернете
8. Проблемы и вызовы стандартизации безопасности в условиях быстро меняющегося ИТ-ландшафта
9. Адаптация международных стандартов к специфике локальных рынков
10. Влияние технологий блокчейн на стандарты безопасности в сети Интернет
11. Стандарты безопасности для IoT: проблемы и решения
12. Оценка рисков и управление ими в процессе стандартизации безопасности
13. Будущее стандартов безопасности в свете новых технологий (AI, ML)
14. Роль правительственных организаций в процессе стандартизации безопасности
15. Практические примеры внедрения стандартов безопасности в корпоративной среде

Тема 4. Особенности государственных стандартов программных продуктов

1. Введение в государственные стандарты программных продуктов
2. История развития государственных стандартов в области программного обеспечения
3. Основные цели и задачи государственных стандартов программных продуктов
4. Классификация государственных стандартов программных продуктов
5. Влияние международных стандартов на государственные стандарты программного обеспечения
6. Процесс разработки и утверждения государственных стандартов
7. Роль государственных органов в стандартизации программных продуктов
8. Примеры государственных стандартов программных продуктов в разных странах
9. Актуальные проблемы и вызовы в стандартизации программного обеспечения
10. Влияние технологий на государственные стандарты программных продуктов
11. Соответствие государственных стандартов требованиям безопасности
12. Оценка соответствия и сертификация программных продуктов по государственным стандартам
13. Практические аспекты внедрения государственных стандартов в организациях
14. Будущее государственных стандартов программных продуктов в условиях цифровизации
15. Сравнительный анализ государственных стандартов программных продуктов разных стран

Тема 5. Государственные стандарты: общие положения.
1. Введение в государственные стандарты: определение и значение
2. История развития государственных стандартов в России
3. Основные цели и задачи государственных стандартов
4. Классификация государственных стандартов: виды и категории
5. Процесс разработки государственных стандартов: этапы и участники
6. Роль государственных органов в системе стандартизации

7. Влияние международных стандартов на национальные системы стандартизации
8. Примеры государственных стандартов в разных отраслях экономики
9. Актуальные проблемы и вызовы в области стандартизации
10. Соответствие государственных стандартов требованиям качества
11. Оценка соответствия: методы и процедуры
12. Практические аспекты внедрения государственных стандартов в организациях
13. Будущее государственных стандартов в условиях цифровой трансформации
14. Сравнительный анализ государственных стандартов разных стран
15. Роль государственных стандартов в обеспечении безопасности продукции

Тема 6. Руководящий документ Гостехкоммиссии: Межсетевые экраны
1. Введение в межсетевые экраны: назначение и функции
2. Основные требования Гостехкомиссии к межсетевым экранам
3. Классификация межсетевых экранов по архитектуре и функциям
4. Принципы работы межсетевых экранов: фильтрация и контроль трафика
5. Роль межсетевых экранов в обеспечении информационной безопасности
6. Актуальные угрозы и риски для сетевой инфраструктуры
7. Процесс сертификации межсетевых экранов в соответствии с требованиями Гостехкомиссии
8. Методики тестирования и оценки эффективности межсетевых экранов
9. Современные технологии и тренды в области межсетевых экранов
10. Интеграция межсетевых экранов с другими средствами защиты информации
11. Примеры успешного применения межсетевых экранов в организациях
12. Ошибки и проблемы при внедрении межсетевых экранов
13. Будущее межсетевых экранов: прогнозы и перспективы развития
14. Роль межсетевых экранов в контексте киберугроз и атак
15. Практические рекомендации по выбору и настройке межсетевых экранов

Тема 7. Основы сертификации (на примере средств защиты информации).
1. Введение в сертификацию средств защиты информации
2. Законодательные и нормативные основы сертификации в России
3. Процесс сертификации: этапы и процедуры
4. Роль аккредитованных органов по сертификации в области защиты информации
5. Классификация средств защиты информации и их сертификация
6. Методы оценки соответствия средств защиты информации
7. Стандарты и требования к средствам защиты информации
8. Примеры успешной сертификации средств защиты информации
9. Актуальные проблемы и вызовы в области сертификации
10. Влияние международных стандартов на сертификацию средств защиты информации
11. Сертификация программного обеспечения для защиты информации
12. Оценка рисков и сертификация: связь и взаимодействие
13. Роль сертификации в обеспечении информационной безопасности организаций
14. Будущее сертификации средств защиты информации в условиях цифровизации
15. Практические аспекты внедрения сертифицированных средств защиты информации в организациях

Тема 8. Сертификация на соответствие требованиям по безопасности информации
1. Введение в сертификацию безопасности информации
2. Основные стандарты и нормы в области сертификации
3. Процесс сертификации: этапы и процедуры
4. Роль сертификации в обеспечении информационной безопасности

5. Требования к системам управления информационной безопасностью (СУИБ)
6. Сертификация программного обеспечения на безопасность
7. Аудит и оценка соответствия: методы и подходы
8. Влияние сертификации на доверие пользователей и клиентов
9. Проблемы и вызовы в процессе сертификации безопасности информации
10. Примеры успешной сертификации в различных отраслях
11. Сертификация в контексте международных стандартов (ISO/IEC 27001)
12. Роль аккредитованных органов в процессе сертификации
13. Тренды и перспективы развития сертификации безопасности информации
14. Соответствие требованиям законодательства в области защиты информации
15. Практические рекомендации по подготовке к сертификации на соответствие требованиям безопасности информации

Тема 9. Системы сертификации средств защиты информации: требования безопасности информации.

1. Введение в системы сертификации средств защиты информации
2. Основные требования безопасности информации в сертификации
3. Классификация средств защиты информации и их сертификация
4. Процесс сертификации: этапы и методологии
5. Роль стандартов ISO в сертификации средств защиты информации
6. Оценка соответствия средств защиты информации: методы и подходы
7. Аудит систем защиты информации и его значение для сертификации
8. Проблемы и вызовы в сертификации средств защиты информации
9. Сертификация программного обеспечения и его безопасность
10. Влияние сертификации на рынок средств защиты информации
11. Практические примеры сертификации средств защиты информации
12. Законодательные требования к сертификации в области информационной безопасности
13. Роль аккредитованных органов в процессе сертификации
14. Тренды и перспективы развития систем сертификации средств защиты информации
15. Рекомендации по подготовке к сертификации средств защиты информации

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 безопасности информации

Исследования понятия безопасности информации, его ключевых компонентов, принципов и методов обеспечения безопасности, а также в анализе современных угроз и вызовов в области информационной безопасности.

Вопросы для самоконтроля:

1. Что такое безопасность информации и почему она важна в современном обществе?
2. Какие основные компоненты входят в понятие безопасности информации?
3. Каковы основные цели безопасности информации?
4. Какие существуют классификации угроз безопасности информации?
5. Какие методы и средства защиты информации наиболее распространены?

Цель работы–ознакомление с основными понятиями информационной безопасности и освоение принципов классификации видов угроз и средств защиты информации

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. Международные и российские стандарты по защите информации: их взаимосвязь и различия.

Формирование теоретических навыков по изучению международной и отечественной нормативной базы в области защиты информации, ознакомление с ключевыми международными и российскими стандартами, изучение их сходств и отличий.

Вопросы для самоконтроля:

1.Какие основные международные стандарты регулируют сферу защиты информации?

2.Какие отечественные нормативные документы являются основой правовой охраны персональных данных?

3.В чём заключаются принципиальные различия международного и российского подхода к вопросам защиты информации?

4.Почему важно учитывать международный опыт при формировании национальных стандартов?

Цель работы- формирование теоретических навыков по изучению международной и отечественной нормативной базы в области защиты информации, ознакомление с ключевыми международными и российскими стандартами, изучение их сходств и отличий.

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. Особенности процесса стандартизации и стандарты безопасности в сети Интернет.

Стандартизация в интернете и стандарты безопасности. Роль стандартов в обеспечении интероперабельности, доступности и безопасности. Обзор основных организаций по стандартизации (IETF, W3C, ISO). Наиболее важные стандарты безопасности (TLS/SSL, DNSSEC, HTTPS, криптографические протоколы). Уязвимости, связанные с несоблюдением стандартов.

Вопросы для самоконтроля:

1.Какова роль стандартизации в развитии и функционировании интернета?

2.Какие организации занимаются стандартизацией в интернете?

3.Какие стандарты безопасности вы знаете и для чего они используются?

4.Какие последствия могут возникнуть из-за несоблюдения стандартов безопасности?

5.Как TLS/SSL обеспечивает безопасность передачи данных в интернете?

Цель работы− Ознакомление с процессом стандартизации в интернете и понимание влияния соблюдения стандартов безопасности на устойчивость и защищенность сетевой инфраструктуры. Получение практических навыков анализа уязвимостей, связанных с несоблюдением стандартов.

В работе используется база данных выполненная в MS Access/

Критерии оценивания выполнения практического задания:

Оценка	Критерии
«Отлично»	*Задание выполнено самостоятельно. Алгоритм решения задания верный, в логических рассуждениях нет ошибок/*
«Хорошо»	*Задание выполнено с помощью преподавателя. Алгоритм решения задания в целом верный, в логическом рассуждении и выполнении нет существенных ошибок; есть объяснение выполнения заданий, допущено не более двух несущественных ошибок.*
«Удовлетворительно»	*Задание выполнено с подсказками преподавателя. Задание понято правильно, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в поставленной задаче; задание выполнено не полностью или в общем виде.*
«Неудовлетворительно»	*Задание не выполнено..*

Тема 4. Особенности государственных стандартов программных продуктов

Обзор государственных стандартов в области разработки программного обеспечения. ГОСТы, определяющие требования к жизненному циклу ПО, качеству, безопасности и документированию. Роль государственных стандартов в обеспечении совместимости, надежности и безопасности программных продуктов, особенно в критически важных областях. Сравнение с международными стандартами (ISO, IEEE). Процесс сертификации программного обеспечения на соответствие государственным стандартам.

Вопросы для самоконтроля:

1.Какие государственные стандарты в области разработки ПО вам известны?

2.Какова цель применения государственных стандартов к программным продуктам?

3.В чем заключаются основные требования госстандартов к качеству, безопасности и документированию ПО?

4.В чем отличия государственных стандартов от международных (ISO, IEEE) в области ПО?

5.Как происходит процесс сертификации ПО на соответствие государственным стандартам?

Цель работы− Ознакомление с особенностями государственных стандартов в области разработки программного обеспечения, понимание их роли в обеспечении качества, безопасности и совместимости программных продуктов, а также формирование навыков анализа соответствия ПО требованиям стандартов.

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 5. Государственные стандарты: общие положения.

Основы государственной стандартизации. Цели, задачи и принципы стандартизации. Законодательная база стандартизации (ФЗ "О стандартизации в Российской Федерации"). Уровни стандартизации (международный, региональный, национальный, организации). Структура национальной системы стандартизации. Категории стандартов (ГОСТ, ГОСТ Р, ГОСТ Р ИСО, ГОСТ Р МЭК, и др.). Процесс разработки, утверждения и применения государственных стандартов.

Вопросы для самоконтроля:

1.Каковы основные цели и задачи государственной стандартизации?

2.На каких принципах строится система стандартизации в Российской Федерации?

3.Какие законы регулируют отношения в области стандартизации в РФ?

4.Какие уровни стандартизации существуют?

5.Какие категории стандартов применяются в Российской Федерации (ГОСТ, ГОСТ Р и др.)?

6.Опишите процесс разработки и утверждения государственного стандарта.

Цель работы− Получение знаний об основах государственной стандартизации, ее целях, задачах, принципах, и законодательной базе. Развитие навыков анализа структуры национальной системы стандартизации и процесса разработки стандартов.

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 6. Руководящий документ Гостехкоммиссии: Межсетевые экраны

Анализ руководящего документа Гостехкомиссии (ФСТЭК России) по межсетевым экранам (МЭ). Цели и задачи регулирования. Классификация МЭ по функциональным возможностям и областям применения. Требования к функциональности, безопасности и надежности МЭ. Процедуры оценки соответствия МЭ требованиям безопасности. Сравнение требований Гостехкомиссии с международными стандартами (например, Common Criteria).

Вопросы для самоконтроля:

1.Какова цель издания руководящих документов ФСТЭК России по межсетевым экранам?

2.Какие основные классы межсетевых экранов выделяются согласно требованиям ФСТЭК?

3.Какие требования предъявляются к функциональности, безопасности и надежности межсетевых экранов?

4.Как осуществляется оценка соответствия межсетевых экранов требованиям безопасности, установленным ФСТЭК?

5.В чем заключаются основные отличия требований ФСТЭК к межсетевым экранам от международных стандартов (например, Common Criteria)?

Цель работы− Изучение руководящего документа ФСТЭК России, определяющего требования к межсетевым экранам, понимание целей и задач государственного регулирования в области защиты информации, а также формирование навыков анализа требований к МЭ и процедур оценки соответствия.

.

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 7. Основы сертификации (на примере средств защиты информации).

Сертификация средств защиты информации (СЗИ) в Российской Федерации. Цели и принципы сертификации. Законодательная и нормативная база. Органы по сертификации и испытательные лаборатории. Схемы сертификации. Процедура сертификации СЗИ: подача заявки, проведение испытаний, выдача сертификата. Инспекционный контроль. Виды сертификатов. Ответственность изготовителей и поставщиков СЗИ. Добровольная и обязательная сертификация.

Вопросы для самоконтроля:

1.Каковы основные цели сертификации средств защиты информации?

2.Какие органы в Российской Федерации осуществляют сертификацию СЗИ?

3.Опишите основные этапы процесса сертификации СЗИ.

4.Что такое инспекционный контроль и для чего он проводится?

5.В чем разница между добровольной и обязательной сертификацией СЗИ?

6.Какова ответственность изготовителей и поставщиков СЗИ за соответствие продукции требованиям безопасности?

Цель работы− Освоение теоретических основ сертификации СЗИ, понимание целей, принципов и процедур сертификации, а также формирование навыков анализа нормативной базы и процедур оценки соответствия СЗИ требованиям безопасности.

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 8. Сертификация на соответствие требованиям по безопасности информации

Требования к безопасности информации, используемые при сертификации. Стандарты и руководящие документы ФСТЭК России (например, по межсетевым экранам, антивирусным средствам, системам обнаружения вторжений). Уровни доверия к средствам защиты информации. Методы и средства контроля соответствия требованиям безопасности: тестирование, анализ исходного кода, документации. Критерии оценки соответствия: функциональность, устойчивость к угрозам, соответствие документации. Практические аспекты подготовки к сертификации: разработка технической документации, проведение предварительных испытаний.

Вопросы для самоконтроля:

1.Какие основные стандарты и руководящие документы ФСТЭК России используются при сертификации на соответствие требованиям по безопасности информации?

2.Что такое уровень доверия к средству защиты информации, и какие уровни доверия существуют?

3.Какие методы и средства контроля соответствия требованиям безопасности используются при сертификации?

4.Какие критерии используются для оценки соответствия средства защиты информации требованиям безопасности?

5.Какие практические шаги необходимо предпринять для подготовки к сертификации на соответствие требованиям по безопасности информации?

Цель работы: Углубление знаний о требованиях по безопасности информации, применяемых при сертификации, изучение методов и критериев оценки соответствия, а также приобретение практических навыков подготовки к сертификации.

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 9. Системы сертификации средств защиты информации: требования безопасности информации.

Анализ различных систем сертификации средств защиты информации (СЗИ) с точки зрения предъявляемых ими требований безопасности. Национальная система сертификации ФСТЭК России. Международные системы сертификации (Common Criteria, ISO/IEC 27001). Сравнение требований безопасности, предъявляемых различными системами сертификации к одним и тем же типам СЗИ. Идентификация наиболее строгих требований. Влияние выбора системы сертификации на стоимость и сроки проведения работ.

Вопросы для самоконтроля:

1.Какие основные системы сертификации средств защиты информации существуют?

2.Какие требования безопасности предъявляются к СЗИ в рамках национальной системы сертификации ФСТЭК России?

3.Какие требования безопасности предъявляются к СЗИ в рамках международной системы сертификации Common Criteria?

4.В чем заключаются основные различия между требованиями безопасности, предъявляемыми различными системами сертификации?

5.Как выбор системы сертификации влияет на стоимость и сроки проведения работ по сертификации?

Цель работы: Сравнение требований к безопасности информации в различных системах сертификации СЗИ, понимание преимуществ и недостатков каждой системы, и формирование навыков выбора оптимальной системы сертификации в зависимости от конкретных задач..

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 безопасности информации.

1. Что такое безопасность информации?
А) Защита информации от несанкционированного доступа +
Б) Процесс хранения данных
В) Увеличение объема данных
Г) Упрощение доступа к информации

2. Какой из следующих аспектов не относится к безопасности информации?
А) Конфиденциальность
Б) Доступность
В) Неправомерное использование +
Г) Целостность

3. Какой тип угрозы информации является физическим?
А) Вирусы
Б) Фишинг
В) Пожар +
Г) Социальная инженерия

4. Что такое криптография?
А) Наука о хранении информации
Б) Метод защиты информации с использованием шифрования +
В) Процесс передачи данных
Г) Способ удаления данных

5. Какой из следующих методов является мерой по обеспечению безопасности информации?
А) Регулярное обновление программного обеспечения +
Б) Увеличение объема памяти устройства
В) Установка дополнительных приложений для игр
Г) Использование одинаковых паролей для всех аккаунтов

6. Что такое фишинг?
А) Метод шифрования данных
Б) Атака, направленная на получение конфиденциальной информации через обман+
В) Способ защиты от вирусов
Г) Процесс резервного копирования данных

7. Какой из следующих факторов не влияет на безопасность информации?
А) Обучение сотрудников
Б) Использование сложных паролей
В) Объем хранимых данных +
Г) Регулярные аудиты безопасности

8. Что такое брандмауэр?

А) Программа для шифрования данных

Б) Устройство или программа, контролирующая входящий и исходящий сетевой трафик +

В) Средство для резервного копирования информации

Г) Способ защиты от физических угроз

9. Какой из следующих методов является примером социальной инженерии?

А) Взлом пароля через перебор

Б) Поддельные электронные письма от имени банка +

В) Установка антивирусного ПО

Г) Использование VPN-сервисов

10. Какой из следующих принципов безопасности информации подразумевает защиту данных от несанкционированного изменения?

А) Конфиденциальность

Б) Доступность

В) Целостность +

Г) Аутентификация

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. Международные и российские стандарты по защите информации: их взаимосвязь и различия.

1. Какой международный стандарт является основным для управления информационной безопасностью?

А) ISO/IEC 27001 +

Б) ISO 9001

В) ISO 14001

Г) ISO/IEC 20000

2. Какой российский стандарт соответствует международному стандарту ISO/IEC 27001?

А) ГОСТ Р ИСО/IEC 27001 +

Б) ГОСТ Р 50922

В) ГОСТ Р 57580
Г) ГОСТ Р 52633

3. Что обозначает аббревиатура GDPR?
А) General Data Protection Regulation +
Б) Global Data Privacy Regulation
В) General Data Policy Regulation
Г) Global Data Protection Rules

4. Какой из следующих стандартов применяется в России для оценки рисков информационной безопасности?
А) ISO/IEC 27005 +
Б) ГОСТ Р 51141
В) ISO 31000
Г) ГОСТ Р 57580

5. Какой из перечисленных стандартов не является международным?
А) ISO/IEC 27002
Б) NIST SP 800-53
В) ГОСТ Р ИСО/IEC 27002 +
Г) COBIT

6. Какой из следующих принципов является основополагающим в стандарте ISO/IEC 27001?
А) Принцип минимизации данных
Б) Принцип целостности данных
В) Принцип управления рисками +
Г) Принцип доступности данных

7. Какой стандарт определяет требования к системам менеджмента информационной безопасности в России?
А) ISO/IEC 27003
Б) ГОСТ Р ИСО/IEC 27001 +
В) ISO/IEC 27005
Г) ГОСТ Р 50922

8. Что из следующего не является целью стандарта ISO/IEC 27002?
А) Обеспечение конфиденциальности информации
Б) Обеспечение доступности информации
В) Определение требований к юридическим аспектам бизнеса +
Г) Обеспечение целостности информации

9. Какой из следующих документов регулирует защиту персональных данных в России?
А) Федеральный закон "О защите персональных данных" +
Б) GDPR

В) ISO/IEC 27018
Г) NIST SP 800-37

10. Что обозначает термин "взаимосвязь" в контексте международных и российских стандартов защиты информации?
А) Различия в подходах к защите информации
Б) Совпадение требований и принципов стандартов разных стран +
В) Конфликт между стандартами разных стран
Г) Отсутствие общих норм и правил
Правильный ответ: b)

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. Особенности процесса стандартизации и стандарты безопасности в сети Интернет.

1. Какой из следующих стандартов определяет основные принципы безопасности в интернете?
А) ISO/IEC 27001 +
Б) RFC 1918
В) ISO/IEC 27002
Г) NIST SP 800-53

2. Какой орган отвечает за разработку стандартов в области сетевой безопасности в США?
А) ISO
Б) NIST +
В) ITU
Г) IEEE

3. Что означает аббревиатура SSL?
А) Secure Socket Layer +
Б) Secure System Layer
В) Safety Socket Layer
Г) Secure Service Layer

4. Какой протокол используется для защищенной передачи данных в интернете?
А) HTTP
Б) FTP
В) HTTPS +

Г) SMTP

5. Какой стандарт описывает меры по обеспечению безопасности персональных данных в интернете?

А) ISO/IEC 27018 +
Б) ISO 9001
В) ISO/IEC 20000
Г) ISO 14001

6. Что такое DDoS-атака?

А) Атака на базу данных
Б) Распределенная атака на отказ в обслуживании +
В) Атака на шифрование данных
Г) Атака на локальную сеть

7. Какой из следующих документов является основным в области управления рисками информационной безопасности?

А) ISO/IEC 27001
Б) ISO/IEC 31000 +
В) NIST SP 800-30
Г) COBIT

8. Какой стандарт касается управления инцидентами в области информационной безопасности?

А) ISO/IEC 27035 +
Б) ISO/IEC 27005
В) ISO/IEC 27002
Г) ISO/IEC 27017

9. Какой из следующих протоколов обеспечивает безопасность электронной почты?

А) IMAP
Б) POP3
В) SMTP с TLS +
Г) FTP

10. Какой стандарт используется для оценки уровня зрелости процессов управления безопасностью информации?

А) CMMI +
Б) ISO/IEC 27001
В) COBIT
Г) ITIL
Правильный ответ: а)

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 Особенности государственных стандартов программных продуктов

1. Какой из следующих документов определяет основные требования к программным продуктам в России?

А) ГОСТ Р 51522 +
Б) ГОСТ Р 51141
В) ГОСТ Р 52780
Г) ГОСТ Р 57150

2. Что означает аббревиатура "ГОСТ"?

А) Государственный стандарт +
Б) Глобальный стандарт
В) Генеральный стандарт
Г) Групповой стандарт

3. Какой стандарт регламентирует процесс разработки программного обеспечения?

А) ГОСТ Р ИСО/МЭК 12207 +
Б) ГОСТ Р 50779.42
В) ГОСТ Р 57580
Г) ГОСТ Р 50779.42-2010

4. Какой из следующих стандартов описывает требования к документации на программное обеспечение?

А) ГОСТ Р 51141
Б) ГОСТ Р 50779.41 +
В) ГОСТ Р 52780
Г) ГОСТ Р 57150

5. Какой из стандартов касается оценки качества программного обеспечения?

А) ГОСТ Р 50779.42
Б) ГОСТ Р 57580
В) ГОСТ Р 51267 +
Г) ГОСТ Р 51141

6. Что такое "сертификация" программного продукта?

А) Процесс разработки нового ПО
Б) Оценка соответствия ПО установленным требованиям +
В) Процесс тестирования программного обеспечения
Г) Процесс обновления ПО

7. Какой стандарт регулирует безопасность программных продуктов?

А) ГОСТ Р 51522

Б) ГОСТ Р ИСО/МЭК 27001

В) ГОСТ Р 50779.43 +

Г) ГОСТ Р 57580

8. Какое из следующих утверждений верно для государственных стандартов?

А) Они обязательны только для государственных организаций.

Б) Они не применимы к частным компаниям.

В) Они обязательны для всех организаций, работающих с государственными заказами. +

Г) Они действуют только в пределах одной области.

9. Какой из следующих стандартов используется для оценки жизненного цикла программного обеспечения?

А) ГОСТ Р ИСО/МЭК 12207 +

Б) ГОСТ Р 57580

В) ГОСТ Р 51141

Г) ГОСТ Р 50779.41

10. Какой стандарт охватывает вопросы управления проектами в области разработки ПО?

А) ГОСТ Р 51267

Б) ГОСТ Р ИСО/МЭК 15504 +

В) ГОСТ Р 57150

Г) ГОСТ Р ИСО 9001

Критерии оценивания тестовых заданий для текущего контроля

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

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

Тест №5

Тема 5 Государственные стандарты: общие положения.

1. Что такое государственный стандарт (ГОСТ)?

А) Нормативный документ, устанавливающий требования к продукции +

Б) Личный документ, подтверждающий квалификацию специалиста

В) Справочник по техническим условиям

Г) Документ, регулирующий внутренние процессы компании

2. Какова основная цель государственных стандартов?

А) Упрощение бухгалтерского учета

Б) Обеспечение единства измерений и качества продукции +

В) Увеличение прибыли компаний

Г) Ограничение доступа на рынок

3. Какой из следующих документов не является государственным стандартом?

А) ГОСТ Р 51522

Б) Технические условия (ТУ) +

В) ГОСТ Р ИСО 9001

Г) ГОСТ Р 51141

4. Кто разрабатывает и утверждает государственные стандарты в России?

А) Министерство финансов

Б) Федеральное агентство по техническому регулированию и метрологии (Росстандарт) +

В) Министерство юстиции

Г) Министерство образования

5. Какой принцип лежит в основе разработки государственных стандартов?

А) Конфиденциальность информации

Б) Открытость и доступность для всех заинтересованных сторон +

В) Защита интересов отдельных компаний

Г) Принцип частного регулирования

6. Какой из следующих аспектов не охватывается государственными стандартами?

А) Качество продукции

Б) Условия труда сотрудников +

В) Безопасность продукции

Г) Экологические требования

7. Что такое "нормативные ссылки" в контексте ГОСТов?

А) Ссылки на рекламные материалы

Б) Указания на другие стандарты или нормативные документы, которые необходимо учитывать +

В) Ссылки на личные мнения экспертов

Г) Ссылки на международные соглашения

8. Какой из следующих видов стандартов является обязательным для исполнения?

А) Рекомендательные стандарты

Б) Обязательные стандарты +

В) Информационные стандарты

Г) Методические рекомендации

9. Как часто пересматриваются государственные стандарты?

А) Каждые 5 лет
Б) По мере необходимости, но не реже чем каждые 5 лет +
В) Каждые 10 лет
Г) Никогда не пересматриваются

10. Какое значение имеет соблюдение государственных стандартов для бизнеса?
А) Увеличивает риски для компании
Б) Обеспечивает конкурентные преимущества и доверие потребителей +
В) Не имеет значения для бизнеса
Г) Увеличивает затраты на производство

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 Руководящий документ Гостехкоммиссии: Межсетевые экраны.

1. Что такое межсетевой экран?
А) Устройство для хранения данных
Б) Система, контролирующая входящий и исходящий трафик в сети+
В) Программа для обработки изображений
Г) Устройство для подключения к интернету

2. Какова основная функция межсетевого экрана?
А) Ускорение передачи данных
Б) Защита сети от несанкционированного доступа +
В) Оптимизация работы приложений
Г) Создание резервных копий данных

3. Какой тип межсетевого экрана обеспечивает фильтрацию на уровне приложений?
А) Пакетный фильтр
Б) Прокси-сервер +
В) Stateful firewall
Г) Настраиваемый фильтр

4. Какой из следующих протоколов чаще всего используется для управления межсетевыми экранами?
А) HTTP
Б) FTP

В) SNMP +
Г) SMTP

5. Какой из следующих типов межсетевых экранов работает на уровне сети?
А) Приложенческий межсетевой экран
Б) Пакетный фильтр +
В) Прокси-сервер
Г) Системы предотвращения вторжений (IPS)

6. Какой метод аутентификации часто используется в межсетевых экранах?
А) Анонимная аутентификация
Б) Двухфакторная аутентификация +
В) Одноразовые пароли
Г) Базовая аутентификация

7. Какой из следующих параметров не является критически важным для настройки межсетевого экрана?
А) Политики безопасности
Б) Настройки времени и даты +
В) Список разрешенных IP-адресов
Г) Журналирование событий

8. Что такое "политика безопасности" в контексте межсетевых экранов?
А) Набор правил, определяющих, какой трафик разрешен или запрещен +
Б) Документ, описывающий процесс установки оборудования
В) Список всех пользователей сети
Г) Инструкция по эксплуатации устройства

9. Какой из следующих методов защиты может использоваться совместно с межсетевыми экранами?
А) Антивирусное программное обеспечение +
Б) Оптимизация маршрутизации
В) Увеличение пропускной способности сети
Г) Установка дополнительных сетевых кабелей

10. Какой из следующих аспектов является важным при выборе межсетевого экрана для организации?
А) Цвет устройства
Б) Легкость в использовании и настройке +
В) Бренд производителя
Г) Наличие встроенного Wi-Fi

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 № 7

Тема 7 Основы сертификации (на примере средств защиты информации).

1. Что такое сертификация средств защиты информации?
   А) Процесс проверки соответствия средств защиты установленным требованиям +
   Б) Процесс установки программного обеспечения
   В) Процесс обучения пользователей
   Г) Процесс обновления оборудования

2. Какова основная цель сертификации средств защиты информации?
   А) Увеличение продаж
   Б) Обеспечение доверия к продукту и его безопасности +
   В) Упрощение работы с документацией
   Г) Снижение затрат на оборудование

3. Какой документ подтверждает успешную сертификацию средства защиты информации?
   А) Лицензия
   Б) Сертификат +
   В) Договор
   Г) Инструкция по эксплуатации

4. Кто обычно проводит сертификацию средств защиты информации?
   А) Производитель оборудования
   Б) Независимые аккредитованные организации +
   В) Конечные пользователи
   Г) Государственные органы без лицензии

5. Что такое аккредитация в контексте сертификации?
   А) Процесс получения лицензии на продажу продукта
   Б) Процесс признания компетентности организации, проводящей сертификацию +
   В) Процесс разработки новых стандартов
   Г) Процесс обучения сотрудников

6. Какой из следующих стандартов может быть использован для сертификации средств защиты информации?

А) ISO/IEC 27001 +
Б) ISO 9001
В) ISO 14001
Г) ISO 50001

7. Что включает в себя процесс сертификации?
А) Только тестирование продукта
Б) Анализ документации, тестирование и оценка соответствия +
В) Только собеседование с разработчиками
Г) Установку программного обеспечения на компьютеры пользователей

8. Какой из следующих факторов не влияет на выбор метода сертификации?
А) Тип и сложность средства защиты информации
Б) Бюджет организации на сертификацию
В) Местоположение офиса компании +
Г) Требования законодательства и регуляторов

9. Как часто необходимо проводить повторную сертификацию средств защиты информации?
А) Каждые 5 лет
Б) В зависимости от изменений в законодательстве и технологии +
В) Каждый год без исключений
Г) Никогда, если продукт уже сертифицирован

10. Какой из следующих аспектов является важным для успешной сертификации?
А) Наличие рекламного бюджета
Б) Соответствие требованиям стандартов и норм +
В) Популярность продукта на рынке
Г) Количество сотрудников в компании-разработчике

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 № 8

Тема 8 Сертификация на соответствие требованиям по безопасности информации

1. Что такое сертификация на соответствие требованиям по безопасности информации?
А) Процесс оценки и подтверждения соответствия системы защиты информации

установленным стандартам +

Б) Процесс установки антивирусного ПО

В) Процесс обучения сотрудников по безопасности

Г) Процесс разработки новых технологий защиты

2. Какой стандарт часто используется для сертификации систем управления информационной безопасностью?

А) ISO/IEC 9001

Б) ISO/IEC 27001 +

В) ISO 14001

Г) ISO 50001

3. Кто может проводить сертификацию на соответствие требованиям по безопасности информации?

А) Только производители программного обеспечения

Б) Независимые аккредитованные организации +

В) Конечные пользователи

Г) Любая компания без лицензии

4. Какой документ подтверждает успешное прохождение сертификации?

А) Лицензия

Б) Сертификат соответствия +

В) Договор

Г) Инструкция пользователя

5. Что такое аккредитация в контексте сертификации?

А) Процесс получения лицензии на продажу продукта

Б) Процесс признания компетентности организации, проводящей сертификацию +

В) Процесс разработки новых стандартов

Г) Процесс обучения сотрудников

6. Какой из следующих аспектов не является частью процесса сертификации?

А) Оценка документации

Б) Проведение тестирования системы

В) Обучение персонала +

Г) Оценка рисков безопасности

7. Как часто необходимо проводить повторную сертификацию?

А) Каждые 5 лет

Б) В зависимости от изменений в законодательстве и технологии +

В) Каждый год без исключений

Г) Никогда, если система уже сертифицирована

8. Какой из следующих факторов может повлиять на выбор метода сертификации?

А) Размер компании

Б) Сложность и тип защищаемой информации +

В) Местоположение офиса компании
Г) Количество сотрудников в компании

9. Что необходимо для подготовки к сертификации?
А) Разработка рекламной кампании
Б) Подготовка всей необходимой документации и проведение внутреннего аудита +
В) Установка нового оборудования
Г) Нанимание дополнительных сотрудников

10. Какой из следующих аспектов важен для поддержания сертификата соответствия?
А) Регулярное обновление программного обеспечения и соблюдение стандартов безопасности +
Б) Увеличение числа сотрудников в IT-отделе
В) Публикация отчетов о продажах
Г) Участие в выставках и конференциях

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 № 9

Тема 9 Системы сертификации средств защиты информации: требования безопасности информации.

1. Что такое система сертификации средств защиты информации?
А) Процесс разработки новых технологий защиты
Б) Оценка и подтверждение соответствия средств защиты информации установленным требованиям +
В) Установка антивирусного программного обеспечения
Г) Обучение сотрудников по вопросам безопасности

2. Какой стандарт часто используется для сертификации средств защиты информации в России?
А) ISO/IEC 27001
Б) ГОСТ Р 50922-96 +
В) ISO 9001
Г) ISO 14001

3. Кто проводит сертификацию средств защиты информации?

А) Только производители программного обеспечения

Б) Независимые аккредитованные органы +

В) Конечные пользователи

Г) Любая компания без лицензии

4. Какой документ подтверждает соответствие средств защиты информации требованиям безопасности?

А) Лицензия

Б) Сертификат соответствия +

В) Инструкция пользователя

Г) Договор на поставку

5. Что такое аккредитация в контексте сертификации?

А) Процесс получения лицензии на продажу продукта

Б) Признание компетентности организации, проводящей сертификацию +

В) Процесс разработки новых стандартов

Г) Обучение сотрудников по безопасности

6. Какой из следующих аспектов не является частью процесса сертификации средств защиты информации?

А) Оценка документации и испытания

Б) Проведение тестирования системы

В) Обучение персонала +

Г) Оценка рисков безопасности

7. Как часто необходимо проводить повторную сертификацию средств защиты информации?

А) Каждые 5 лет

Б) В зависимости от изменений в законодательстве и технологии +

В) Каждый год без исключений

Г) Никогда, если средство уже сертифицировано

8. Что является основным критерием для оценки средств защиты информации при сертификации?

А) Эстетические качества интерфейса

Б) Соответствие установленным требованиям безопасности +

В) Стоимость продукта

Г) Популярность на рынке

9. Какой из следующих документов может быть частью процесса сертификации?

А) Техническое задание на разработку

Б) Отчет о результатах испытаний +

В) Маркетинговый план

Г) Договор с клиентом

10. Какой аспект важен для поддержания сертификата соответствия средств защиты информации?

А) Регулярное обновление программного обеспечения и соблюдение стандартов безопасности +

Б) Увеличение числа сотрудников в компании

В) Публикация отчетов о продажах

Г) Участие в выставках и конференциях

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 означает термин "безопасность информации"?

А) Защита от вирусов

Б) Защита информации от несанкционированного доступа, повреждения и уничтожения +

В) Хранение информации в облаке

Г) Использование паролей для доступа

2. Какова основная цель сертификации средств защиты информации?

А) Увеличение продаж

Б) Подтверждение соответствия установленным требованиям безопасности +

В) Обучение пользователей

Г) Разработка новых технологий

3. Что такое межсетевой экран?

А) Устройство для защиты от вирусов

Б) Программное или аппаратное средство, контролирующее трафик между сетями +

В) Программное обеспечение для резервного копирования

Г) Устройство для увеличения скорости интернета

4. Какой документ определяет требования к межсетевым экранам в России?

А) ГОСТ Р 50922-96

Б) Федеральный закон о защите информации

В) Руководящий документ Гостехкомиссии +

Г) ISO/IEC 27001

5. Какой из следующих стандартов является международным стандартом по управлению безопасностью информации?

А) ГОСТ Р 50922-96

Б) ISO/IEC 27001 +

В) NIST SP 800-53

Г) ФЗ-152

6. Что такое аккредитация в контексте сертификации?

А) Процесс получения лицензии на продажу продукта

Б) Признание компетентности организации, проводящей

сертификацию +

В) Процесс разработки новых стандартов

Г) Обучение сотрудников по безопасности

7. Какой из следующих аспектов не является частью процесса сертификации?

А) Оценка документации и испытания

Б) Проведение тестирования системы

В) Обучение персонала+

Г) Оценка рисков безопасности

8. Каковы основные этапы процесса сертификации?

А) Подготовка, оценка, выдача сертификата, мониторинг +

Б) Разработка, продажа, поддержка

В) Исследование, обучение, внедрение

Г) Анализ, тестирование, маркетинг

9. Что такое государственные стандарты программных продуктов?

А) Нормативные документы, определяющие требования к разработке и эксплуатации ПО +

Б) Рекомендации по использованию ПО

В) Лицензии на продажу программного обеспечения

Г) Стандарты качества для производителей ПО

10. Какой стандарт определяет общие положения для сертификации средств защиты информации в России?

А) ГОСТ Р 50922-96 +

Б) ГОСТ Р ИСО/МЭК 27001-2012

В) ФЗ-152

Г) ГОСТ Р 57580-2017

11. Как часто необходимо проводить повторную сертификацию средств защиты информации?

А) Каждые 5 лет

Б) В зависимости от изменений в законодательстве и технологии +

В) Каждый год без исключений

Г) Никогда, если средство уже сертифицировано

12. Что такое стандарты безопасности в сети Интернет?

А) Правила использования интернета для пользователей

Б) Нормативные документы, определяющие требования к

безопасности сетевых технологий и данных +

В) Рекомендации по созданию веб-сайтов

Г) Лицензии на использование интернет-сервисов

13. Какой из следующих документов может быть частью процесса сертификации?

А) Техническое задание на разработку

Б) Отчет о результатах испытаний +

В) Маркетинговый план

Г) Договор с клиентом

14. Какова роль международных стандартов в сертификации средств защиты информации?

А) Они не имеют значения для национальных стандартов

Б) Они служат основой для разработки национальных стандартов и обеспечивают согласованность требований +

В) Они заменяют все национальные стандарты

Г) Они используются только для информационных технологий в Европе

15. Какой из следующих аспектов важен для поддержания сертификата соответствия средств защиты информации?

А) Регулярное обновление программного обеспечения и соблюдение стандартов безопасности +

Б) Увеличение числа сотрудников в компании

В) Публикация отчетов о продажах

Г) Участие в выставках и конференциях

16. Что такое риск в контексте безопасности информации?

А) Вероятность того, что произойдет инцидент с информацией и его последствия +

Б) Уровень защищенности системы от атак

В) Количество пользователей системы безопасности

Г) Стоимость средств защиты информации

17. Какие факторы влияют на уровень безопасности информации в организации?

А) Технические средства, политики безопасности, обучение персонала+

Б) Только технические средства

В) Только обучение персонала

Г) Только политики безопасности

18. Что такое оценка соответствия в контексте сертификации?

А) Процесс анализа финансовых показателей компании

Б) Процесс проверки выполнения установленным требованиям и стандартам безопасности +

В) Процесс разработки новых технологий защиты

Г) Процесс обучения сотрудников

19. Какой из следующих факторов не влияет на выбор средств защиты информации?

А) Уровень угрозы безопасности информации

Б) Бюджет организации

В) Эстетические предпочтения руководства +

Г) Соответствие требованиям законодательства

20. Что такое система управления безопасностью информации (СУБИ)?

А) Комплекс мер по защите информации в организации +

Б) Набор программных продуктов для защиты данных

В) Политика конфиденциальности

Г) Сертификат соответствия

Праильный ответ: а)

21. Какой из следующих стандартов описывает требования к управлению информационной безопасностью?

А) ISO/IEC 27001 +

Б) ISO 9001

В) ISO 14001

Г) ISO/IEC 20000

22. Что такое классификация информации?

А) Процесс определения ценности информации для организации и ее уровня защиты +

Б) Процесс создания резервных копий данных

В) Процесс обучения сотрудников по вопросам безопасности

Г) Процесс разработки новых программных продуктов

23. Какой из следующих аспектов важен при разработке политики безопасности в организации?

А) Учет специфики деятельности и возможных угроз +

Б) Ориентация только на технические средства защиты
В) Игнорирование мнения сотрудников
Г) Установка жестких правил без объяснения их необходимости

24. Соотнесите термины и определения

Термины	Определения
1) Сертификация	А) Процесс, в ходе которого проверяется соответствие системы установленным требованиям безопасности.
2) Аккредитация	Б) Набор мер и процедур, направленных на защиту информации в организации.
3) Межсетевой экран	В) Процесс получения признания компетентности организации, проводящей сертификацию.
4) Оценка соответствия	Г) Программное или аппаратное средство, контролирующее трафик между сетями.
5) Управление безопасностью информации (УБИ)	Д) Вероятность возникновения инцидента с информацией и его последствия.
6) Риск	Е) Нормативный документ, определяющий требования к управлению безопасностью информации.
7) Стандарт ISO/IEC 27001	Ж) Процесс определения ценности информации для организации и ее уровня защиты
8) Классификация информации	З) Официальное подтверждение, что продукт или услуга соответствуют установленным стандартам.

Ответы:А-4,Б-5,В-2,Г-3,Д-6;Е-7;Ж-8;З-1

25. Государственный стандарт (ГОСТ) — это документ, который устанавливает _____ к продукции, процессам или услугам.

Ответ : требования

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 №____