Федеральное государственное бюджетное образовательное учреждение высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ

УТВЕРЖДАЮ

И.О. декана РТФ

В.А. Баженов

27. 06 2018 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

(приложение к рабочей программе дисциплины)

СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

(наименование дисциплины)

вариативной части образовательной программы по специальности
10.05.03 «Информационная безопасность автоматизированных систем»

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
(наименование специализации программы)

Факультет – **РАДИОТЕХНИЧЕСКИЙ**
Кафедра – **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Калининград 2018

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Б1.В.ДВ.07.01 «Системы защиты от утечки конфиденциальной информации»
(код) (наименование дисциплины)

№ п/п	Контролируемые модули, разделы (темы) дисциплины	Код контролируемой компетенции	Оценочные средства	Способ контроля
			наименование	
1	Тема 1. Теоретические основы защиты конфиденциальной информации от внутренних угроз.	ПК-22, ПСК-7.5	собеседование, доклад	устный
2	Тема 2. Нормативно-правовые аспекты защиты конфиденциальной информации от внутренних угроз.	ПК-22, ПСК-7.5	собеседование, контрольная работа, защита практического занятия	устный письменный
3	Тема 3. Административно-организационные аспекты корпоративной защиты от внутренних угроз.	ПК-17, ПК-22, ПСК-7.5	собеседование, контрольная работа, защита практического занятия	устный письменный
4	Тема 4. Защита корпоративной информации с использованием автоматизированной системы контроля информационных потоков.	ПК-3, ПК-17, ПК-22, ПСК-7.5	собеседование, контрольная работа, защита практического занятия	устный письменный

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Б1.В.ДВ.07.01 «Системы защиты от утечки конфиденциальной информации»

(код) (наименование дисциплины)

№ п/п	Код компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины студенты должны:		
			знать	уметь	владеть
1.	ПК-3	способность проводить анализ защищенности автоматизированных систем	требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; технические каналы утечки информации	разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений	- навыками формальной постановки и решения задачи обеспечения информационной безопасности автоматизированных систем
2.	ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	навыками приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, направленных на развитие социальных и профессиональных компетенций, изменение вида своей профессиональной деятельности
3.	ПК-22	способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах	эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности автоматизированных систем	навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительные системы; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках

4.	ПСК-7.5	способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации	принципы проектирования системы корпоративной защиты от внутренних угроз; основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах; инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз	разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности; проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации; администрировать автоматизированные технические средства управления и контроля информации и информационных потоков.	навыками подготовки нормативно-правовой базы и регламентирующих документов; разработки и внедрения политики информационной безопасности в хозяйствующем субъекте; проведения корпоративного информационного аудита; работы с автоматизированными техническими средствами управления и контроля информации и информационных потоков.

ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ИЗУЧЕНИЯДИСЦИПЛИНЫ

Б1.В.ДВ.07.01 «Системы защиты от утечки конфиденциальной информации»

(код) (наименование дисциплины)

Семестр А

№ п/п	Код контролируемой компетенции (или ее части)	№ учебной недели											
		1	2	3	4	5	6	7	8	9	10	11	12
		Этапы формирования компетенции											
1.	ПК-3								+	+	+	+	+
2.	ПК-17			+	+								
3.	ПК-22	+	+				+	+	+				
4.	ПСК-7.5	+	+			+	+			+	+	+	+

ПОКАЗАТЕЛИ И КРИТЕРИИ ОПРЕДЕЛЕНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

№ п/п	Код контролируемой компетенции (или ее части)	Уровни сформированности компетенции		
		пороговый	продвинутый	высокий
	ПК-3	Знать:		
		классификацию АС и перечень требований по защите информации к каждому классу автоматизированных систем	требования стандарта ISO по номенклатуре услуг, предоставляемых системой безопасности	основные положения концепции защиты и показатели защищенности АС от несанкционированного доступа к информации
		Уметь:		
		определять цель, объект и место проведения анализа АС, уточнять вид проводимого инструментального контроля, составлять перечень исследуемых систем	применять существующую методическую базу проведения оценки защищенности технических средств от утечки информации	проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию
		Владеть:		
		навыками систематизации, обобщения справочной, нормативно-технической информации	навыками поиска, обобщения, систематизации научно-технической информации, составления кратких отчетов, рефератов	навыками обобщения и систематизации научно-технической информации из предметной области исследований и других областей науки и техники, непосредственно примыкающих к проведенным исследованиям
	ПК-17	Знать:		
		принципы и правила построения защищенных автоматизированных систем предприятия (организации)	формальные модели безопасности и основные принципы построения модели защиты АС	основные принципы и методы планирования функционирования защищенных автоматизированных систем
		Уметь:		
		производить анализ и оценку защищенности автоматизированных систем	проводить оценку функциональной целостности организационно-технической системы безопасности АС	применять типовые модели анализа проектных решений по обеспечению безопасности АС
		Владеть:		
		навыками разработки нормативно-методических материалов по регламентации системы организационной защиты информации	навыками работы с нормативно-правовыми актами	методологией прикладных научных исследований в предметной области
	ПК- 22	Знать:		
		основные принципы, реализуемые при разработке политики информационной безопасности организации	основные принципы, реализуемые при разработке политики информационной безопасности организации	основные принципы, реализуемые при разработке политики информационной безопасности организации
		Уметь:		
		разрабатывать функциональные обязанности должностных лиц организации по во-	разрабатывать функциональные обязанности должностных лиц органи-	разрабатывать функциональные обязанности должностных лиц органи-

		просам защиты информации	зации по вопросам защиты информации	зации по вопросам защиты информации
		Владеть:		
		навыками разработки материалов системы организационной защиты информации	навыками работы с нормативно-правовыми актами	методологией прикладных научных исследований в предметной области
	ПСК-7.5	Знать:		
		основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации в сетях ЭВМ	способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	принципы построения систем защиты информации
		Уметь:		
		классифицировать и оценивать угрозы безопасности информации для объекта информатизации	разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	разрабатывать политики безопасности информации автоматизированных систем
		Владеть:		
		навыками обоснования и контроля результатов управленческих решений в области безопасности информации автоматизированных систем	навыками оценки информационных рисков	навыками обоснования критериев эффективности функционирования защищенных автоматизированных систем

ПЕРЕЧЕНЬ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися. Обсуждаются отдельные части, разделы, темы, вопросы изучаемого курса, обычно не включаемые в тематику семинарских и других практических учебных занятий, а также рефераты, проекты и иные работы обучающихся. Коллоквиум ставит следующие задачи: - проверка и контроль полученных знаний по изучаемой теме; - углубление знаний при помощи использования дополнительных материалов при подготовке к занятию; - студенты должны продемонстрировать умения работы с различными видами исторических источников; - формирование умений коллективного обсуждения (поддерживать диалог в микрогруппах, находить компромиссное решение, аргументировать свою точку зрения, умение слушать оппонента).	Вопросы по темам/разделам дисциплины
Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.Во время проверки и оценки контрольных письменных работ проводится анализ результатов выполнения, выявляются типичные ошибки, а также причины их появления. Анализ работ проводится оперативно. При проверке контрольных работ преподавателюнеобходимо исправить каждую допущенную ошибку и определить полноту изложения вопроса, качество и точность расчетной и графической части, учитывая при этом развитие письменной речи, четкость и последовательность	Комплект контрольных заданий по вариантам

	изложения мыслей, наличие и достаточность пояснений, культуру в предметной области.	
Рабочая тетрадь	Рабочая тетрадь студента является учебно-методическим пособием, целью которого является закрепление знаний, полученных на лекциях, и формирование у студентов навыков и умения самостоятельной работы с рекомендованной литературой. Его задача – организовать самостоятельную работу студента и контроль за ней со стороны преподавателя, помочь систематизировать важнейшие материалы изучаемого курса, развить способность логично и содержательно выражать свои мысли в письменной форме. Необходимость создания рабочей тетради и ее тематика определяется кафедрой. Она бывает вызвана, например, наличием труднодоступных для студента, но очень важных для осмысления проблем дисциплины источников. Кафедра может обеспечить студенту возможность работы с этими источниками, опубликовав их в составе рабочей тетради с соблюдением установленных правил такой публикации и снабдив вопросами и заданиями. Как показывает практика, формат тетради весьма удобен для решения студентами конкретных ситуаций, задач. В этом случае работа студента способствует выработке необходимых практических навыков, предусмотренных требованиями к уровню подготовки по данной дисциплине.	Образец рабочей тетради
Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а так же собственные взгляды на неё.	Темы рефератов
Доклад, сообщение	Доклад – это краткое публичное устное изложение результатов индивидуальной учебно-исследовательской деятельности, имеет регламентированную структуру, содержание и оформление. Задачами являются: формирование умений самостоятельной работы обучающихся с источниками литературы, их систематизация; развитие навыков логического мышления; углубление теоретических знаний по проблеме исследования; развитие навыков изложения своих мыслей и идей перед аудиторией, умения уверенно пользоваться научной терминологией.	Темы докладов, сообщений.
Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанная на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
Тест	Форма контроля, направленная на проверку уровня освоения контролируемого теоретического и практического материала по дидактическим единицам дисциплины (терминологический аппарат, основные методы, информационные технологии, приемы, документы, компьютерные программы, используемые в изучаемой области).	Перечень тестов
Зачет	Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения учебного материала практических и семинарских занятий, успешного прохождения производственной и преддипломной практик и выполнения в процессе этих практик всех учебных поручений в соответствии с утвержденной программой.	Вопросы на зачет

ФГБОУ ВО «КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
БАЛТИЙСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ РЫБОПРОМЫСЛОВОГО ФЛОТА

Типовые вопросы к зачету*

Дисциплина:	Основыинформационной безопасности	Специальность:	10.05.03.
Семестр:	IV		
Кафедра:	Информационная безопасность		

1.	Определение и место информационной безопасности в общей совокупности информационных проблем современного общества.
2.	Законодательная база Российской Федерации по обеспечению информационной безопасности.
3.	Международные нормативно-правовые акты в области информационной безопасности.
4.	Современная постановка задачи защиты информации.
5.	Методологический базис решения задач защиты информации.
6.	Система стандартизации в области защиты информации.
7.	Моделирование процессов защиты информации.
8.	Понятие угрозы безопасности информации. Риски и управление рисками
9.	Системная классификация угроз безопасности информации.
10.	Методы оценки уязвимости информации. Формула оценки уязвимости информации.
11.	Методы оценки достоверности информации.
12.	Методы оценки ущерба от реализации угроз безопасности информации.
13.	Способы несанкционированного доступа к данным. Методы обеспечения недоступности данных.
14.	Анализ методик определения требований к защите информации.
15.	Параметры защищаемой информации.
16.	Принципы защиты информации от несанкционированного доступа.
17.	Методы идентификации и аутентификации пользователей.
18.	Методы контроля доступа.
19.	Системы блочного шифрования: DES и ГОСТ.
20.	Цифровая подпись и система шифрования с открытым ключом.
21.	Средства антивирусной защиты.
22.	Вирусное подавление как форма радиоэлектронной борьбы.
23.	Защита информационно-программного обеспечения на уровне операционных систем.
24.	Защита информации на уровне систем управления базами данных.
25.	Способы защиты информации в локальных и глобальных компьютерных сетях.
26.	Основные виды технических каналов и источников утечки информации в автоматизированных системах.
27.	Физические основы утечки защищаемой информации по акустическому каналу, линиям связи и каналу побочного электромагнитного излучения.
28.	Характеристики каналов утечки информации в автоматизированных системах.
29.	Способы предотвращения утечки информации по техническим каналам.

30.	Классификация средств вычислительной техники по защищенности от НСД.
31.	Классификация автоматизированных систем по защищенности от НСД.
32.	Классификация межсетевых экранов по защищенности от НСД.
33.	Обобщенная схема обеспечения информационной безопасности. Структура унифицированной концепции защиты информации.
34.	Классификация (критерии) технических средств защиты информации.
35.	Общие принципы создания и функционирования системы обеспечения безопасностью предприятия.
36.	Назначение политики безопасности и ее содержание.
37.	Этапы создания систем защиты информации.
38.	Назначение и функции службы безопасности предприятия.
39.	Содержание деятельности службы безопасности.
40.	Типовая структура службы безопасности предприятия. Обязанности сотрудников.
41.	Система стандартов в области защиты информации.
42.	Основное содержание стандарта ISO27001 (17799):2005. Результаты работы предприятия по подготовке к сертификации по стандарту.
43.	Основы проектирования и оценка систем физической защиты. Последовательность и содержание работ по проектированию систем физической защиты.
44.	Основное содержание Протокола обследования предприятия.
45.	Основное содержание отчета об оценке анализа уязвимости предприятия.
46.	Определение и место информационной безопасности в общей совокупности информационных проблем современного общества.
47.	Законодательная база Российской Федерации по обеспечению информационной безопасности.
48.	Международные нормативно-правовые акты в области информационной безопасности.

Вопросы рассмотрены и утверждены на заседании кафедры	Дата:	Протокол №
Заведующий кафедрой	подпись	

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебныхзанятий	Организация деятельности студента
Лекция	В ходе лекционного занятия рекомендуется вести конспектирование учебного материала.Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект должен быть грамотным, т.е. включать только самое основное, с использованием системы знаков, сокращений и выделений. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Самостоятельная подготовка студента к лекции в первую очередь предполагает повторение законспектированного материала предыдущей лекции. Это помогает лучше понять материал новой лекции, опираясь на предшествующие знания. Преподаватель может стимулировать чтение конспекта предыдущей лекции

	с помощью проведения устного или письменно экспресс-опроса студентов по ее содержанию в начале следующей лекции. Важным в период подготовки к лекционным занятиям является научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения.
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом (указать текст из источника и др.). Прослушивание аудио- и видеозаписей по заданной теме, решение расчетно-графических заданий, решение задач по алгоритму и др.
Контрольная работа	Контрольная работа выступает, как средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу. Основная цель проведения контрольной работы: знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме.При подготовке к контрольной работе студент должен: 1. Повторить изученный на лекциях и семинарских занятиях материал с помощью имеющихся конспектов, учебных пособий, научных статей и монографий и др. 2. Восполнить пробелы в знаниях (если по каким-либо причинам таковые имеются) путем переписывания конспектов у одногруппников, самостоятельного изучения раздела/темы/вопроса/части вопроса и т.д., консультирования с преподавателем. 3. Особое внимание следует уделить повторению основных понятий и определений дисциплины, а также ключевым моментам изучаемых концепций.
Коллоквиум/ собеседование	Этапы проведения коллоквиума 1. Подготовительный этап: - формулирование темы и проблемных вопросов для обсуждения; - предоставление списка дополнительной литературы; - постановка целей и задач занятия; - разработка структуры занятия; - консультация по ходу проведения занятия; 2. Начало занятия: - подготовка аудитории: поскольку каждая микрогруппа состоит из 5 - 7 студентов, то парты нужно соединить по две, образовав квадрат, и расставить такие квадраты по всему помещению. - комплектация микрогрупп. - раздача вопросов по заданной теме для совместного обсуждения в микрогруппах. 3. Подготовка учащихся по поставленным вопросам. 4. Этап ответов на поставленные вопросы: - впорядке, установленном преподавателем, представители от микрогрупп зачитывают выработанные, в ходе коллективного обсуждения, ответы; - студенты из других микрогрупп задают вопросы отвечающему, комментируют и дополняют предложенный ответ; - преподаватель регулирует обсуждения, задавая наводящие вопросы, корректируя неправильные ответы; - после обсуждения каждого вопроса необходимо подвести общие выводы и логично перейти к обсуждению следующего вопроса; - после обсуждения всех предложенных вопросов преподаватель подводит

	общие выводы; Заключительный этап суммирует все достигнутое с тем, чтобы дать новый импульс для дальнейшего изучения и решения обсуждаемых вопросов (в рамках одного занятия невозможно решить все поставленные проблемы, одна из задач подобного вида занятий, спровоцировать интерес к обсуждаемым проблемам). Преподаватель должен охарактеризовать работу каждой микрогруппы, выделить наиболее грамотные и корректные ответы учащихся.
Реферат	Написание реферата условно разделяется на два этапа: подготовительный и основной; теоретический и практический. На первом этапе студент определяется с темой исследования: А) Преподаватель распределяет темы лично (учитывая ваши возможности и способности).Б) Студенту предоставляется право выбора темы из списка, составленного преподавателем.В) Студент может самостоятельно придумать тему для своего реферата с учетом пройденного материала и дисциплины (обязательно согласовывается с преподавателем заранее).Кроме того, на подготовительном этапе студенты активно должны поработать с литературой и другими источниками информации. Сначала вы должны ознакомиться со всеми доступными источниками информации по заданной теме, постепенно производя отбор публикаций, которые касаются исключительно вашей темы. Можно делать библиографические записи на небольших карточках (по типу библиотечных) или в специальной тетради или блокноте. После того как вы завершите выборку, необходимо не только изучить материалы, но и обработать их различными способами. Если ваша работа будет проверяться системой антиплагиата, то обычное воспроизведение не подходит. Вам следует во время чтения составлять краткий конспект или аннотацию, написанные своими словами. Кроме того, используйте прямое цитирование, если при перефразировании теряется смысл текста. Итогом теоретической части должен стать подробный план вашего реферата. Вы можете составить 5 -6 основных пунктов или разделить их на подпункты, возможно, удобнее разделить весь информационный массив на несколько глав с параграфами. После того, как вы определились с темой, нужно собрать информацию в соответствии с правилами оформления документа. Образец реферата обычно составляет 8-16 страниц, иногда изложение может составлять до 20 страниц текста. Традиционно оно состоит из таких блоков: • Титульный лист реферата. • План работы. • Введение. • Общее изложение темы. • Заключение. • Перечень использованных литературных источников. Чтобы грамотно составить научный доклад следует более подробно остановиться на каждом пункте. Титульный лист вашего реферата. Здесь прописываются полные данные о вашем вузе (факультете, кафедре), специальность или дисциплина, тема исследования, а также личные данные исполнителя и проверяющего преподавателя, в конце обычно указывают город и год написания реферативной работы. Раздел Введения строится по аналогии с курсовой работой и включает такие данные: • Актуальность темы исследования. • Цель и задачи. • Методика и методология исследования. Первая глава обычно содержит данные о становлении проблемы и различных исторических периодах, когда этим вопросом занимались разные известные ученые. Но можно представить это материал в виде библиографического обзора, в котором автор представляет перечень различных источников, где

	описана данная проблема. Постарайтесь максимально использовать наглядный материал. Таблицы, графики, схемы продемонстрируют качество вашей подготовки и заинтересованность темой исследования. В качестве небольшого вывода, стоит отметить степень изученности вашей темы на этом этапе развития науки. Второй раздел может описывать ваши личные исследования, эксперименты, опытные методики, результаты анкетирования или соцопросов и пр. Тогда третья глава будет сопоставлять свежие данные ваших экспериментов и сведения, которые вы почерпнули из литературных источников.В конце реферата автор кратко резюмирует проделанную работу. Выводы оформляют в виде стандартного Заключения, но можно использовать тезисную форму подачи информации. Кроме заключения, автор должен предоставить библиографический список, на который в тексте должны быть ссылки. Количество источников может варьировать от сложности реферата и требований преподавателя, но не стоит ссылаться всего 3–4 пособия, если объем вашей работы более 20 страниц. Будет неплохо, если ваша библиография будет насчитывать от 6 до 10 источников.
Доклад	Подготовленное студентом самостоятельно публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научнойпроблемы. Количество и вес критериев оценки доклада зависят от того, является ли доклад единственным объектом оценивания или он представляет собой только егочасть. Доклад как единственное средство оценивания эффективен, прежде всего, тогда, когда студент представляет результаты своей собственной учебно/научно-исследовательской деятельности, и важным является именно содержание и владение представленной информацией. В этом случае при оценке доклада может быть использована любая совокупность из следующихкритериев: - соответствие выступления теме, поставленным целям изадачам; - проблемность /актуальность; - новизна / оригинальность полученныхрезультатов; - глубина / полнота рассмотрениятемы; - доказательная база / аргументированность / убедительность / обоснованностьвыводов; - логичность / структурированность / целостностьвыступления; - речевая культура (стиль изложения, ясность, четкость, лаконичность, красота языка, учет аудитории, эмоциональный рисунок речи, доходчивость, пунктуальность, невербальное сопровождение, оживление речи афоризмами, примерами, цитатами ит.д.); - используются ссылки на информационные ресурсы (сайты,литература); - наглядность / презентабельность (еслитребуется); - самостоятельность суждений / владение материалом /компетентность. Если доклад сводится к краткому сообщению (10 – 15 минут, может сопровождаться презентацией (10-15 слайдов) и не может дать полного представления о проведенной работе, то необходимо оценивать ответы на вопросы и, если есть, отчет/пояснительную записку.
Рабочая тетрадь	Обязательным элементом является пояснительная записка. В ней указывается предназначение тетради, цели работы с ней, структура, даются указания по использованию тетради, могут быть конкретизированы компетенции, формируемые в ходе работы с рабочей тетрадью. Пояснительная записка должна также знакомить студентов со сроками представления преподавателю заполненной тетрадью, критериями оценки решений и ответов, ее влиянием на итоговую оценку по дисциплине. Содержательная часть структурирована по тематическим разделам. Каждая тема содержит перечень вопросов

	(заданий). Помимо заданий в рабочей тетради должно быть предусмотрено место для ответов студента и оценочных заключений преподавателя. Каждый раздел (тема) рабочей тетради обязательно должен включать в себя методические указания к изучению раздела (темы) и выполнению заданий, а также список рекомендуемых для изучения источников и литературы. Обязательным элементом оформления рабочей тетради студента является титульный лист, содержащий следующие реквизиты: - название вида издания (рабочая тетрадь студента); - принадлежность – студент (ФИО), факультет, курс, группа; - преподаватель, проверяющий - (ФИО).

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Макеты методических материалов, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

ВОПРОСЫ ДЛЯ КОЛЛОКВИУМОВ, СОБЕСЕДОВАНИЯ

по дисциплине «Системы защиты от утечки конфиденциальной информации»
(наименование дисциплины)

Тема 1.
Теоретические основы защиты конфиденциальной информации от внутренних угроз

1. Обосновать соотношение информационной безопасности человека и общества, государства и предпринимательских структур.
2. Классифицировать информационные ресурсы, определить свойства классификационных групп.
3. Дать определение информационной безопасности и проанализировать ее цели, задачи и структуру.
4. Проанализировать содержание концепции информационной безопасности.
5. Обосновать необходимость информационной безопасности человека и общества.
6. Определить место информационной безопасности в структуре информационного права.
7. Проанализировать современные проблемы информационной безопасности предпринимательской деятельности.
8. Дать определение информационным ресурсам, охарактеризовать их основные свойства, взаимосвязь с материальными и иными ресурсами.
9. Проанализировать особенности информационных ресурсов в условиях рыночных отношений.
10. Проанализировать правовые и экономические предпосылки охраны интеллектуальной собственности и защиты предпринимательской информации.

Тема 2.
Нормативно-правовые аспекты защиты конфиденциальной информации от внутренних угроз.

1. Назовите обязательные признаки информации с ограниченным доступом.
2. На какие классы по функциональному назначению подразделяются документы по защите государственной тайны?

3. Дайте определение понятию «гриф секретности».
4. Какие сведения не относятся к государственной тайне и не подлежат засекречиванию?
5. Перечислите органы защиты государственной тайны.
6. Какие существуют методы защиты сведений, составляющих государственную тайну?
7. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.
8. Какие сведения относятся к банковской тайне?
9. Перечислите известные вам виды профессиональной тайны.
10. Раскройте порядок обращения с документами, содержащими служебную тайну.
11. Какая информация относится к сведениям конфиденциального характера?
12. Что представляет собой информация, составляющая коммерческую тайну?
13. Что понимается под разглашением информации, составляющей коммерческую тайну?
14. По каким признакам определяется перечень сведений, составляющих коммерческую тайну предприятия?
15. В отношении, каких сведений не может быть установлен режим коммерческой тайны?
16. Приведите меры по охране конфиденциальности информации в соответствии с законом «О коммерческой тайне».

Тема 3.
Административно-организационные аспекты корпоративной защиты от внутренних угроз.

1. Определить сущность несанкционированного канала утраты конфиденциальной информации.
2. Классифицировать организационные каналы утраты конфиденциальной информации.
3. Классифицировать технические каналы утраты конфиденциальной информации.
4. Показать соотношение организационных и технических каналов утраты информации в компьютерах и локальных сетях.
5. Обосновать необходимость защиты информационных ресурсов от несанкционированного доступа.
6. Концептуальные особенности защиты информации, ее органическая связь с информационной безопасностью.
7. Дать определение термину "защита информации", специфики его использования.
8. Определить понятие "система защиты информации", обосновать ее цель, задачи и принципы построения.
9. Обосновать структуру системы защиты информации, охарактеризовать ее комплексность.

Тема 4.
Защита корпоративной информации с использованием автоматизированной системы контроля информационных потоков.

1. Определить понятие угрозы информации, классифицировать угрозы по различным основаниям.
2. Назначение и содержание правового элемента системы защиты.
3. Назначение и содержание организационного элемента системы защиты.
4. Назначение и содержание инженерно-технического элемента системы защиты.
5. Назначение и содержание программно-аппаратного элемента системы защиты.
6. Назначение и содержание криптографического элемента системы защиты.
7. Критерии формирования системы защиты в зависимости от ценности информации, размера прибыли или убытков и стоимости системы защиты.
8. Определить состав простейших методов защиты информации в некрупных фирмах.
9. Концепция использования конфиденциальной информации в практической работе фирмы.

10. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
11. Дать соотношение понятий "допуск" и "доступ" к конфиденциальной информации.
12. Дать перечень методов расчленение (дробления) тайны фирмы на составные элементы.
13. Обосновать принципы практической реализации системы доступа персонала к конфиденциальной информации.
14. Проанализировать обязанности руководителей и специалистов в сфере персональной ответственности за сохранность носителя и конфиденциальность информации.
15. Определить порядок классификации конфиденциальных информационных ресурсов в предпринимательских структурах различного типа.
16. Проанализировать состав показателей (граф и зон) перечня конфиденциальных сведений фирмы, обосновать целевое назначение показателей и их взаимосвязь.

Критериоценки

«5 (отлично)»

- глубокое и прочное усвоение программного материала;
- полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания;
- свободно справляющиеся с поставленными задачами, знания материала;
- правильно обоснованные принятые решения;
- владение разносторонними навыками и приемами выполнения практических работ.

«4 (хорошо)»

- знание программного материала;
- грамотное изложение, без существенных неточностей в ответе на вопрос;
- правильное применение теоретических знаний;
- владение необходимыми навыками при выполнении практических задач.

«3 (удовлетворительно)»

- усвоение основного материала;
- при ответе допускаются неточности;
- при ответе недостаточно правильные формулировки;
- нарушение последовательности в изложении программного материала;
- затруднения в выполнении практических заданий;

«2 (неудовлетворительно)»

- не знание программного материала;
- при ответе возникают ошибки;
- затруднения при выполнении практических работ.

ТЕМЫ РЕФЕРАТОВ, ДОКЛАДОВ

по дисциплине «Системы защиты от утечки конфиденциальной информации»
(наименование дисциплины)

1. Понятие, проблемы и структура информационной безопасности (на примере фирм различных типов).
2. Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
3. Информационная безопасность, история формирования.
4. Концепция информационной безопасности.
5. Основы экономической безопасности предпринимательской деятельности.
6. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
7. Информационная безопасность (по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну.
12. Построение и функционирование защищенного документооборота.
13. Анализ инструкции по обработке и хранению конфиденциальных документов.
14. Направления и методы защиты документов на бумажных носителях.
15. Направления и методы защиты машиночитаемых документов.
16. Направления и методы защиты электронных документов.
17. Архивное хранение конфиденциальных документов.
18. Направления и методы защиты аудио и визуальных документов.
19. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
20. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
21. Соотношение источников, каналов распространения и каналов утечки информации.
22. Анализ опыта защиты информации в зарубежных странах.
23. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
24. Основы технологии обработки и хранения конфиденциальных документов.
25. Назначение, виды, структура и технология функционирования системы защиты информации.
26. Направления экономического анализа системы защиты информации.
27. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
28. Направления и методы защиты профессиональной тайны.
29. Направления и методы защиты служебной тайны.
30. Направления и методы защиты персональных данных о гражданах.
31. Методы защиты личной и семейной тайны.
32. Проблемы управления персоналом и защиты информации в предпринимательской деятельности.
33. Порядок подбора персонала для работы с конфиденциальной информацией.
34. Тестирование и проведение собеседования с претендентами на должность, связанную с секретами фирмы.
35. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
36. Порядок подготовки и проведения переговоров и совещаний по конфиденциальным вопросам.

37. Задачи, функции и графическая структура служб конфиденциальной документации в фирмах различных типов, нормативно-методическое обеспечение их деятельности.
38. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
39. Направления защиты компьютеров и локальных сетей от несанкционированного доступа к информации.
40. Аналитический обзор различных технологий хранения конфиденциальных документов.
41. Назначение, виды и технология учета конфиденциальных документов.
42. Составление библиографии по проблемам экономической безопасности, защиты предпринимательской тайны и конфиденциальной информации (российская и зарубежная литература).
43. Процессуальные проблемы защиты информации в зарубежных странах.
44. Анализ существующих схем доступа персонала в помещения фирмы.
45. Аналитический обзор опыта зарубежных стран в регламентации управления персоналом, обладающим конфиденциальной информацией.
46. Аналитический обзор российского и зарубежного исторического опыта в предотвращении утраты ценной информации по вине сотрудников.
47. Анализ существующих правил поведения персонала и охраны фирмы в экстремальных ситуациях различного типа.
48. Проблемы управления персоналом и защиты информации в предпринимательской деятельности (теоретический очерк).
49. Цели, задачи, стадии и методы работы с персоналом, обладающим конфиденциальной информацией.
50. Классификация персонала фирмы и окружающих фирму людей по степени их осведомленности в тайнах фирмы, анализ каждой классификационной группы.
51. Классификация экстремальных ситуаций, угрожающих персоналу фирмы в рабочее и нерабочее время, анализ выделенных классификационных групп и методов локализации опасности.
52. Порядок и методика проведения служебного расследования по фактам нарушения правил защиты информации фирмы.
53. Классификация противоправных действий персонала фирмы с конфиденциальной информацией.
54. Принципы построения, организация и совершенствование пропускного режима на фирме, методика идентификации различных категорий сотрудников и посетителей.

Критерии оценивания за устное выступление при обсуждении вопроса

5 «Отлично»	выступление (доклад) отличается последовательностью, логикой изложения. Легко воспринимается аудиторией. При ответе на вопросы выступающий (докладчик) демонстрирует глубину владения представленным материалом. Ответы формулируются аргументировано, обосновывается собственная позиция в проблемных ситуациях.
4 «Хорошо»	выступление (доклад) отличается последовательностью, логикой изложения. Но обоснование сделанных выводов не достаточно аргументировано. Неполно раскрыто содержание проблемы.
3 «Удовлетворительно»	выставляется, если выступающий (докладчик) передает содержание проблемы, но не демонстрирует умение выделять главное, существенное. Выступление воспринимается аудиторией сложно.
2 «Неудовлетворительно»	выступление (доклад) краткий, неглубокий, поверхностный.

Критерии оценивания за подготовку реферата

5 «Отлично»	выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
4 «Хорошо»	основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
3 «Удовлетворительно»	имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
2 «Неудовлетворительно»	тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Критерии оценивания доклада с презентацией

2 «Неудовлетворительно»	Студент демонстрирует первичное восприятие некоторых основных элементов медиаработы. Она проста и незакончена. Проблема не раскрыта. Отсутствуют выводы. Не использованы возможности визуализации материала в PowerPoint. Больше 4 ошибок в представляемой информации.
3 «Удовлетворительно»	Некоторая степень владения большинством элементов медиаработы. Частично присутствует гармоничная интеграция элементов в целое, но работа незавершенная. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Частично использованы возможности визуализации материала в PowerPoint. 3-4 ошибки в представляемой информации.
4 «Хорошо»	Студент показывает владение элементами медиаработы. В основном, она ясная и целостная. Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы. Использованы информационные технологии (PowerPoint). Не более 2 ошибок в представляемой информации.
5 «Отлично»	Студент продемонстрировал уверенное владение и интеграцию всех элементов медиаработы. Работа целостна, креативна. Использован творческий подход. Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы. Широко использованы информационные технологии (PowerPoint). Отсутствуют ошибки в представляемой информации.

ФГБОУ ВО «КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
БАЛТИЙСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ РЫБОПРОМЫСЛОВОГО ФЛОТА

Типовые тестовые (или контрольные) задания

Дисциплина:	Основыинформационной безопасности	Специальность:	10.05.03.
Семестр:	IV		
Кафедра:	Информационная безопасность		

1.	Каким свойством не обладает информация в форме сообщения? а) материальность б) измеримость г) простота д) проблемная ориентированность
2.	Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия, является угрозой: а) конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности б) информационному обеспечению государственной политики РФ г) развитию отечественной индустрии информации, включая индустрию телекоммуникации, связи и средств информатизации д) безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России
3.	Информационным ресурсом является: а) вся накопленная информация, в том числе и недостоверная, представленная сомнительными фактами, ложными положениями, потерявшая конкретность б) только достоверная информация из проверенных источников г) вся накопленная информация, в том числе и недостоверная, представленная сомнительными фактами, ложными положениями, но не потерявшая своей конкретности д) достоверная информация из проверенных источников, включая устаревшую информацию
4.	Утечка информации – это … а) несанкционированный процесс переноса информации от источника к злоумышленнику б) процесс раскрытия секретной информации в) процесс уничтожения информации г) непреднамеренная утрата носителя информации
5.	Информация, поступающая к человеку обладает следующими свойствами: а) идеальность, объективность, динамичность б) идеальность, объективность, простота г) динамичность, субъективность, накапливаемость д) субъективность, неидеальность, информационная неуничтожаемость
6.	Преднамеренной угрозой безопасности информации является: а) наводнение б) повреждение кабеля, по которому идет передача, в связи с погодными условиями в) кража г) ошибка разработчика
7.	Концепция системы защиты от информационного оружия не должна включать… а) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры б) средства нанесения контратаки с помощью информационного оружия в) признаки, сигнализирующие о возможном нападении г) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей
8.	В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на … а) соблюдение норм международного права в сфере информационной безопасности б) выявление нарушителей и привлечение их к ответственности

	в) разработку методов и усовершенствование средств информационной безопасности г) соблюдение конфиденциальности информации ограниченного доступа
9.	Информация, составляющая государственную тайну, не может иметь гриф… а) «для служебного пользования» б) «секретно» в) «совершенно секретно» г) «особой важности»
10.	Одной из основных угроз доступности информации является: а) злонамеренное изменение данных б) хакерская атака в) непреднамеренные ошибки пользователей г) перехват данных
11.	Что не относится к компьютерной преступности? а) подделка компьютерной информации б) хищение информации в) распространение вирусов г) согласованное копирование данных
12.	Как называется комплекс мероприятий направленных на обеспечение информационной безопасности? а) защитой информации б) авторизацией в) информационной безопасностью г) безопасным состоянием
13.	Кто отвечает за защиту автоматизированной системы от несанкционированного доступа к информации? а) пользователь б) аутентификатор в) авторизатор г) администратор защиты
14.	Перехват данных является угрозой… а) доступности б) целостности в) конфиденциальности г) для администратора
15.	Сбор и накопление информации о событиях, происходящих в информационной системе, называется… а) протоколированием б) аудитом в) экранированием г) криптографией
16.	Что не относится к основополагающим документам в области информационной безопасности? а) концепция о криптостойкости систем б) оранжевая книга в) рекомендации X.800 г) концепция защиты от несанкционированного доступа Гостехкомиссии при Президенте РФ
17.	Как называется набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию? а) эффективность защиты б) политика безопасности в) гарантированность г) гармонизированность безопасности
18.	Что не входит в аспекты информационной безопасности? а) доступность б) целостность в) стойкость г) конфиденциальность

19.	Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем б) объективных проблем современной технологии программирования в) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы г) постоянные атаки хакеров
20.	В число принципов управления персоналом входит: а) разделяй и властвуй б) разделение обязанностей в) метод кнута и пряника г) разделение доступа
21.	Меры информационной безопасности направлены на защиту от: а) нанесения неприемлемого ущерба б) нанесения любого ущерба в) подглядывания в замочную скважину г) нанесения морального вреда
22.	На межсетевые экраны целесообразно возложить следующие функции: а) антивирусный контроль "на лету" б) антивирусный контроль компьютеров внутренней сети в) антивирусный контроль компьютеров внешней сети г) антивирусный контроль всех съемных носителей
23.	На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют: а) меры ограниченной направленности б) мерынаправляющие и координирующие в) меры по обеспечению информационной независимости г) меры по поддержанию государственной безопасности
24.	Системы анализа защищенности помогают: а) оперативно пресечь известные атаки б) предотвратить известные атаки в) восстановить ход известных атак г) восстановить логические связи
25.	Сложность обеспечения информационной безопасности является следствием: а) невнимания широкой общественности к данной проблематике б) все большей зависимости общества от информационных систем в) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним г) обширной структуры предмета информационная безопасность
26.	Уровень безопасности С, согласно "Оранжевой книге", характеризуется: а) произвольным управлением доступом б) принудительным управлением доступом в) верифицируемой безопасностью г) комплексным управлением доступом
27.	Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что: а) с программно-технической точки зрения, информационная безопасность - ветвь информационных технологий и должна развиваться по тем же законам б) объектно-ориентированный подход популярен в академических кругах в) объектно-ориентированный подход поддержан обширным инструментарием г) объектно-ориентированный подход широко применяется в государственных структурах
28.	В число принципов физической защиты входят: а) беспощадный отпор б) непрерывность защиты в пространстве и времени в) минимизация защитных средств г) наличие охранника
29.	Что из перечисленного не относится к числу основных аспектов информационной безопасности: а) доступность б) конфиденциальность

	в) целостность г) масштабируемость
30.	Совместно с криптографическими сервисами туннелирование может применяться для достижения следующих целей: а) обеспечение гарантированной полосы пропускания б) обеспечение высокой доступности сетевых сервисов в) обеспечение конфиденциальности и целостности передаваемых данных г) обеспечение максимального уровня защищенности хранимых данных

Вопросы рассмотрены и утверждены на заседании кафедры	Дата:	Протокол №
Заведующий кафедрой	подпись	

Критерии оценивания выполнения тестирования (контрольного задания)

а) типовые задания к тесту

Формы тестовых заданий:
- выбор правильных ответов из перечисленных;
- установление правильной последовательности;
- установление соответствия.

б) критерии оценивания

Критерием оценивания теста является количество правильно выполненныхтестовых заданий, свидетельствующих о полноте знаний теоретического материала вобласти экономико-математического моделирования.

в) описание шкалы оценивания

5 «Отлично» - процент правильно выполненных заданий составляет от 80% до 100.
4 «Хорошо» - процент правильно выполненных заданий составляет от 60% до 79.
3 «Удовлетворительно» - процент правильно выполненных заданий составляет от50% до 59%.
2 «Неудовлетворительно» - процент правильно выполненных заданий составляетменее 50%.

Критерии оценивания отчета по лабораторным работам

а) разделы отчета

- наименование лабораторной работы;
- постановка задачи, исходные данные;
- описание методов и способов решения;
- этапы решения задачи и (или) ее алгоритмическое обеспечение;
- результаты, представленные в виде таблиц, графиков и т.п. с краткимипояснениями;
- выводы.

б) критерии оценивания

Студент должен продемонстрировать:
- умения применять математические методы для формализации и решенияприкладных задач; строить модели экономических процессов, исследовать их ивырабатывать рекомендации к их применению на практике; организовыватьвычислительный эксперимент на компьютере для исследования поведения экономическихобъектов, систем, процессов;
- владение навыками работы с пакетами прикладных программ для моделирования ианализа экономических процессов.

в) описание шкалы оценивания

- **«Зачтено»** выставляется в случае, если студент выполнил в полном объемелабораторную работу, не допустил ошибок в расчетах, сделал выводы, свободно излагаетэтапы решения и результаты работы.
- **«Незачтено»** выставляется в случае, если студент не выполнил лабораторнуюработу, либо выполнил, но допустил существенные ошибки в расчетах и (или) не сделалвыводы, и (или) не может изложить этапы решения и результаты работы.

Критерии оценивания зачета

Критерии оценок на **дифференцированном зачете** по дисциплине (отлично, хорошо, удовлетворительно, неудовлетворительно):

- «ОТЛИЧНО» выставляется в случае правильных, полных и четких ответов на теоретические вопросы, с их проецированием и интерпретацией на сегодняшнюю ситуацию. Допускаются непринципиальные погрешности или небольшая незавершенность ответов, диктуемых лимитом времени.
- «ХОРОШО» выставляется в случаях: правильных и четких ответов при незначительных замечаниях, неточностях.
- «УДОВЛЕТВОРИТЕЛЬНО» выставляется в случаях ответа на большую часть (не менее 50% основных положений); при правильном ответе на один вопрос или неполных ответах на два вопроса.
- «НЕУДОВЛЕТВОРИТЕЛЬНО» выставляется при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

Зачет по дисциплине осуществляется при условии выполнения заданий всех практических занятий, самостоятельной работы, а также результатами проведенной оценки остаточных знаний.

Формат сведений о ФОС и ее согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины

Б1.В.ДВ.07.01 «Системы защиты от утечки конфиденциальной информации»
(код) (наименование дисциплины)

образовательной программы специалитетапо специальности
10.05.03. Информационная безопасность автоматизированных систем

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
(наименование специализации)

утвержденной «27» июня 2018г.

Автор фонда – доцент кафедры ИБ Жестовский А.Г.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры «Информационной безопасности»

(протокол № 9 от 14 июня 2018г.)

Заведующий кафедрой ИБ _____/Великите Н.Я./

Фонд оценочных средств рассмотрен и одобрен на заседании методической комиссии радиотехнического факультета

(протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии факультета

_____/А.Г. Жестовский/

Согласовано

Начальник отдела мониторинга и контроля

_____/Борисевич Ю.В./