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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ОСНОВЫ 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 «Основы 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 «Основы информационной безопасности» и установление уровня сформированности компетенций обучающегося.

ОМ предназначен для проведения текущего контроля успеваемости и промежуточной аттестации.

ОМ включает оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации.

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины «Основы информационной безопасности».

1. Паспорт оценочных материалов по дисциплине «Основы информационной безопасности»

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-1.1. Демонстрирует умение оценивать роль информации и информационных техно- логий при решении задачи профессиональной деятельности	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности Владеет видами защищаемой информации, классификациями, навыками оценивания угроз информационной безопасности	Тема 1. Защита информации как объективная закономерность эволюции постиндустриального общества. Тема 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Тема 3. Угрозы информационной безопасности в компьютерных системах Тема 4. Общая характеристика средств и методов защиты информации	Рефераты (Темы 1-4) Тесты (тема 1-4)	Тест (1-17 тестового задания)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства[1]	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
	ОПК-1.2. Демонстрирует умение оценивать роль информационной безопасности при решении задачи профессиональной деятельности	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности Владеет	Тема 4. Общая характеристика средств и методов защиты информации Тема 5. Организационно- правовое обеспечение защиты информации. Тема 6. Защита компьютерных систем от несанкционированного вмешательства. Тема 7. Криптографические методы защиты информации Тема 8. Комплексная защита информации в компьютерных системах.	Рефераты (Темы 4-8) Тесты (Тема 4-8 Лабораторные работы (Тема 1-4)	Тест (18-40 тестового задания)

2. Оценочные материалы по дисциплине «Основы информационной безопасности»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема1. Защита информации как объективная закономерность эволюции постиндустриального общества.

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.

Тема 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.

1. Соотношение понятий «информационная безопасность» и «национальная безопасность»
2. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
3. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
4. Система обеспечения информационной безопасности. Обеспечение информационной безопасности Российской Федерации.
5. Понятие информационной войны. Проблемы информационной войны.

Тема 3. Угрозы информационной безопасности в компьютерных системах.

1. Информационное оружие и его классификация.
2. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
3. Уровни ведения информационной войны. Информационные операции. Психологические операции. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
4. Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по

реализации государственной политики обеспечения информационной безопасности.

5. Классификация баз данных.

Тема 4. Общая характеристика средств и методов защиты информации

1. Виды защищаемой информации в сфере государственного и муниципального управления.

2. Обеспечение информационной безопасности организации.

3. Управление и защита информации в информационно-телекоммуникационных сетях.

4. Характеристика эффективных стандартов по безопасности. Требования к полноте эффективных стандартов по безопасности.

5. Фактографические и документальные базы данных.

Тема 5. Организационно- правовое обеспечение защиты информации.

1. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.

2. Стандарты предприятия по использованию персональных компьютеров. Практические меры безопасности для персональных компьютеров.

3. Уровень доступа к данным. Уровень информационного доступа

4. Базы данных оперативной и ретроспективной информации.

5. Уровень администрирования

Тема 6. Защита компьютерных систем от несанкционированного вмешательства.

1. Виды и характеристика Информационных ресурсов.

2. Защита информации от утечки.

3. Каналы утечки информации

4. Виды правонарушений в сети Internet.

5. Задачи методы обеспечения информационной безопасности

Тема 7. Криптографические методы защиты информации.

1. Условия для реализации угроз безопасности информации

2. Поиск и использовании уязвимостей информации

3. Классификацию угроз информационной безопасности

4. Конфиденциальность и целостность информации

Тема 8. Комплексная защита информации в компьютерных системах.

1. Нарушения целостности информации

2. Виды отказов информационной системы

3. Автоматизированная информационная система

4. Методы и средства, направленные на противодействие комплексу угроз

5. Модели доступа к данным

6. Политика безопасности информационной системы

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, предъявляемые к 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.

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 лабораторных работ

Тема 1. Защита информации как объективная закономерность эволюции постиндустриального общества.

Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана.

Формы отчетности, основная и дополнительная литература.

Информация и ее роль в современном обществе.

Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации.

Глобализация информационных отношений.

Информационные технологии. Информационные ресурсы.

Объективная необходимость и общественная потребность в защите информации. Сущность защиты информации.

Правовое регулирование вопросов защиты информации.

Вопросы для самоконтроля:

1. Что включают в себя предмет, содержание и задачи курса?
2. Что такое Информация и ее роль в современном обществе?
3. Что такое информационные технологии и информационные ресурсы услуги?
4. В чем заключается сущность правового регулирования вопросов защиты информации?

Цель работы – получение теоретических навыков работы с информационными технологиями.

В работе используется презентация слайдов выполненная в MS Powerpoint

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Тема 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.

Право на информацию в системе гражданских прав личности. Возможные ограничения.

Массовая информация и информация ограниченного доступа.

Неприкосновенность частной жизни, персональные данные.

Виды тайн. Коммерческая тайна. Государственная тайна.

Документированная информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности РФ.

Информационные войны, информационное оружие. Доктрина информационной безопасности РФ.

Вопросы для самоконтроля:

1. Что такое массовая информация и информация ограниченного доступа?
2. Неприкосновенность частной жизни, персональные данные?
3. Какие существуют виды тайн. Коммерческая тайна. Государственная тайна

4. Что такое документированная информация как объект права собственности?

5. Что такое информационные войны, информационное оружие и Доктрина информационной безопасности РФ?

Цель работы – формирование информационная безопасность личности, общества и государства.

В работе используется презентация слайдов выполненная в MS Powerpoint.

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Тема 3. Угрозы информационной безопасности в компьютерных системах.

Компьютерная система (КС) как объект защиты информации.

Понятие угрозы информационной безопасности в КС.

Классификация и общий анализ угроз информационной безопасности в КС.

Общие сведения о компьютерных вирусах.

Темы для индивидуальной лабораторной работы:

1. Преднамеренные угрозы информационной безопасности.
2. Случайные угрозы информационной безопасности.
3. Виды сбоев и отказов.
4. Общие сведения о кодах для обнаружения и исправления случайных ошибок.
5. Система охраны объектов КС.
6. Основные виды технических каналов утечки информации.

7. Техника промышленного шпионажа.
8. Классификация компьютерных вирусов.
9. Механизмы заражения компьютерными вирусами.

Цель работы − формирование практических навыков по преодолению угроз информационной безопасности в компьютерных системах.

В работе используется база данных выполненная в MS Access/

Критерии оценивания выполнения лабораторной работы:

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. Общая характеристика средств и методов защиты информации

Эволюция концепции информационной безопасности в компьютерных системах.

Реализация угроз информационной безопасности путём несанкционированного доступа.

Модель поведения потенциального нарушителя.

Обобщённые модели систем защиты информации.

Основные принципы обеспечения информационной безопасности в КС. Понятие комплексной системы защиты информации (КСЗИ).

Вопросы для самоконтроля:

1. В чем заключается реализация угроз информационной безопасности путём несанкционированного доступа?
2. Какова модель поведения потенциального нарушителя?
3. Обобщённые модели систем защиты информации.
4. Основные принципы обеспечения информационной безопасности в КС..

Цель работы− формирование теоретических навыков по изучению и характеристике средств и методов защиты информации.

В работе используется презентация слайдов выполненная в MS Powerpoint.

Критерии оценивания выполнения практического задания:

Оценка «отлично» выставляется, если: работа выполнена в полном объеме с соблюдением необходимой последовательности действий; работа проведена в условиях, обеспечивающих получение правильных результатов и выводов; соблюдены правила техники безопасности; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

Оценка «хорошо» выставляется, если: работа выполнена правильно с учетом 1-2 мелких погрешностей или 2-3 недочетов, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» выставляется, если: работа выполнена правильно не менее чем наполовину, допущены 1-2 погрешности или одна грубая ошибка.

Оценка «неудовлетворительно» выставляется, если: допущены две (и более) грубые ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя или работа не выполнена полностью.

Типовые тесты

Тест №1

Тема 1. Защита информации как объективная закономерность эволюции постиндустриального общества.

1. Информационная система – это …

a) набор программных и технических средств;

b) упорядоченную совокупность документов, информационных технологий и программно - аппаратных средств, реализующих информационные процессы;

c) упорядоченная совокупность документов, относящихся к определенной области;

d) набор программных средств, относящихся к одной задаче.

2. Информационными ресурсами называют:

a) документы (массивы документов), существующие в составе информационных систем;

b) документы (массивы документов), существующие отдельно или в составе информационных систем;

c) документы (массивы документов), существующие отдельно от информационных систем;

d) все определения не верны.

3. Информацию по степени доступа разделяют на:

a) открытую и ограниченного доступа;

b) открытую;

c) закрытую;

d) тайную и ограниченную.

4. 1. Выберите наиболее подходящее определение информации:

a) сведения о лицах, предметах;

b) сведения о лицах, предметах, фактах, событиях;

c) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

d) сведения о лицах независимо от формы их представления.

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. Информационная безопасность личности, общества и государства: социально-правовые аспекты..

5. К информации ограниченного доступа относятся:

a) государственная тайна;

b) конфиденциальная информация;

c) персональные данные;

d) все ответы верны.

6. Собственник информационных ресурсов, систем и технологий – это:

a) субъект с полномочиями владения указанными объектами;

b) субъект с полномочиями владения и пользования указанными объектами;

c) субъект с полномочиями владения, пользования и распоряжения указанными объектами;

d) Все ответы верны.

7. Информационная безопасность являются переводом на русский язык английского термина:

a) information security;

b) information system;

c) information currency;

d) information crypto.

8. Защитой информации называют:

a) деятельность по предотвращению утечки любой информации;

b) деятельность по предотвращению утечки защищаемой информации;

c) деятельность по предотвращению утечки доступной информации;

d) все ответы верны.

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. Угрозы информационной безопасности в компьютерных системах.

9. Под утечкой понимают:

a) неконтролируемое распространение защищаемой информации путём её разглашения или несанкционированного доступа к ней;

b) неконтролируемое распространение скрытой информации путём её разглашения или несанкционированного доступа к ней;

c) неконтролируемое распространение конфиденциальной информации путём её разглашения или несанкционированного доступа к ней;

d) все верно.

10. Под непреднамеренным воздействием на защищаемую информацию понимают:

a) воздействие на неё из-за ошибок пользователя, сбоя технических или программных средств, иных нецеленаправленных действий;

b) воздействие на неё из-за ошибок пользователя, сбоя технических средств;

c) воздействие на неё из-за ошибок пользователя, программных средств, иных нецеленаправленных действий;

d) все ответы верны.

11. Что не является характеристикой информации:

a) статичность;

b) тип доступа;

c) время отклика;

d) стоимость создания.

12. Способность информации изменяться в процессе использования – это:

a) статичность;

b) тип доступа;

c) время жизни;

d) стоимость создания.

13. Промежуток времени, пока информация актуальна – это:

a) статичность;

b) тип доступа;

c) время жизни;
d) стоимость создания

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 Общая характеристика средств и методов защиты информации

14. По оценке экспертов самым привлекательным сектором российской экономики для преступников является:

a) финансовая система;
b) кредитно-финансовая система;
c) кредитная система;
d) нет верного ответа.

15. Какая стоимость будет наиболее велика для пластиковой карты?

a) стоимость создания;
b) стоимость потери конфиденциальности;
c) стоимость скрытого нарушения целостности;
d) стоимость утраты.

16. К наиболее распространённым правонарушениям в сети Internet не относится:

a) мошенническая деятельность;
b) перлюстрация частной переписки;
c) нарушение авторских и смежных прав;
d) нелегальное получение товаров и услуг.

17. Что не относится к задачам информационной безопасности:

a) целостность и секретность;
b) электронная подпись и датирование;
c) устойчивость связи и определение трафика;
d) неотказуемость и анонимность.

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. Организационно- правовое обеспечение защиты информации.

18. К методам обеспечения информационной безопасности не относятся:

a) корпоративные;
b) административные;
c) правовые;
d) технические.

19. Какие методы не относятся к обеспечению информационной безопасности:

a) принуждение и побуждение;
b) управление доступом и регламентация;
c) маскировка и препятствие;
d) скрытый доступ и копирование сообщений.

20. Методы защиты информации можно разбить:

a) на три большие группы;
b) на две большие группы;
c) на четыре большие группы;
d) на пять больших групп.

21. Методы, не имеющие математического обоснования стойкости, часто называют методами:

a) С чёрным ящиком;
b) С белым квадратом;
c) С желтым кругом;
d) Нет верного ответа.

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. Защита компьютерных систем от несанкционированного вмешательства.

22. Методы, функционирующие по принципу "черного ящика", называют
a) Security Through Obscurity;
b) System Through Obscurity;
c) Security Through;
d) System Obscurity.

23. Метод физического преграждения пути злоумышленнику к информации:
a) управление доступом;
b) маскировка;
c) принуждение;
d) побуждение.

24. Метод защиты информации путем ее криптографического преобразования:
a) Принуждение;
b) Побуждение;
c) Маскировка;
d) управление доступом.

25. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам:
a) Уполномочивание;
b) Контроль доступа;
c) Сертификация;
d) Нет верного ответа.

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. Криптографические методы защиты информации.

26. Известность содержания информации только имеющим соответствующие полномочия субъектам – это:
a) Целостность;
b) Статичность;
c) Конфиденциальность;
d) Аутентификация.

27. Возможность получения информации или информационной услуги за приемлемое время – это:

конфиденциальность;

a) целостность;

b) доступность;

c) статичность;

28. Основными характеристиками защищаемой информации являются:

a) конфиденциальность, целостность и статичность;

b) конфиденциальность, целостность и доступность;

c) аутентификация, целостность и доступность;

d) аутентификация, статичность и время создания.

29. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:

a) уязвимость;

b) атака;

c) угроза;

d) нет верного ответа.

30. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого её состояния, при котором создаются условия для реализации угроз безопасности информации - это:

a) атака;

b) угроза;

c) уязвимость;

d) статичность.

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. Комплексная защита информации в компьютерных системах.

31. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:

a) статичность;

b) атака;

c) угроза;

d) изъян.
32. Классификацию угроз ИБ можно выполнить по нескольким критериям:
a) по аспекту информационной безопасности;
b) по компонентам информационной системы;
c) по способу осуществления;
d) все ответы верны.
33. Конфиденциальная информация может быть разделена на:
a) предметную и служебную;
b) служебную и закрытую;
c) предметную и открытую;
d) открытую и закрытую.
34. Целостность информации может быть разделена на:
a) статическую и динамическую;
b) статическую и служебную;
c) служебную и динамическую;
d) все верно.
35. Примером нарушения статической целостности не является:
a) ввод неверных данных;
b) несанкционированное изменение данных;
c) изменение программного модуля вирусом;
d) внесение дополнительных пакетов в сетевой трафик.
36. Примером нарушения динамической целостности не является:
a) нарушение атомарности транзакций;
b) внесение дополнительных пакетов в сетевой трафик;
c) несанкционированное изменение данных;
d) дублирование данных.
37. Угроза отказа служб может быть разбита на следующие типы:
a) отказ пользователей;
b) внутренний отказ информационной системы;
c) отказ поддерживающей инфраструктуры;
d) все ответы верны.
38. Что не относится к внутреннему отказу ИС:
a) ошибки при переконфигурировании системы;
b) отказы программного и аппаратного обеспечения;
c) разрушение данных;
d) нарушение работы систем связи.
39. Что не относится к отказу служб:
a) нарушение работы систем связи;
b) разрушение и повреждение помещений;
c) нарушение работы электропитания;
d) разрушение данных.
40. Нарушители" классифицируются по одному из следующих критериев:
a) уровень профессиональной подготовки противника;
b) тип доступа противника к системе;
c) способы атаки;

d) все ответы верны.

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 (в форме контрольной работы)

Часть 1:

Тема 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.

Вариант 1.

Задание 1. Виды тайн. Коммерческая тайна. Государственная тайна.

Задание 2. Управление доступом по схеме однократного входа.

1. Что такое база информация?

Варианты:

a) сведения о лицах, предметах;

b) сведения о лицах, предметах, фактах, событиях;

c) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

d) сведения о лицах независимо от формы их представления.

Обоснование информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Вариант 2.

Задание 1. Пароли. Строгая аутентификация.

Задание 2. Информационные войны, информационное оружие.

2. Что называют информационной системой?

Варианты:

a) набор программных и технических средств;

b) упорядоченную совокупность документов, информационных технологий и программно - аппаратных средств, реализующих информационные процессы;

c) упорядоченная совокупность документов, относящихся к определенной области;

d) набор программных средств, относящихся к одной задаче.

Обоснование: информационная система — упорядоченная совокупность документов, информационных технологий и программно - аппаратных средств, реализующих информационные процессы.

Вариант 3.

Задание 1. Неприкосновенность частной жизни, персональные данные..

Задание 2. Защита электронного документооборота.

3. Что называют информационными ресурсами?

Варианты:

a) документы (массивы документов), существующие в составе информационных систем;

b) документы (массивы документов), существующие отдельно или в составе информационных систем;

c) документы (массивы документов), существующие отдельно от информационных систем;

d) все определения не верны.

Обоснование: информационные ресурсы — документы (массивы документов), существующие в составе информационных систем.

Тема 3. Угрозы информационной безопасности в компьютерных системах.

Вариант 1.

Задание 1. Компьютерная система (КС) как объект защиты информации.

Задание 2. Защита беспроводных сетей.

4. Что такое информация ограниченного доступа?

Варианты:

a) государственная тайна;

b) конфиденциальная информация;

c) персональные данные;

d) все ответы верны.

Обоснование: информация ограниченного доступа — сведения, связанные с военной, экономической, внешнеполитической, разведывательной деятельностью.

Вариант 2.

Задание 1. Классификация и общий анализ угроз информационной безопасности в КС.

Задание 2. Безопасность в открытых сетях.

5. Какой тип связи между таблицами описывает ситуацию: «Один клиент может сделать много заказов, но каждый заказ принадлежит только одному клиенту»?

Варианты:

A) Один к одному (1:1)

B) Один ко многим (1:N)

C) Многие ко многим (M:N)

D) Нет связи

Обоснование: Связь «один ко многим» — наиболее распространённый тип. Один клиент → много заказов. Обратная связь — «многие к одному».

Вариант 3.

Задание 1. Обеспечение безопасности ОС UNIX и Windows.

Задание 2. Случайные угрозы информационной безопасности.

6. Выберите правильный перевод на русский язык английского термина Информационная безопасность:

Варианты:

a) information security;

b) information system;

c) information currency;

d) information crypto.

Обоснование: Информационная безопасность — это «information security».

Вариант 4.

Задание 1. Защита на канальном уровне – протоколы PPTP

Задание 2. . Преднамеренные угрозы информационной безопасности.

7. Что определяется как «Защита информации»?

Варианты:

a) деятельность по предотвращению утечки любой информации;

b) деятельность по предотвращению утечки защищаемой информации;

c) деятельность по предотвращению утечки доступной информации;

d) все ответы верны.

Обоснование: Защита информации - это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Тема 4. Общая характеристика средств и методов защиты информации

Вариант 1.

Задание 1. Эволюция концепции информационной безопасности в компьютерных системах.

Задание 2. Обнаружение и предотвращение вторжений. Система IPS.

8. Процесс подтверждения подлинности пользователя – это:

Варианты:

a) Идентификация;

b) Аутентификация;

c) Методология;

d) Интеграция;

Обоснование: Аутентификация — процесс проверки подлинности пользователя или системы.

Вариант 2.

Задание 1. Организация защищенного удаленного доступа.

Задание 2. Классификация вредоносных программ.

9. Какого шифра не существует:

Варианты:

a) Шифр Цезаря;
b) Шифр Кардано;
c) Шифр Трисемуса;
d) Шифр Хартли;

Обоснование: Шифра Хартли не существует.

Вариант 3.

Задание 1. Реализация угроз информационной безопасности путём несанкционированного доступа.

Задание 2. Основы работы антивирусных программ.

10. В современных шифрах применяется принцип:

Варианты:

a) Керкхоффса;
b) Хофмана;
c) Шенона;
d) Эль гаммеля;

Обоснование: В современных шифрах применяется принцип Керкхоффса.

Вариант 4.

Задание 1. Основные принципы обеспечения информационной безопасности в КС.

Задание 2. Защита ИС от вирусов и вредоносных программ.

11. Когда вышел стандарт ISO в области информационной безопасности:

Варианты:

a. 1998;
b. 1999;
c. 1997;
d. 2000;

Обоснование: стандарт ISO в области информационной безопасности вышел в 2000 г.

Тема 5. Организационно - правовое обеспечение защиты информации.

Вариант 1.

Задание 1. Защита на сетевом уровне – протокол IPSec.

Задание 2. Общие сведения о кодах для обнаружения и исправления случайных ошибок.

12. Когда появились первые антивирусные утилиты?

Варианты:

a) 1980;
b) 1982;
c) 1984;
d) 1986;

Обоснование: 1984.

Вариант 2.

Задание 1. Система охраны объектов КС.

Задание 2. Классификация компьютерных вирусов.

13. По особенностям реализуемого алгоритма вирусы делятся на:

Варианты:

a) Спутники, стелсы, паразиты, призраки;
b) стелсы, спутники, призраки, черви;
c) паразиты, призраки, черви, стелсы;
d) нет верного ответа;

Обоснование: вирусы делятся на — Спутники, стелсы, паразиты, призраки.

Тема 6. Защита компьютерных систем от несанкционированного вмешательства.

Вариант 1.

Задание 1. . Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам.

Задание 2. Защита программных средств от несанкционированного копирования и исследования.

14. Наиболее эффективное средство для защиты от сетевых атак:

Варианты:

a) использование сетевых экранов или «firewall»
b. использование антивирусных программ
c. посещение только «надёжных» Интернет-узлов
d. использование только сертифицированных программ-броузеров при доступе к сети Интернет

Обоснование: использование сетевых экранов или «firewall»

Вариант 2.

Задание 1. . Защита от несанкционированного изменения структуры КС в процессе эксплуатации.

Задание 2. Контроль целостности программ и данных в процессе эксплуатации.

15. Под угрозой удаленного администрирования в компьютерной сети понимается угроза:

Варианты:

b) несанкционированного управления удаленным компьютером;

c) внедрения агрессивного программного кода в рамках активных объектов Web-страниц;

d) перехвата или подмены данных на путях транспортировки;

e) вмешательства в личную жизнь;

Обоснование: несанкционированного управления удаленным компьютером

Методические требования выполнения индивидуальных заданий:

В каждом варианте индивидуальных заданий представлено по четыре наименования вопросов. При выполнении индивидуального задания обучающийся, должен привести полную характеристику каждого из представленных вопросов, в их практическом применении в конкретных организациях. Работа оформляется в печатном варианте.

Критерии оценки:

Оценка «отлично»: обучающийся продемонстрировал глубокое исчерпывающее понимание содержания представленной информации, правильное понимание сущности и взаимосвязи исследуемых процессов и явлений. По результатам исследования правильно, развернуто, содержательно сформулированы выводы. Структура, содержание и оформление отчета полностью соответствуют установленным требованиям. Основная часть изложена логично, последовательно. В процессе защиты даны правильные исчерпывающие ответы на все вопросы.

Оценка «хорошо»: обучающийся продемонстрировал достаточно полное понимание содержания информации, правильное понимание сущности и взаимосвязи исследуемых процессов и явлений при несущественных неточностях по отдельным аспектам. Основная часть изложена логично, последовательно. Выводы верно сформулированы. В процессе защиты даны правильные ответы на все вопросы при несущественных неточностях по отдельным аспектам.

Оценка «удовлетворительно»: обучающийся продемонстрировал понимание основного содержания информации. Структура, содержание и оформление отчета в целом соответствуют установленным требованиям. Основная часть изложена логично, последовательно. Выводы сформулированы без грубых ошибок и неточностей. В процессе защиты в целом даны правильные ответы на большинство заданных вопросов.

Оценка «неудовлетворительно» – обучающимся не выполнены условия для выставления оценки «удовлетворительно».

Часть 2: Вопросы с выбором нескольких верных ответов (5 шт.)
16. Какие из перечисленных являются реляционными СУБД?
Варианты:
A) MySQL
B) MongoDB
C) PostgreSQL
D) Redis
E) Oracle Database
Обоснование:
MySQL, PostgreSQL и Oracle — классические реляционные СУБД, поддерживающие SQL и табличную структуру. MongoDB — документоориентированная NoSQL, Redis — in-memory key-value хранилище.

17. Какие из перечисленных операторов SQL относятся к языку манипулирования данными (DML)?
Варианты:
A) CREATE
B) SELECT
C) INSERT
D) DROP
E) UPDATE
Обоснование:
DML (Data Manipulation Language) — операторы для работы с данными: SELECT, INSERT, UPDATE, DELETE.
DDL (Data Definition Language) — CREATE, ALTER, DROP — для структуры.

18. Какие из перечисленных ограничений (constraints) могут быть применены к столбцам таблицы?
Варианты:
A) PRIMARY KEY
B) FOREIGN KEY
C) UNIQUE
D) NOT NULL
E) MAX VALUE
Обоснование:
Эти ограничения используются для обеспечения целостности данных:

PRIMARY KEY — уникальность + NOT NULL
FOREIGN KEY — ссылочная целостность
UNIQUE — уникальность значений
NOT NULL — обязательное заполнение
«MAX VALUE» — не является стандартным ограничением SQL (можно реализовать через CHECK, но не отдельный constraint).
19. Какие из перечисленных действий могут повысить производительность

запросов к базе данных?
Варианты:
A) Создание индексов по часто используемым полям
B) Нормализация базы до 5NF
C) Использование оператора SELECT * вместо перечисления полей
D) Разделение больших таблиц (денормализация при необходимости)
E) Оптимизация структуры запросов и использование JOIN вместо вложенных SELECT
Обоснование:
Индексы ускоряют поиск. Денормализация иногда улучшает производительность за счёт избыточности (в аналитических БД). Оптимизация запросов критически важна.
Нормализация до 5NF может ухудшить производительность из-за множества JOIN. SELECT * — неэффективно, если нужны не все поля.

20. Какие из перечисленных свойств характерны для реляционной модели данных?
Варианты:
A) Данные организованы в виде таблиц
B) Поддержка ссылочной целостности
C) Использование иерархической структуры (дерево)
D) Наличие первичных и внешних ключей
E) Хранение данных в формате JSON по умолчанию
Обоснование:
Реляционная модель основана на таблицах, ключах и связях. Иерархическая структура — для иерархических БД (например, древние IMS). JSON — типично для документоориентированных NoSQL-баз.

Часть 3: Вопросы на установление соответствия (5 шт.)
21. Установите соответствие между SQL-оператором и его назначением:
1. SELECT
A. Изменение существующих записей
2. INSERT
B. Удаление записей
3. UPDATE
C. Добавление новых записей
4. DELETE
D. Выборка данных из таблицы
Обоснование:
Это основные DML-операторы SQL: SELECT — чтение, INSERT — вставка, UPDATE — обновление, DELETE — удаление.

22. Установите соответствие между типом ключа и его описанием:
1. Первичный
A. Ссылается на первичный ключ другой таблицы

2. Внешний
B. Уникально идентифицирует запись в таблице
3. Составной
C. Первичный ключ, состоящий из нескольких полей
4. Кандидатский
D. Поле, которое может быть первичным ключом
Обоснование:
Первичный — основной уникальный идентификатор. Внешний — обеспечивает связь между таблицами. Составной — из нескольких столбцов. Кандидатский — любой уникальный NOT NULL столбец, подходящий на роль первичного.

23. Установите соответствие между уровнем архитектуры БД и его описанием:
1. Внешний
A. Физическое хранение данных на диске
2. Концептуальный
B. Представление данных для конкретного пользователя или приложения
3. Внутренний
C. Общая логическая структура всей базы данных
Обоснование:
Архитектура ANSI/SPARC:

Внешний — view для пользователя/приложения
Концептуальный — логическая модель (ER-диаграмма, таблицы, связи)
Внутренний — как данные хранятся физически (индексы, файлы, страницы)
24. Установите соответствие между нормальной формой и её требованием:
1. 1НФ
A. Отсутствие транзитивных зависимостей
2. 2НФ
B. Все поля атомарны, нет повторяющихся групп
3. 3НФ
C. Нет частичных зависимостей неключевых атрибутов от составного ключа
Обоснование:

1НФ: атомарность значений, уникальность строк
2НФ: при составном ключе — все неключевые атрибуты зависят от всего ключа
3НФ: неключевые атрибуты зависят только от ключа, а не от других неключевых атрибутов (нет транзитивных зависимостей)

25. Установите соответствие между типом связи и примером:
1. Один к одному
A. Студент — Зачётная книжка
2. Один ко многим
B. Автор — Книги

3. Многие ко многим
C. Студенты — Курсы (через таблицу-посредник)
Обоснование:
1:1: одна запись в одной таблице соответствует только одной в другой (зачётка принадлежит одному студенту)
1:N: один автор — много книг
M:N: студент может учиться на многих курсах, курс могут посещать многие студенты → требует промежуточной таблицы

Тест 1. Установите правильную последовательность этапов проектирования реляционной базы данных. Элементы:
A. Физическое проектирование (выбор СУБД, индексы, оптимизация)
B. Концептуальное проектирование (ER-диаграмма)
C. Сбор и анализ требований
D. Логическое проектирование (нормализация, создание таблиц, ключей)
Обоснование:
Проектирование базы данных начинается со сбора требований (что нужно бизнесу), затем создаётся концептуальная модель (ER-диаграмма), после чего — логическая (таблицы, нормализация), и завершается физическим проектированием под конкретную СУБД.

Тест 2. Установите последовательность выполнения операций в SQL-транзакции для корректного перевода средств между счетами:
Элементы:
A. Фиксация транзакции (COMMIT)
B. Начало транзакции (BEGIN TRANSACTION)
C. Списание средств с первого счёта (UPDATE счет1 SET баланс = баланс - 100)
D. Зачисление средств на второй счёт (UPDATE счет2 SET баланс = баланс + 100)
Обоснование:
Транзакция должна начинаться с BEGIN, затем выполняются операции (сначала списание, потом зачисление — чтобы избежать временного "исчезновения" денег), и только после успешного выполнения — COMMIT. Если ошибка — ROLLBACK.

Тест 3. Установите последовательность нормальных форм от наименее до наиболее строгой:
Элементы:
A. Третья нормальная форма (3NF)
B. Вторая нормальная форма (2NF)
C. Первая нормальная форма (1NF)
D. Нормальная форма Бойса-Кодда (BCNF)
Обоснование:
Нормальные формы последовательно устраняют зависимости:

1NF — атомарность и отсутствие повторяющихся групп
2NF — устранение частичных зависимостей
3NF — устранение транзитивных зависимостей
BCNF — усиленная 3NF, где каждый детерминант — кандидатский ключ

Тест 4. Установите последовательность выполнения частей SQL-запроса SELECT (логический порядок обработки):
Элементы:
A. SELECT (выбор столбцов)
B. FROM (указание таблиц)
C. WHERE (фильтрация строк)
D. GROUP BY (группировка)
E. HAVING (фильтрация групп)
F. ORDER BY (сортировка)
Обоснование:
Хотя синтаксис SQL пишется как SELECT ... FROM ... WHERE ..., логически СУБД сначала определяет источник данных (FROM), затем фильтрует строки (WHERE), группирует (GROUP BY), фильтрует группы (HAVING), выбирает столбцы (SELECT) и сортирует (ORDER BY).
Это важно для понимания, почему, например, в WHERE нельзя использовать алиасы из SELECT, а в HAVING — можно.

Тест 5. Установите последовательность действий при создании реляционной базы данных «Интернет-магазин»:
Элементы:
A. Создание таблиц: «Клиенты», «Товары», «Заказы», «Состав заказа»
B. Определение связей: Клиент → Заказы (1:N), Заказы → Состав заказа (1:N), Товары → Состав заказа (1:N)
C. Анализ предметной области: какие сущности, атрибуты, связи нужны
D. Назначение первичных и внешних ключей
E. Нормализация структуры таблиц
Обоснование:
Сначала анализируется предметная область, затем моделируются связи (часто через ER-диаграмму), после чего создаются таблицы, определяются ключи, и проводится нормализация для устранения избыточности и обеспечения целостности.

Часть 2: Задание открытого типа с развёрнутым ответом
1. Прочитайте текст и напишите развёрнутый обоснованный ответ:
В компании «Алгоритм» используется база данных для учёта товаров и поставок. Аналитик заметил, что в таблице «Товары» хранятся не только данные о товаре (название, цена, категория), но и данные о поставщике (название поставщика, телефон, адрес) и данные о последней поставке (дата, количество). При этом один и тот же поставщик может поставлять много товаров, а один товар всегда поставляется одним поставщиком.

Вопрос: Какие проблемы могут возникнуть при такой структуре? Как следует перепроектировать базу данных? Обоснуйте с точки зрения нормализации, целостности данных и производительности.
Развёрнутый обоснованный ответ:

2. Рекомендуемая структура (нормализация):
Необходимо разделить данные на три таблицы:
Таблица «Поставщики»
Поля: id_поставщика (PK), название, телефон, адрес
Таблица «Товары»
Поля: id_товара (PK), название, цена, категория, id_поставщика (FK → Поставщики)
Таблица «Поставки»
Поля: id_поставки (PK), id_товара (FK), дата, количество
Связи:
Поставщик → Товары (1:N)
Товар → Поставки (1:N)

3. Преимущества новой структуры:
Соблюдение нормальных форм:
Все таблицы находятся минимум в 3НФ — отсутствуют избыточность и транзитивные зависимости.
Целостность данных:
Внешние ключи обеспечивают ссылочную целостность: нельзя добавить товар с несуществующим поставщиком, нельзя удалить поставщика, если есть связанные товары (без каскадного удаления).
Гибкость и масштабируемость:
Можно добавлять поставщиков независимо от товаров, вести историю множества поставок по каждому товару.
Производительность и удобство:
Поиск поставщика по ID быстрее, чем по текстовому полю. Индексы на внешние ключи ускоряют JOIN-запросы. Обновление данных поставщика — в одной строке.
Упрощение отчётов:
Легко получить отчёт «все товары поставщика», «история поставок по товару», «поставщики без товаров» и т.д.
4. Дополнительно: денормализация для аналитики (опционально)
Если система активно используется для аналитики и отчётов, можно создать материализованное представление или денормализованную таблицу фактов (например, «Товары с поставщиками»), где данные объединены для ускорения чтения — но только после построения нормализованной OLTP-структуры.

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 №____