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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

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 Математические методы защиты информации

обсуждены и рекомендованы к утверждению решением кафедры гуманитарных дисциплин и иностранных языков от 21 марта 2025 г., протокол № 7

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 Математические методы защиты информации 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 Математические методы защиты информации.

1. Паспорт оценочных материалов по дисциплине «Математические методы защиты информации»

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
ПК-3.5 Способен разрабатывать требования по защите, формированию политик безопасности компьютерных систем и сетей на основе менеджмента, аудита и оценки рисков информационной	ПК-3.5.1. Реализует формирование политик безопасности компьютерных систем	Знать: методы разработки и реализации политик безопасности компьютерных систем, принципы построения защищенных информационных инфраструктур, стандарты информационной безопасности и способы оценки рисков. Уметь: разрабатывать и внедрять политики безопасности компьютерной системы, оценивать риски угроз и обеспечивать защиту конфиденциальных данных, организовывать мероприятия по обеспечению соответствия стандартам информационной безопасности. Владеть: навыками проектирования и внедрения комплексных решений по защите компьютерных систем, методами анализа уязвимостей и мониторинга состояния безопасности инфраструктуры, инструментами управления доступом и защиты информации.	Тема 1. Математика криптографии. Тема 2. Алгоритмы шифрования Тема 3. Безопасность информационных систем предприятия Тема 4. Алгоритмы реализации электронно-цифровой подписи Тема 5. Безопасность корпоративной сети Тема 6. Безопасность в клиентско-серверных приложений Тема 7. Методы защиты информации	Реферат (темы 1-7)	Лабораторная работа 1-7
	ПК-3.5.2.	Знать: методы выявления объектов и	Тема 1. Математика	Реферат (темы	Лабораторная

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
	Принимает решения о необходимости защиты информа-ции, содержащейся в ИС	субъектов информационной безопасности, критерии классификации уровней конфиденциальности информации, механизмы принятия решений относительно защиты информации в информационных системах. Уметь: анализировать угрозы и риски утечки или повреждения информации, определять необходимость защиты информации, содержащейся в информационных системах, формулировать требования к уровню защиты и механизмам контроля доступа. Владеть: навыками анализа и обоснования выбора методов и технологий защиты информации, принятием решений о применении конкретных мер защиты и контроле эффективности защитных мероприятий.	криптографии. Тема 2. Алгоритмы шифрования Тема 3. Безопасность информационных систем предприятия Тема 4. Алгоритмы реализации электронно-цифровой подписи Тема 5. Безопасность корпоративной сети Тема 6. Безопасность в клиентско-серверных приложений Тема 7. Методы защиты информации	1-7) Тест 1 Практическое задание 1,2,3	работа 1-7
	ПК-3.5.3 Анализирует компьютерную систему с целью определения	Знать: методики анализа и оценки рисков информационной безопасности, процедуры менеджмента информационной безопасности, инструменты и технологии аудита компьютерных систем, классификацию	Тема 1. Математика криптографии. Тема 2. Алгоритмы шифрования Тема 3.	Реферат (темы 1-7) Тест 2 Практическое	Лабораторная работа 1-7

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
	необходимого уровня защищенности и доверия на основе менеджмента, аудита и оценки рисков информационной безопасности	уровней защищённости и доверия. Уметь: проводить аудит информационной безопасности компьютерной системы, выявлять потенциальные угрозы и уязвимости, определять необходимый уровень защищённости и доверия, формировать рекомендации по улучшению механизмов защиты. Владеть: навыками анализа компьютерных систем с точки зрения информационной безопасности, осуществления комплексной оценки рисков, принятия управленческих решений по повышению уровня защищённости и доверия на основе результатов аудита и анализа рисков.	Безопасность информационных систем предприятия Тема 4. Алгоритмы реализации электронно-цифровой подписи Тема 5. Безопасность корпоративной сети Тема 6. Безопасность в клиентско-серверных приложений Тема 7. Методы защиты информации	задание 4,5,6	

2. Оценочные материалы по дисциплине «Математические методы защиты информации»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов по темам 1-7

1. Криптоалгоритмы хэш-алгоритмы. Общая структура и классификация.
2. Ассиметричное шифрование. Общий подход. Односторонняя и криптографически- односторонняя функция. Общие требования.
3. Общие понятия электронной цифровой подписи. Функции и область применения.
4. Цифровой сертификат. Жизненный цикл.
5. Алгоритмы построения ЭЦП на основе RSA и El-gamal
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
7. Атаки на информационную систему в современной экономике. Понятие и классификация.
8. Государственное регулирование систем защиты от НСД. Реестры ФСТЭК и ФСБ России.
9. Модели цифровой зрелости правительства.
10. Этика и цифра: этические проблемы при использовании современных информационных технологий.
11. Этика искусственного интеллекта.
12. Системы принятия решений.
13. Self-service аналитика.
14. Предикативная аналитика.
15. Экосистема Internet of Things.
16. Облачный BI.
17. DSS (Decision Support System) системы: понятие, назначение, классификация.

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

Задание 1.

Направление связи состоит из n1 основных, n2 резервных каналов связи, общего накопителя емкостью на L сообщений, n источников. Интервалы T1, T2, ..., Tn поступления сообщений случайные. При нормальной работе сообщения передаются по основным каналам. Время Tп1, Tп2, ..., Tпn передачи случайное. Основные каналы подвержены

отказам. Интервалы времени Тот1, Тот2, ..., Тотn1 между отказами случайные. Если отказ происходит во время передачи, то отыскивается исправный и свободный основной канал. Если такого нет, включается один из резервных каналов, если он исправен и свободен. Время Твк1, Твк2, ..., Твкn2 включения постоянное для соответствующего канала. Сообщение, передача которого была прервана, передается по включенному резервному каналу. Время Тпр1, Тпр2, ..., Тпрn2 передачи случайное. Отказавший основной канал восстанавливается. Время Тв1, Тв2, ..., Твn1 восстановления случайное. После восстановления резервный канал выключается, и восстановленный канал продолжает работу с передачи очередного сообщения. Резервные каналы также подвержены отказам. Интервалы времени Тотр1, Тотр2, ..., Тотрn2 между отказами случайные. Отказавший резервный канал восстанавливается. Время Твр1, Твр2, ..., Тврn2 восстановления случайное. Для прерванного сообщения отыскивается возможность передачи по любому исправному и свободному каналу. В случае полного заполнения накопителя, поступающие сообщения теряются.

Задание на исследование. Разработать имитационную модель функционирования направления связи. Исследовать влияние емкости накопителя, интервалов времени поступления сообщений и количества каналов на вероятность отказа в передаче сообщений от каждого источника и по направлению связи в целом. Время моделирования – Т часов. Провести дисперсионный анализ. Факторы и их уровни выбрать самостоятельно. 9 Сделать выводы о загруженности каналов связи и необходимых мерах по повышению эффективности функционирования направления связи.

Задание 2.

Постановка задачи. На дежурстве находятся n1 средств связи (СС) n2 типов (n21 + n22 + ... + n2n2 = n2) в течение n3 часов. Каждое СС может в любой момент времени выйти из строя. В этом случае его заменяют резервным, причем либо сразу, либо по мере его появления. Тем временем, вышедшее из строя СС ремонтируют, после чего содержат в качестве резервного. Всего количество резервных СС n4. Ремонт неисправных СС производят n5 мастеров. Время Т1, Т2, ..., Тn2 ремонта случайное и зависит от типа СС, но не зависит от того, какой мастер это СС ремонтирует. Интервалы времени Т21, Т22, ..., Т2n2 между отказами находящихся на дежурстве СС случайные. Прибыль от СС, находящихся на дежурстве, составляет S1 денежных единиц в час. Почасовой убыток при отсутствии на дежурстве одного СС – S2 денежных единиц. Оплата мастера за ремонт неисправного СС S31, S32, ..., S3n2 денежных единиц в час. Затраты на содержание одного резервного СС составляют S4 денежных единиц в час.

Задание на исследование. Разработать имитационную модель функционирования системы ремонта средств связи. Исследовать через промежутки времени ΔТ влияние на ожидаемую прибыль различного количества резервных средств связи и мастеров. Определить абсолютные величины и относительные коэффициенты ожидаемой прибыли для каждого промежутка ΔТ по каждому типу средств связи и в целом. Результаты моделирования необходимо получить с точностью ε = 0,01 и доверительной вероятностью α = 0,99. Сделать выводы о загруженности средств связи, мастеров по промежуткам ΔТ и необходимых мерах по совершенствованию системы ремонта.

Задание 3.

Выполните модель простого события A, вероятность наступления которого равна 0,3. Произведите однократный пуск модели. Ответьте на вопрос: что регистрируют блоки Scope, Scope1, Display? Что вы наблюдаете при многократном пуске модели и почему? • Измените вероятность появления события на 0,8. Что произойдет с показаниями блока Scope? Почему? 26 • Доработайте модель путем замены блока UniformRandomNumber на блок InterpretedMATLABFunction. При этом выберите генератор случайных чисел, формирующий равномерно распределенные случайные числа в интервале (0, 1). Проведите моделирование и

ответьте на вопрос: чем отличаются показания регистрирующих блоков в данной модели и предыдущей? Почему?

Задание 4.

Соберите модель двух синхронных процессов: 1-й процесс – процесс обслуживания заявки (процесс оплаты в кассе, при этом время обслуживания не равно «0», данный процесс подчиненный по отношению ко второму процессу). 2-й процесс – процесс потока заявок на обслуживание (поток покупателей, подходящих к кассе). Интервал между заявками (покупателями) соизмерим с временем обслуживания заявки (процессом оплаты). Исходные данные для моделирования: Закон плотности распределения интервалов между заявками и времени обслуживания – экспоненциальный. Среднее время между заявками (интервал между покупателями) Tср = 1 мин, среднее время обслуживания заявки (обслуживания в кассе) Tср.касс = 5 мин. Закон плотности распределения суммы покупки – нормальный с параметрами MD = 3000 рублей, среднее квадратическое отклонение SD = 700 рублей. Завершите моделирование по условию: сумма, поступившая в кассу, равна 2000 рублей.

Задание 5.

Разработайте имитационную модель работы билетных касс. В кассы есть единая очередь, которую обслуживают две основные кассы. Если основные кассы не справляются с потоком покупателей, то открывается третья касса. Поток покупателей меняется в зависимости от времени суток и становится больше в выходные дни. Расписание потока покупателей приведено ниже. Рабочие дни: 8:00–13:00 – десять человек в час; 13:00–16:00 – пятнадцать человек в час; 16:00–22:00 – двадцать человек в час. Выходные дни: 9:00–12:00 – двадцать человек в час; 12:00–21:00 – сорок человек в час. Покупатели, время ожидания покупки у которых превысило час, уходят из касс, не купив билета. Время обслуживания одного покупателя в кассах меняется случайным образом от 2 до 15 минут и в среднем составляет 5 минут. Предусмотреть в модели учет купивших и некупивших билеты. Выявите узкие места в модели и предложите решение.

Задание 6.

Имитационная модель циклов роста и падений в экономике (кризисов). Задачей имитационного моделирования является исследования причинно-следственного механизма возникновения циклов и кризисов перепроизводства. Предположим, промышленность выпускает автомобили. Существует постоянно растущая потребность в данном товаре. Полагаем, что производство полностью удовлетворяет потребности, но с задержкой (время на разработку новой модели автомобиля, подготовка производства к выпуску и т.д.). Выпущенные автомобили поступают в эксплуатацию от производителей. Поскольку автомобили – вещь долговременного пользования, то происходит их накопление. По истечении сроков эксплуатации, износа, аварий и т.д. происходит их выбытие из эксплуатации. Модель должна вычислять предложение на автомобильном рынке, спрос на товар при изменении задержки при производстве автомобилей и позволять оценить степень устойчивости производства к кризисам и циклам. Используя блок-схему модели, приведенную на рисунке, постройте имитационную модель кризисов, дополнив ее имитацией случайных факторов. Такими факторами могут быть: растущий, но ежегодно колеблющийся спрос на продукцию; срок службы товара как случайная величина. Вид закона распределения случайного фактора и его параметры задайте самостоятельно и

поясните, почему вы приняли именно такой закон и параметры. Задайте параметры блоков модели, придав параметрам конкретное физическое толкование. Добейтесь работоспособности модели путем подбора параметров и пробных прогонов модели. Поясните назначение блоков модели и параметров блоков модели. Исследуйте с помощью построенной модели зависимость устойчивости системы (производства автомобилей) при различных лагах производства. Что происходит при увеличении задержки производства, т.е. отставания реакции производства на спрос, почему? Исследуйте влияние параметра срока службы на показатели экономической системы (устойчивость, появление кризисов). Приведите результаты и поясните их. Укажите, при каких параметрах модели система будет устойчива? 34 Учитывая, что под начальным дефицитом понимается разница между необходимым и реальным парком автомобилей на момент моделирования, измените величину начальных условий на интеграторе блока «Поступление» и исследуйте влияние дефицита на показатели экономической системы, т.е. устойчивость, возможность кризисов. Что следует изменить в модели, чтобы повысить адекватность моделирования? Придайте случайным факторам конкретное экономическое или техническое толкование.

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.

ЛАБОРАТОРНЫЕ РАБОТЫ

Наименование раздела, темы дисциплины	Содержание лабораторных работ
Тема 1. Лабораторная работа № 1. Математика криптографии. Поиск чисел НОД	Ознакомление студентов с методами нахождения наибольшего общего делителя (НОД) двух целых чисел и закрепление практических навыков вычисления НОД для решения криптографических задач. Методы вычисления НОД:метод перебора делителей: алгоритм заключается в последовательном переборе всех возможных общих делителей меньшего из двух чисел и выборе максимального среди них. Алгоритм Евклида: используется принцип деления остатков. Для пары (a,b), где $a>b$, повторяем деление большего числа на меньшее, пока остаток не станет равным нулю. Последний ненулевой остаток является искомым НОД. Расширенный алгоритм Евклида: позволяет

Наименование раздела, темы дисциплины	Содержание лабораторных работ
	дополнительно находить коэффициенты линейного представления НОД, т.е. целые числа x и y такие, что $ax+by=\gcd(a,b)$. Используется для решения диофантовых уравнений и построения обратимых элементов в кольцах вычетов. Подробное изложение методов вычисления НОД. Примеры расчета НОД различными методами. Выводы о преимуществах каждого метода. Программную реализацию любого выбранного вами метода на Python.
Тема 2. Лабораторная работа № 2. Поля Галуа, Многочлены, Примитивность многочлена	Изучение свойств конечных полей Галуа, операций над элементами поля, примитивных многочленов и формирование практических навыков работы с ними. Основные понятия и обозначения: Поле Галуа: конечное поле с числом элементов p^n, где p — простое число, называется полем Галуа и обозначается GF(p^n). Если n=1, поле называют простым полем, примитивный элемент: Элемент поля, порождающий мультипликативную группу поля, называется примитивным элементом, простой неприводимый многочлен. Операции в полях Галуа: сложение и умножение.
Тема 3. Лабораторная работа № 3. Безопасность информационных систем предприятия.	Практическое изучение механизмов защиты информационной инфраструктуры предприятий, освоение методик оценки рисков и разработка мер противодействия угрозам информационной безопасности. Информационная безопасность предприятия включает защиту конфиденциальных данных, предотвращение несанкционированного доступа, контроль целостности информации и обеспечение доступности ресурсов. Оценка риска включает выявление уязвимостей системы, определение вероятных угроз и оценку последствий атак. Изучение топологии локальной сети предприятия. Идентификация ключевых компонентов ИТ-инфраструктуры. Моделирование потенциальных киберугроз (DDoS атаки, фишинговые кампании, вирусы-шифровальщики и др.). Разработка сценария действий злоумышленника. Настройка межсетевых экранов (firewall) и антивирусных решений. Использование технологии виртуальных частных сетей (VPN) для удалённого доступа сотрудников.
Тема 4. Лабораторная работа № 4. Алгоритмы реализации электронно цифровой подписи.	Изучить принципы функционирования электронных цифровых подписей (ЭЦП), освоить базовые алгоритмы их формирования и верификации, закрепить практические навыки разработки приложений, обеспечивающих надежную цифровую подпись документов. Электронная цифровая подпись (ЭЦП) используется для подтверждения подлинности документа, целостности передаваемых данных и ответственности отправителя за содержание информации. Основой большинства современных схем ЭЦП являются асимметричные криптографические алгоритмы, использующие ключи шифрования и дешифрования. Авторизация сообщений и подтверждение происхождения информации. Целостность данных: защита от изменения или искажения содержания. Ознакомление с основными принципами и

Наименование раздела, темы дисциплины	Содержание лабораторных работ
	свойствами ЭЦП. Изучение математической основы наиболее популярных алгоритмов цифровой подписи (RSA, DSA, ECDSA). Освоение процедуры генерации открытых и закрытых ключей для указанных алгоритмов. Рассмотрение форматов хранения и распространения сертификатов открытого ключа. Реализация процесса хеширования документа и создание цифровой подписи с использованием закрытого ключа. Запись формата подписи в файл и сохранение вместе с документом.
Тема 5. Лабораторная работа № 5. Безопасность корпоративной сети.	Освоение основ проектирования безопасной корпоративной сети, изучение методов защиты корпоративных информационных систем, обучение построению эффективной модели управления доступом и защиты каналов передачи данных. Проектирование надежной архитектуры корпоративной сети с применением соответствующих стандартов и технологий. Изучение методов защиты периметра сети, включая использование брандмауэров, IDS/IPS, VPN и прокси-серверов. Освоение методов контроля доступа и идентификации пользователей внутри корпоративной сети. Оценка угроз безопасности и выбор оптимальных мер защиты. Изучение требований безопасности при проектировании топологии корпоративной сети. Выбор оптимальной конфигурации аппаратных и программных компонентов. Настройка правил фильтрации и управления пакетами на уровне брандмауэра. Анализ возможностей использования NAT, DHCP и DNS-сервисов для повышения безопасности. Применение механизмов аутентификации и авторизации пользователей (LDAP, Kerberos, Radius). Интеграция сервисов единого входа (SSO).
Тема 6. Лабораторная работа № 6. Безопасность в клиентско серверных приложений.	Изучение и применение методов обеспечения безопасности в клиентско-серверных системах, ознакомление с основными угрозами и способами их нейтрализации, приобретение навыков практической настройки защиты веб-приложений. Освоение базового инструментария и приемов защиты клиентских и серверных частей веб-приложений. Углубленное изучение методов защиты от инъекций SQL, XSS-атак, CSRF-атак и атак типа "перехват сессии". Изучение и реализация практик безопасного кодирования на стороне клиента и сервера. Оценка эффективности применяемых мер защиты и проведение тестов на проникновение.
Тема 7. Лабораторная работа № 7. Решение Диофантовых уравнений, Китайская теорема об остатках	Изучение и практика решения линейных диофантовых уравнений и применения китайской теоремы об остатках для решения задач целочисленной арифметики. Научиться применять расширенный алгоритм Евклида для решения диофантовых уравнений. Овладеть техникой нахождения наименьших положительных решений систем сравнений с помощью китайской теоремы об остатках. Написать программу на выбранном языке программирования (например, Python или JavaScript), которая решает указанные типы задач автоматически. Подробное решение приведённых примеров вручную. Листинг написанной программы с пояснениями к каждому этапу. Результаты расчётов и анализ полученных

Наименование раздела, темы дисциплины	Содержание лабораторных работ
	решений. Выводы о целесообразности использования изученных методов в реальных задачах криптографии и компьютерной безопасности.

Критерии оценивания выполнения лабораторной работы:

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

1.Формы представления информации в плане защиты информации

1. Цифровая, документированная, графическая
2. Программная, алгоритмическая, телекоммуникационная
3.Электронная, реквизитная, текстовая
4. Речевая, документированная, телекоммуникационная

2.Документированной называется информация

1. Представленная на материальных носителях вместе с идентифицирующими ее реквизитами
2. Представленная в виде кодов и сохраненная на лазерных дисках объемом 1,5 Мб.
3.Представленная только на жестких магнитных дисках вместе с идентифицирующими ее реквизитами
4. Закодированная и защищенная паролем, и представленная на носителях вместе с идентифицирующими ее реквизитами

3.К информации ограниченного доступа относится

1. Служебные сведения, не подлежащие распространению в сети интернет
2.Конфиденциальная информация, хранимая в государственных архивах данных
3.Информация, запрашиваемая гражданами в органах государственной власти
4.Государственная тайна и конфиденциальная информация.

4.Под защитой информации понимается

1. Комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности
2. Комплекс мероприятий, направленных на обеспечение целостности информации
3. Комплекс мероприятий, направленных на обеспечение хранения информации

4. Комплекс мероприятий, направленных на ввод, хранения, обработки и передачи данных

5. К основным характеристикам защищаемой информации относится

1. Кодируемость, корректность, целостность
2. Государственность, служебность, доступность
3. Конфиденциальность, целостность и доступность
4. Целостность, защищенность и доступность

6. Угроза безопасности информации это

1.Событие или действие, которое может вызвать изменение функционирования компьютерных систем, связанное с нарушением защищенности, обрабатываемой в ней информации

2. Действие, которое может вызвать искажение обрабатываемой информации
3. Событие, которое может послужить потере конфиденциальной информации
4. Событие или действие, которое может вызвать изменение функционирования физического

канала связи в компьютерных системах, по которому передается защищаемая информация

7. ПЭМИН –это утечка информации через_____

8. Уровни правового обеспечения информационной безопасности

1.Международные договоры, подзаконные акты, государственные стандарты, локальные нормативные акты

2. Международные договоры, Федеральные законы, государственные стандарты, Указы Президента РФ

3. Подзаконные акты, государственные стандарты, Постановления Правительства РФ

4. Локальные нормативные акты, письма Арбитражного Суда РФ, международные договоры

9.Комплексная система защиты информации

1. Это совокупность методов и средств, объединенных единым целевым назначением и

обеспечивающих необходимую эффективность защиты информации в КС.

2. Это совокупность объединенных единым целевым назначением средств, для обеспечения защиты информации в КС.

3. Это совокупность правил, законов и писем, в которых прописаны методы и средства

обеспечивающих необходимую эффективность защиты информации в КС.

4. Это свод правил утвержденные законодательно в целях организации эффективной защиты информации в КС

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

1. Основные способы защиты от несанкционированного доступа к информации в компьютерных системах

1. Идентификация, авторизация, шифрование

2. Аутентификация, авторизация, шифрование

3. Шифрование, аутентификация, электронная цифровая подпись

4. Электронная цифровая подпись, авторизация, шифрование

2.Основные недостатки парольной аутентификации

1.Сложно обеспечить реальную уникальность и сложность каждого вновь выбираемого

пользователем пароля

2. Возможность перехвата пароля в открытом виде или его подбора по хеш-значению

3. Возможность получения или смены пароля в результате обмана

4. Все вышеперечисленные недостатки

3.Сущность модели рукопожатия_____

4. Биометрические характеристики пользователей, которые могут применяться для их аутентификации

1.Отпечатки пальцев, геометрическая форма руки, узор радужной оболочки глаза

2. Рисунок сетчатки глаза, геометрическая форма и размеры лица

3. Тембр голоса, геометрическая форма и размеры уха

4. Все выше перечисленные биометрические характеристики

5.Характерные особенности аутентификации пользователей на основе их клавиатурного

почерка и росписи мышью?

1. Стабильность их характеристик для всех пользователей независимо от возраста и эмоционально- психологического состояния

2. Нестабильность их характеристик у одного и того же пользователя, связанными с улучшением навыков по работе с клавиатурой и мышью или наоборот из-за старения организма, а также с

изменениями, связанными с эмоциональным состоянием пользователя.

3. Нарушение навыков по работе с клавиатурой и мышью или наоборот из-за старения организма, а также с изменениями, связанными с эмоциональным состоянием пользователя.

4. Нестабильность их характеристик у одного и того же пользователя, связанными с улучшением их психологического состояния

6.Элементы аппаратного обеспечения, которые могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем

1. Магнитные диски, пластиковые карты с магнитной полосой, Touch Mamory, карты со штрих-кодом, смарт-карты, маркеры eToken (USB-брелки)

2. Магнитные диски, пластиковые карты, iButton, карты со штрих-кодом, смарт-карты, USBбрелки

3. Магнитные диски, пластиковые карты с магнитной полосой, карты со штрих-кодом, карты с памятью, смарт-карты, маркеры eToken

4. Магнитные диски, пластиковые карты, Touch Mamory, карты со штрих-кодом, смарткарты с паролем, USB-брелки с памятью

7.Touch Memory представляет собой

1. Миниатюрную батарейку с определенным диаметром и толщиной, имеющий один сигнальный контакт и один контакт заземления

2. Миниатюрную батарейку с определенным диаметром 16мм и толщиной в пределах от 3 до 6 мм, имеющий один сигнальный контакт и один контакт заземления

3. Миниатюрную батарейку с определенным диаметром 15 мм и толщиной в пределах от 4 до 6 мм, имеющий один сигнальный контакт и один контакт заземления

4. Миниатюрную батарейку с ПЗУ и ОЗУ со встроенным элементом питания

8.Двухфакторная аутентификация это_____

9. В основе работы протокола S/Key лежит протокол PAP для _____

10.Применяемые разновидности межсетевых экранов

1.фильтрующие маршрутизаторы

2. шлюзы сеансового уровня

3.шлюзы прикладного уровня

4. все вышеперечисленные

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. Как называется свойство информации, означающее, что с ней может ознакомиться только строго

ограниченный круг лиц, определенный ее владельцем?

а) целостность;

б) апеллируемость;

в) доступность;

г) конфиденциальность;

д) аутентичность.

2. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее

владельцем изменений?

а) целостность;

б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

3. Как называется свойство информации, позволяющее достоверно установить ее автора?
а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

4.
Какие предположения включает неформальная модель нарушителя?
а) о мотивах нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о социальном статусе нарушителя;
г) о предыдущих атаках, осуществленных нарушителем;
д) о времени действия нарушителя.

5. Какие предположения включает неформальная модель нарушителя?
а) о возможностях нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о привычках нарушителя;
г) о предыдущих атаках, осуществленных нарушителем;
д) об уровне знаний нарушителя.

6. Какие предположения включает неформальная модель нарушителя?
а) о месте действия нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о мотивах нарушителя;
г) о возможном ущербе АИС в результате действий нарушителя;
д) об уязвимостях системы безопасности, используемых нарушителем.

7. К каким мерам защиты относится «Оранжевая книга»?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

8. К каким мерам защиты относится политика безопасность?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

9. К каким мерам защиты относится управление персоналом?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

10. Администратор закрыл для сотрудников организации доступ в Интернет, разрешив лишь пользование
электронной почтой. К какому виду мер защиты информации относится данная мера?
а) политика безопасности верхнего уровня;
б) политика безопасности среднего уровня;
в) политика безопасности нижнего уровня;
г) принцип минимизации привилегий;
д) защита поддерживающей инфраструктуры.

11. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?
а) политика безопасности верхнего уровня;
б) политика безопасности среднего уровня;
в) политика безопасности нижнего уровня;
г) принцип минимизации привилегий;
д) защита поддерживающей инфраструктуры.

12. Администратор запретил самостоятельную установку программного обеспечения сотрудниками
организации. К какому виду мер защиты информации относится данная мера?
а) политика безопасности верхнего уровня;
б) политика безопасности среднего уровня;
в) политика безопасности нижнего уровня;
г) принцип минимизации привилегий;
д) защита поддерживающей инфраструктуры.

13. К основным принципам построения системы защиты АИС относятся:
а) разумная достаточность;
б) непрерывность;
в) масштабируемость;
г) гибкость;
д) доступность.

14. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;
д) простота.

15. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) независимость подсистем защиты;
в) сложность;
г) масштабируемость;
д) непрерывность.

16. Модель безопасности Белла-ЛаПадулы...
а) ... устанавливает различные уровни «секретности» объектов и субъектов доступа;
б) ... устанавливает набор разрешенных операций доступа для каждой пары «субъект-объект»;
в) ... привязывает набор разрешенных действий к роли, которую выполняет пользователь;

г) ... запрещает некоторым субъектам определенные виды доступа к некоторым объектам.

17. К какой разновидности моделей управления доступом относится модель Белла-ЛаПадулы?
а) модель дискреционного доступа;
б) модель мандатного доступа;
в) ролевая модель.

18. Модель безопасности RBAC...
а) ... устанавливает различные уровни «секретности» объектов и субъектов доступа;
б) ... устанавливает набор разрешенных операций доступа для каждой пары «субъект-объект»;
в) ... привязывает набор разрешенных действий к роли, которую выполняет пользователь;
г) ... запрещает некоторым субъектам определенные виды доступа к некоторым объектам.

19. Какие из следующих высказываний о модели управления доступом RBAC справедливы?
а) каждый пользователь играет в системе некоторую единственную роль;
б) роли упорядочены в иерархию;
в) с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли;
г) несколько пользователей не могут иметь одну и ту же роль одновременно.

20. Какие из следующих высказываний о модели управления доступом RBAC справедливы?
а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей;
б) роли упорядочены в иерархию;
в) с каждым объектом доступа ассоциировано несколько ролей ;
г) для каждой пары «субъект-объект» назначен набор возможных разрешений.

21. Какие требования накладывает модель Белла-ЛаПадулы?
а) несекретный пользователь (или процесс, запущенный от его имени) не может читать данные из
секретного файла;
б) пользователь с уровнем доступа к секретным данным не может читать данные из несекретного
файла;
в) пользователь с уровнем доступа к секретным данным не может записывать данные в несекретный
файл;
г) несекретный пользователь (или процесс, запущенный от его имени) не может записывать данные
в секретный файл;
д) только секретные пользователи могут читать и записывать секретные файлы.

22. В каком из представлений матрицы доступа наиболее просто определить файлы, доступ к которым имеет
конкретный пользователь?
а) ACL;
б) списки полномочий субъектов;
в) атрибутные схемы.

23. В каком из представлений матрицы доступа наиболее просто определить пользователей,

имеющих доступ к
определенному файлу?
а) ACL;
б) списки полномочий субъектов;
в) атрибутные схемы.

24. В каком из представлений матрицы достигается наибольшая экономия памяти для хранения всевозможных
разрешений?
а) ACL;
б) списки полномочий субъектов;
в) атрибутные схемы.

25. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует списки управления доступом для представления матрицы доступа;
в) ... является неотъемлемой частью любой системы обеспечения безопасности;
г) ... фиксирует информацию о попытках доступа в системном журнале; .

26. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует атрибутные схемы для представления матрицы доступа;
в) ... выступает посредником при всех обращениях субъектов к объектам;
г) ... фиксирует информацию о попытках доступа в системном журнале;

27. Диспетчер доступа...
а) ... является неотъемлемой частью любой системы обеспечения безопасности;
б) ... может использовать базу данных защиты, построенную на основе атрибутных схем;
в) ... выступает посредником при всех обращениях субъектов к объектам;
г) ... фиксирует информацию о попытках доступа в системном журнале;

28. Какие объектамы наиболее подвержены угрозам ИБ в сфере экономики (согласно доктрине
информационной безопасности РФ)?
а) система государственной статистики;
б) информационные ресурсы федеральных органов исполнительной власти и СМИ;
в) системы управления сложными исследовательскими комплексами (ядерными реакторами,
ускорителями элементарных частиц, плазменными генераторами и другими);
г) системы бухгалтерского учета;
д) кредитно-финансовая система.

29. Что представляет собой доктрина информационной безопасности РФ?
а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;
б) федеральный закон, регулирующий правоотношения в области информационной безопасности;
в) целевая программа развития системы информационной безопасности РФ, представляющая собой
последовательность стадий и этапов;
г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

30. Какие меры по обеспечению информационной безопасности Российской Федерации в сфере экономики
называет доктрина информационной безопасности РФ?
а) активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России;
б) совершенствование нормативной правовой базы, регулирующей информационные отношения в
сфере экономики;
в) создание системы противодействия монополизации отечественными и зарубежными структурами
составляющих информационной инфраструктуры, включая рынок информационных услуг и средства
массовой информации;
г) разработка национальных сертифицированных средств защиты информации и внедрение их в
системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой,
налоговой, таможенной информации;
д) совершенствование методов отбора и подготовки персонала для работы в системах сбора,
обработки, хранения и передачи экономической информации.

31. 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)

32. В виде СДНФ нельзя представить…… . (Ответ записать цифрой)

33. Имеется некоторое множество из 100 различных натуральных чисел. В нѐм 50 чѐтных чисел, 40 чисел, кратных (делящихся нацело) трѐм, 35 чисел, кратных пяти, 15 чисел, кратных шести, 10 чисел, заканчивающихся нулѐм, 8 чисел, кратных 15 и 3 числа, кратные 30. Есть ли в этом множестве, числа не делящиеся ни на 2, ни на 3, ни на 5? Сколько?
(Ответ записать цифрой)

34. Верно ли утверждение, что возможен принцип асинхронной работы в Loginom Community?
а) Да
б) Нет
в) Только в отдельных случаях
г) Только при создании подмоделей

35. Что такое качественный анализ рисков ИТ-проекта?
а) оценка вероятности возникновения риска и размера ущерба/выгоды
б) оценка рисков в терминах их возможных последствий с использованием установленных критериев
в) оценка объема работ, которые необходимо выполнить для устранения риска ИТ-проекта

г) оценка вероятности срыва проектных сроков

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 №____